Хмельницький національний університет
Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах
Назва теми

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

КРМКІ. 190170.19.01.03 ПЗ

Виконала: студентка 2 курсу, група КІ1м-19-1 _____ Атаманюк А.В.
Підпис

Керівник доц., к. т. н., доцент кафедри КбКСМ _____ Джулій В.М.
Підпис

Нормоконтролер доц., к. т. н., доцент кафедри КбКСМ _____ Муляр І.В.
Підпис

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

4 12 2020 р

Хмельницький, 2020

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж
Освітній рівень магістр
Галузь знань 12 Інформаційні технології
Спеціальність 123 Комп'ютерна інженерія
Освітня програма освітньо-професійна програма підготовки магістра

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки та
комп'ютерних систем і мереж
к.т.н. доцент Кльоц Ю.П.
"4" 09 2020 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Атаманюк Алла Василівна
Прізвище, ім'я, по батькові студента

1. Тема проєкту (роботи) Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах
Науковий керівник Джулій Володимир Миколайович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджена наказом № 118 ректора університету додаток №23 від 01.09.2020
2. Строк подання студентом проєкту (роботи) на кафедру 03.12.2020
3. Вихідні дані до проєкту (роботи) Проведення аналізу основних підходів до моделювання загрози поширення забороненої інформації. Розробити імітаційну модель загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах. Розробити методику формування топології інформаційно-телекомунікаційної мережі.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз та дослідження поширення забороненої інформації в інформаційно-телекомунікаційних мережах
Математичні моделі безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах
Розробка методики формування топології великомасштабної інформаційно-телекомунікаційної мережі
Особливості реалізації автоматизованої системипротидії загрозі поширення забороненоїінформації
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) 1,2.Тема, мета магістерської роботи, об'єкт, предмет, задачі дослідження, наукова новизна, практична цінність, апробація роботи. 3. Структурна схема інформаційно-телекомунікаційної мережі. 4 Функції захисту від забороненої інформації в інформаційно-телекомунікаційній мережі. 5 Аналітична модель динаміки атаки $I(t)$ та модель захисту вузлів $R(t)$. 6. Схема реалізації загрози поширення забороненої інформації в інформаційно-телекомунікаційній мережі. 7. Імітаційна модель загрози пошерення забороненої інформації в інформаційно-телекомунікаційній мережі. 8. SIR–епідеміологічна модель. 9. Розподілене моделювання загрози поширення забороненої інформації в ІТКМ. 10. Висновки.

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Відповідальний за оформлення КРМ	Муляр І.В., доцент, к.т.н.		

7. Дата видачі завдання «01» лютого 2020 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	*Примітка*
1	Ґрунтовне ознайомлення з предметною галуззю	02.02.2020	Виконано
2	Визначення структури магістерської роботи	02.03.2020	Виконано
3	Робота над першим розділом магістерської роботи	01.04.2020	Виконано
4	Робота над першою статтею за результатами обробки літературних джерел	01.05.2020	Виконано
5	Робота над другим розділом магістерської роботи	01.06.2020	Виконано
6	Робота над третім розділом магістерської роботи	01.09.2020	Виконано
7	Робота над четвертим розділом магістерської роботи	01.10.2020	Виконано
8	Підготовка ілюстративного матеріалу	01.11.2020	Виконано
9	Оформлення текстової і графічної частини магістерської роботи	05.11.2020	Виконано
10	Попередній захист магістерської роботи	10.11.2020	Виконано
11	Захист КРМ на засіданні ЕК	08.12.2020	Виконано

Студент _____ А.В. Атаманюк
Підпис Ініціали, прізвище

Керівник проєкту (роботи) _____ В.М. Джулій
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах».

Автор роботи: Атаманюк Алла Василівна.

Керівник роботи: к.т.н., доц. Джулій Володимир Миколайович

Загальний обсяг роботи: 102 сторінки, 58 рисунків, 8 таблиць, 50 посилань, 3 додатки.

ІНФОРМАЦІЙНА БЕЗПЕКА, АНАЛІТИЧНА МОДЕЛЬ, ІМІТАЦІЙНА МОДЕЛЬ, ПОШИРЕННЯ ЗАГРОЗ, ІНФОРМАЦІЙНА ВЗАЄМОДІЯ, МОДЕЛЬ МЕРЕЖІ

Метою дипломної роботи є підвищенні точності прогнозування загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Дана дипломна робота присвячена розробці методу виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах. Запропонована імітаційна модель загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації загрози поширення забороненої інформації від топологічної уразливості мережі.

Дата

04.12.2020

Підпис студента

ANNOTATION

a master's degree work of Atamaniuk Alla

entitled «A method of detecting the threat of dissemination of prohibited information in information and telecommunication networks».

Mentor: Volodymyr Dzhuliy

Total volume of work: 102 pages, 58 figures, 8 tables, 50 references, 3 appendices.

INFORMATION SECURITY, ANALYTICAL MODEL, SIMULATION MODEL, THREAT PROPAGATION, INFORMATION INTERACTION, NETWORK MODEL

The purpose of the thesis is to improve the accuracy of forecasting the threat of dissemination of prohibited information in information and telecommunications networks.

This thesis is devoted to the development of a method for detecting the threat of dissemination of prohibited information in information and telecommunications networks. A simulation model of the threat of dissemination of prohibited information in information and telecommunication networks is proposed, which takes into account the topological characteristics of the network, as well as the features of information interaction of subscribers as human-machine systems. With its help experiments were carried out, the results of which showed the dependence of the realization of the threat of dissemination of prohibited information on the topological vulnerability of the network.

/Date

04.12.2020

Signature

ЗМІСТ

ВСТУП

Актуальність роботи. Інформаційно-телекомунікаційні мережі (ІТКМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. Сучасною проблемою таких систем є їх низький рівень інформаційної безпеки. Для забезпечення захисту інформації в телекомунікаційних мережах, включаючи Інтернет, розроблено безліч методів і засобів, запропонованих в працях Р. Бретта, К. Касперскі, С. Норкатта, В. Столінгса, В.А. Герасименка, С.П. Розторгуєва, П.Д. Зегжди, В.І. Завгороднього, А.А. Малюка, А.А. Груші, В.В. Домарєва. Ефективного захисту абонентів від загрози поширення забороненої інформації, зокрема в умовах широкого використання індивідуально-орієнтованих сервісів і пов'язаних з ними протоколів і технологій (CORBA, SOAP, REST тощо), не існує. Серед безлічі функцій захисту, принциповою в відношенні даних систем, є функція попередження прояву забороненої інформації. Вона реалізується за рахунок механізмів прогнозування загрози поширення і розсилання повідомлень з попередженнями про наслідки дій зі забороненим контентом. Використання інших функцій (попередження, виявлення, локалізації та ліквідації загрози) припускає наявність повного контролю над системою, що в реальних умовах неможливо.

Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗПЗІ) є моделювання з використанням моделей впливу, моделей просочування і зараження (Д.А. Новіков, Д.А. Губанов, А.Г. Чхартішвілі, J. Leveille, D. Watts і S. Strogatz, R. Albert і A. Barabasi, J. Leskovec, M. Gjoka, S.N. Dorogovtsev, M.E.J. Newman і R.M. Ziff, J.O. Kephart і S.R. White та ін.). Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня довжина шляху). Взаємодія між абонентами в межах цих математичних моделей описується переважно гомогенним графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку

прогнозування загрози поширення забороненої інформації більше 30%. Крім того, дані підходи мають в основному теоретичний характер, практика їх використання не виходить за межі експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів загрози поширення забороненої інформації, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Об’єктом дослідження є інформаційно-телекомунікаційні мережі, що знаходяться під впливом загрози поширення забороненої інформації.

Предметом дослідження є моделі загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Мета магістерської роботи полягає в підвищенні точності прогнозування загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Відповідно до вказаної мети в роботі поставлені, обгрунтовані і вирішені наступні завдання:

1. Проведено інформаційний огляд і експерименти для виявлення істотних характеристик об’єкта і зовнішніх чинників, що впливають на процес реалізації загрози поширення забороненої інформації. Проаналізовано основні підходи до моделювання загрози поширення забороненої інформації.

2. Розроблено імітаційну модель загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

3. Синтезовано і показано адекватність аналітичної моделі загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

4. Розроблено методику формування топології інформаційно-телекомунікаційної мережі.

5. Змодельовано процес реалізації загрози поширення забороненої інформації на топології реальної великомасштабної інформаційно-телекомунікаційної мережі з використанням розробленого програмного

забезпечення. Проведено експериментальне дослідження за отриманими результатами.

Методи дослідження. Рішення сформульованої в магістерській роботі, проблеми розробки моделей і алгоритмів виявлення загроз поширення забороненої інформації в інформаційно-телекомунікаційних мережах, базується на методах системного аналізу, теорії ймовірності, випадкових процесів і математичної статистики, методів чисельного аналізу, імітаційного моделювання.

Основні нові результати, отримані в роботі та виносяться на захист:

1. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах

2. Методику формування топології великомасштабної інформаційно-телекомунікаційної мережі, що включає:

- алгоритм формування графа доступної частини мережі, що дозволяє провести збір даних про топологію з будь-якого вузла-абонента;
- алгоритм формування повного графа мережі, що дозволяє в умовах неповноти вихідних даних спрогнозувати топологію частини мережі, якої бракує.

Практична цінність і реалізація результатів роботи. Практична цінність результатів магістерської роботи полягає в отриманих розрахункових виразах, моделях і алгоритмах, що реалізують виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Достовірність наукових положень, висновків і обґрунтованість отриманих в магістерській роботі результатів підтверджується коректною постановкою завдань, коректністю використовуваного математичного апарату, результатами моделювання та апробацією отриманих результатів на конференціях. Отримані в ході виконання магістерського дослідження результати не суперечать раніше отриманим даним, описаним в літературі іншими авторами.

Особистий внесок. Всі дослідження, викладені в магістерській роботі, проведені автором в процесі наукової діяльності. Результати, які виносяться на захист, отримані автором особисто, запозичений матеріал позначений в роботі посиланнями.

Апробація роботи. За темою дипломної роботи ОКР «Магістр» опубліковано 2 наукові статті (одна у фаховому науковому виданні України, одна у нефаховому виданні).

Результати магістерської роботи апробовані на міжнародних науково-технічних конференціях (1 тези доповіді):

- Науково-практична інтернет-конференція молодих науковців і студентів «Інтелектуальний потенціал – 2020» (НПК МНІС ІП-2020), 10 листопада 2020 р, м. Хмельницький.
- XVI Міжнародна науково-практичної конференції “Військова освіта і наука: сьогодення та майбутнє”, 27 листопада 2020 року, м. Київ.

Структура і обсяг роботи. Дипломна робота ОКР «Магістр» складається зі вступу, основної частини, що містить 4 розділи, висновків і списку використаних джерел. Загальний обсяг роботи – 102 сторінки. Робота містить 58 рисунків та 8 таблиць. Список використаної літератури включає 50 бібліографічних джерела.

1 АНАЛІЗ ТА ДОСЛІДЖЕННЯ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1. Аналіз та дослідження безпеки в інформаційно-телекомунікаційних мережах

Інформаційно-телекомунікаційні мережі (ІТКМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. Інформаційно-телекомунікаційна мережа надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярними з ІТКМ є соціальні мережі.

У світі існує величезна кількість різних соціальних мереж, але в кожній країні та регіоні існує кілька найбільш популярних представників (рисунок 1.1). В США це Facebook, MySpace, Twitter та LinkedIn; Nexopia – в Канаді; Bebo – у Великій Британії; Facebook, dol2day – в Німеччині; «ВКонтакте», «Одноклассники», «Мой Мир@mail.ru» – у Росії.

На сьогодні в Україні самими популярними є соціальні мережі: Facebook, Instagram, YouTube.

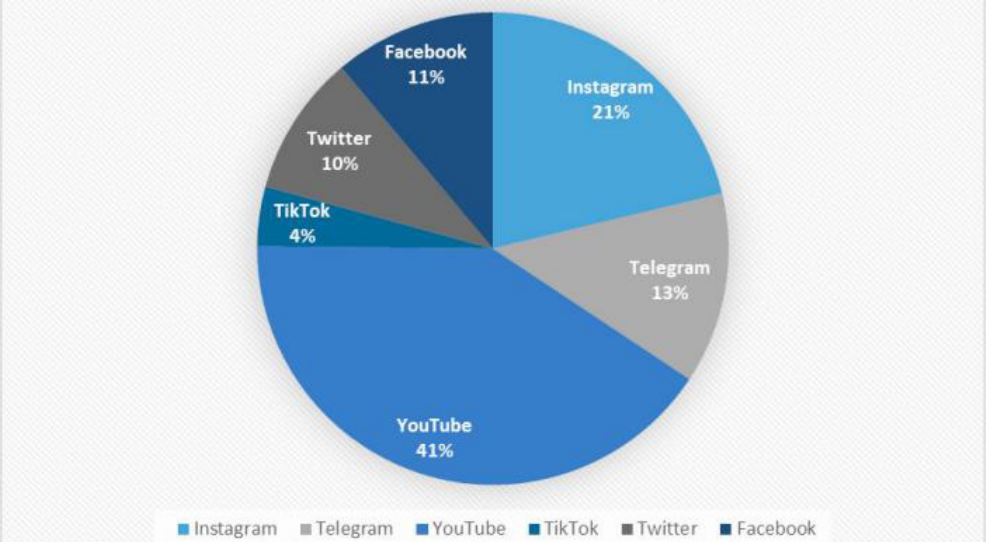


Рисунок 1.1 – Рейтинг соціальних мереж за популярністю у світі [27]

На рисунку 1.2 зображена динаміка зростання користувачів самої популярної соціальної мережі Facebook.

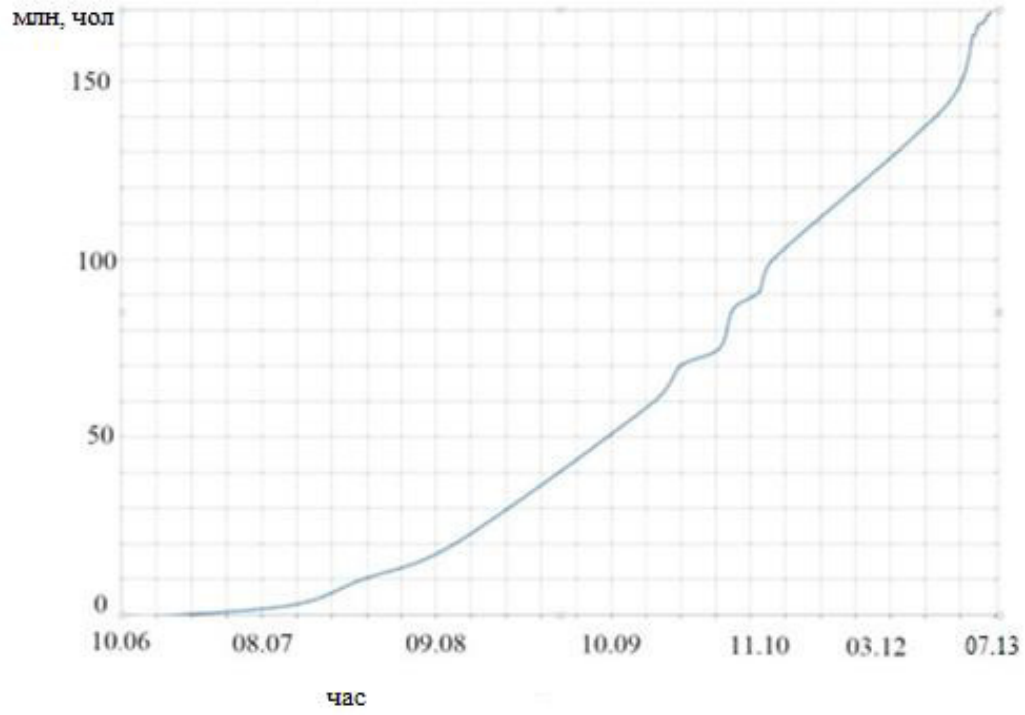


Рисунок 1.2 – Динаміка зростання користувачів соціальної мережі Facebook

З бурхливим ростом кількості користувачів інформаційно-телекомунікаційних мереж виникають і проблеми безпеки в них.

На рисунку 1.3. відображено узагальнену структурну схему інформаційно-телекомунікаційних мереж (ІТКМ). Її склад в загальному випадку утворюють такі функціональні елементи:

- абоненти (А). Під абонентом розуміється людино-машинна система, що складається з пристрою, через який здійснюється доступ до мережі, і безпосередньо користувача ІТКМ. Абоненти можуть бути окремими вузлами мережі (якщо користувач використовує свій домашній комп'ютер), або можуть бути об'єднані в корпоративну обчислювальну мережу (КОМ) (якщо абонент використовує робочий комп'ютер), включають в себе модулі (інформаційного) захисту (МЗ) і програмне забезпечення (браузер) для взаємодії з керуючим елементом;

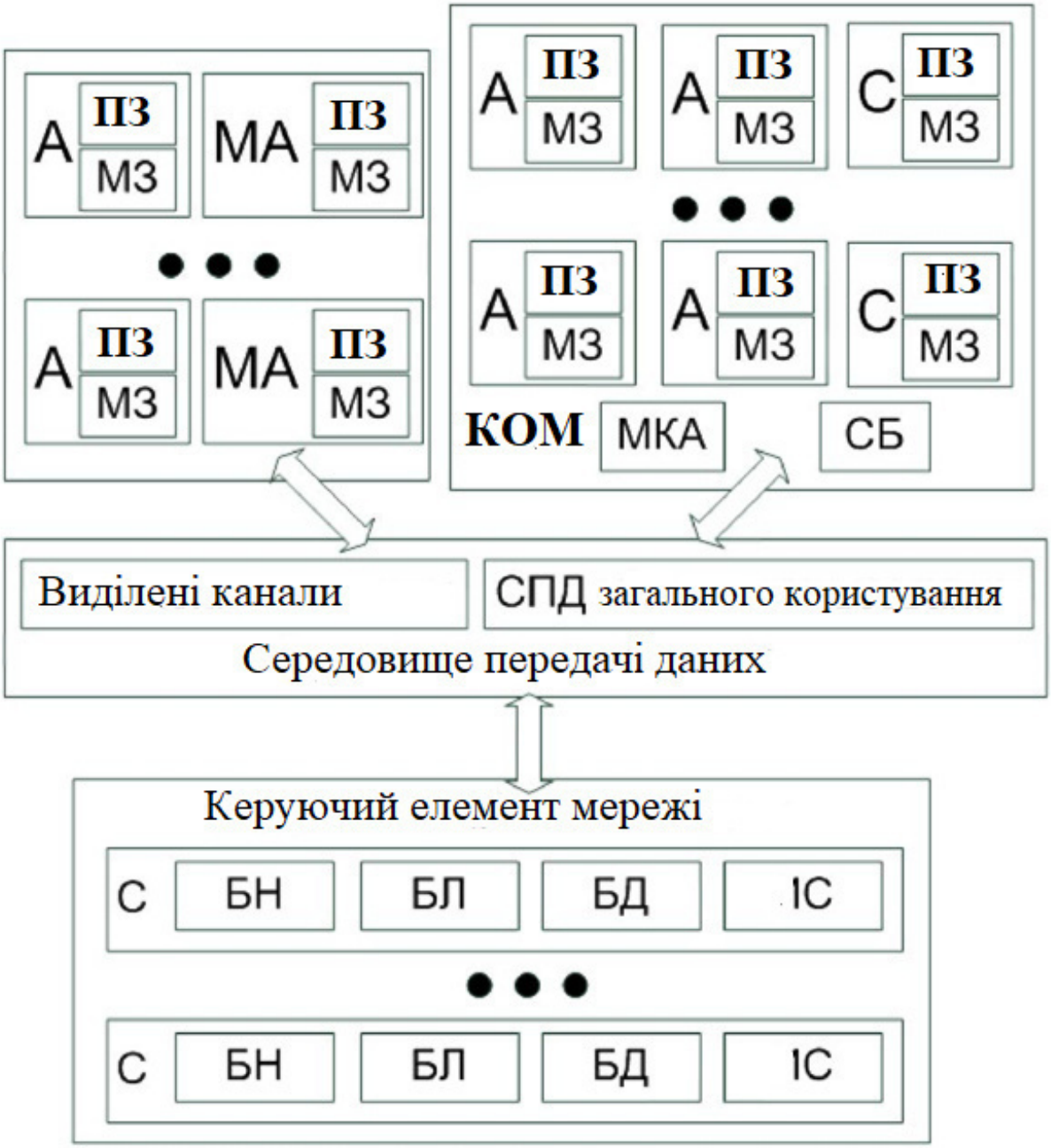


Рисунок 1.3 – Структурна схема ІТКМ

- мобільні абоненти (МА). Користувачі, які використовують мобільні пристрої (смартфони, планшети тощо), для доступу до мережі, а також використовують програмне забезпечення (спеціальний додаток) і модулі захисту (МЗ);

- сервери (С). У корпоративних обчислювальних мережах (КОМ) знаходяться інформаційні сервери різного функціонального призначення, які

беруть участь в інформаційній взаємодії (наприклад, проксі-сервера);

- КОМ містить крім абонентів і серверів, також засоби маршрутизації, комутації та адміністрування (МКА), систему безпеки (СБ), що включає механізми захисту для всієї корпоративної мережі;

- засоби телекомунікації, що забезпечують взаємодію абонентів між собою;

- керуючий елемент технічно є сукупністю комутуючого і серверного устаткування, що реалізує основні функції системи. Включає в себе сервери, які містять в загальному випадку: балансувальник навантаження (БН), елемент бізнес-логіки (БЛ), бази даних (БД), інфраструктурні системи (ІС) (системи статистики, конфігурації, моніторингу тощо).

Опишемо багатошарову архітектуру типового керуючого елемента (рисунок 1.4):

1. Презентаційний шар. На цьому шарі приймаються HTTP-запити від абонентів, зазвичай веб-браузерів, і видаються їм HTTP-відповіді, як правило, разом з HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними. На презентаційному шарі здійснюється розподіл і балансування навантаження, ведення журналу звернень абонентів до ресурсів.

2. Шар бізнес сервісів, який призначений для підбору та обробки даних.

3. Персистентний шар, що виконує обслуговування і управління базою даних і відповідає за цілісність та збереження даних, а також забезпечує операції введення-виведення при доступі абонента до інформації.

4. Шар загальних інфраструктурних систем, на якому розміщуються системи протоколювання статистики, конфігурації додатків, моніторингу.

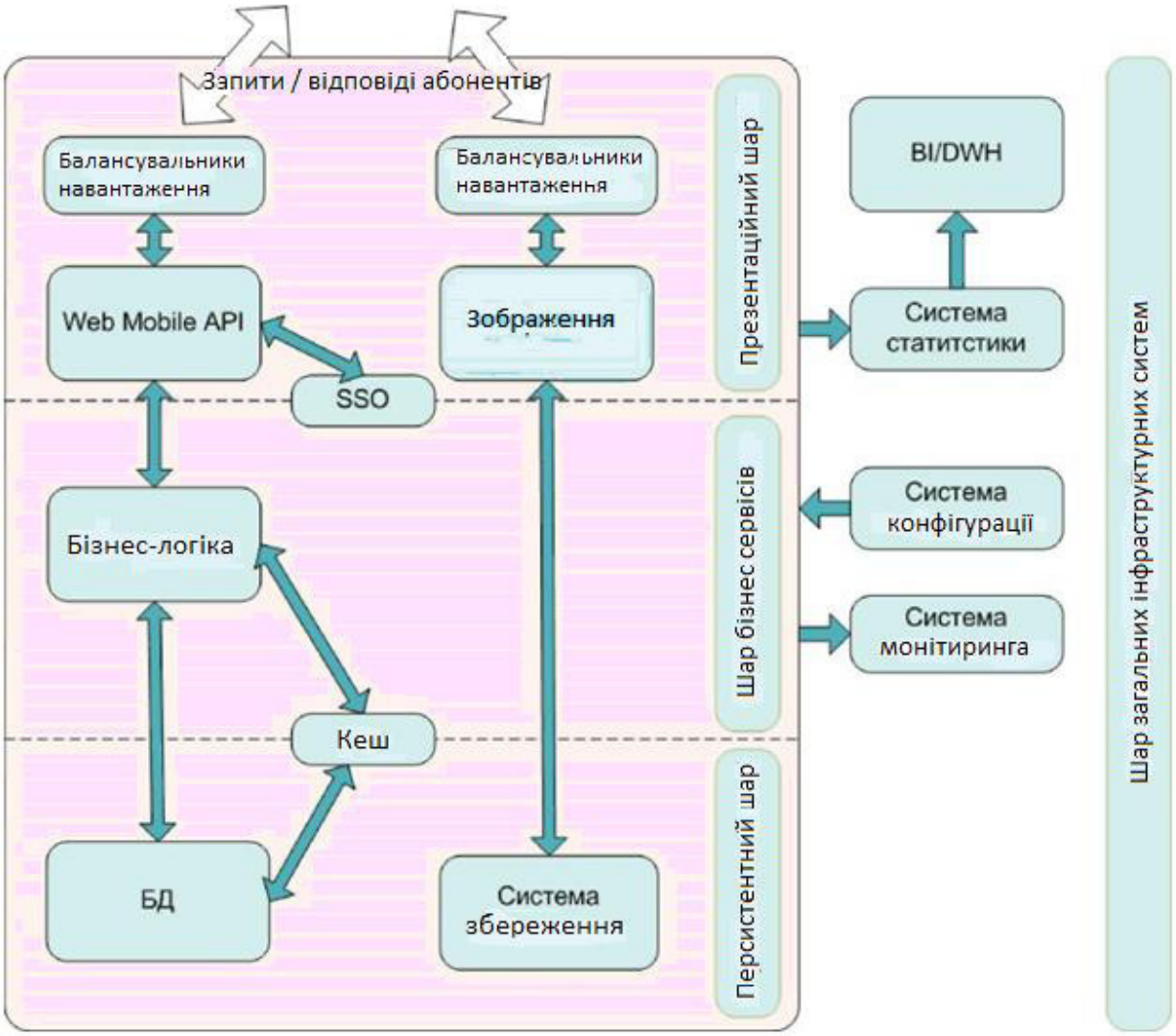


Рисунок 1.4 – Архітектура типового керуючого елемента

SSO (Single Sign-On технологія єдиного входу) – технологія, при використанні якої користувач переходить з одного розділу порталу в інший без повторної аутентифікації.

BI (Business intelligence, бізнес-аналіз, бізнес-аналітика) – методи та інструменти для побудови інформативних звітів про поточну ситуацію в системі.

DWH (Data Warehouse, сховище даних) – предметно-орієнтована інформаційна база даних, спеціально розроблена і призначена для підготовки звітів та бізнес-аналізу.

1.2 Дослідження та виявлення проблем інформаційної безпеки в інформаційно-телекомунікаційних мережах

Розглянемо існуючі проблеми інформаційної безпеки в інформаційно-телекомунікаційних мережах, які актуальні для даного дослідження [4]:

1. Використання глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи. Найбільш вразливими компонентами системи, що часто атакуються, є: сервери; робочі станції; середовище передачі інформації; вузли комутації. Типові інформаційні впливи зловмисників:

- Прослуховування мережевого трафіку. Щоб прослухати трафік (sniffing) мережевий адаптер переводиться в «безладний» режим. У цьому режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даною адресою, як в нормальному режимі функціонування-технології – ARP Spoofing (ARP-poisoning), MAC Flooding і MAC Duplicating [12, 28]. Перехоплення здійснюється з використанням мережевих моніторів, з яких найбільш функціональними є Sniffer Pro від компанії Sniffer Technologies [3], IRIS Network Traffic Analyzer від компанії EYE і TCP Dump [42].

Наслідки. Сучасні мережеві протоколи (TCP / IP, ARP, HTTP, FTP, SMTP, POP3 тощо) не мають механізмів захисту (дані передаються у відкритому вигляді). Зловмисник, що перехоплює трафік між сервером і будь-яким вузлом мережі, може заволодіти аутентифікаційними даними користувача (отримати пароль).

Протидія. Відомо ряд методів визначення наявності запущеного сніфера в мережі, наприклад метод пінга, метод ARP, метод DNS і метод пастки [6, 8, 26].

- Сканування вразливостей. Результатом роботи сканера є інформація про систему, що містить список мережевого обладнання, комп’ютерів з запущеними на них службами, версіями мережевого ПЗ (а отже і вразливостей,

властивих даному ПЗ), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаку. Саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосереднього НСД.

Виявлення. Само по собі сканування не є незаконним. Однак, якщо сканування з боку зовнішньої, по відношенню до системи, мережі звичайне явище, то сканування комп'ютерів з внутрішньої мережі – безумовно, інцидент безпеки, що вимагає негайної реакції з боку мережевого адміністратора. Виявити кроки сканування можна, вивчаючи журнали реєстрації міжмережевих екранів (МЕ). Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти. Тому сучасні МЕ і системи виявлення вторгнень СВВ мають модулі (plug-in) [6], що дозволяють виявити сканування в режимі реального часу. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють здійснювати сканування максимально приховано. Наприклад, в Nmap [12] існують можливості, що дозволяють значно ускладнити виявлення сканування для СВВ.

Протидія. Використання мережевих СВВ, або періодичне вивчення журналів реєстрації МЕ.

- Мережеві атаки. Мережеві атаки можна розділити на: атаки, засновані на переповненні буфера (overflow based attacks). Вони використовують вразливість системи, яка полягає в некоректній програмної обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями; атаки, спрямовані на відмову в обслуговуванні (Denial Of Service attacks). Атаки не обов'язково використовують вразливості в ПЗ системи, що атакується. Порушення працездатності системи відбувається через те, що дані, що їй посилають, призводять до значної витрати ресурсів системи. Найпростішим прикладом атаки цього типу є атака «Ping Of Death» [31, 41]. Суть її в наступному: на комп'ютер жертви надсилається сильно фрагментований ICMP-пакет великого розміру. Реакцією ОС Windows на отримання такого пакету є повне зависання.

- Атаки, засновані на використанні вразливостей в ПЗ мережевих додатків – експлойти (exploit) [20, 33, 42]. Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Експлойти є шкідливими програмами, що реалізують відому вразливість в ОС або прикладному ПЗ, для отримання НСД до вразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій подавлення антивірусних програм і МЕ. Наслідки застосування експлойтів можуть бути самими критичними. У випадку отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути такими: впровадження троянської програми, впровадження набору утиліт для приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких та зовнішніх носіїв інформації, створення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлів з хешами паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи.

Протидія. МЕ і СОВ, встановлені на системі, що атакується, в деяких випадків не в змозі відобразити дію експлойтів [39, 40]. Для успішного відображення атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень заснований на розпізнаванні сигнатур вже відомих атак. Хоча є розробки, здатні за завіреннями розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

- Шкідливі програми. Шкідливі програми – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів або якого іншого впливу, що перешкоджає нормальному функціонуванню мережі. До шкідливих програми відносяться комп'ютерні віруси, троянські коні, мережеві черв'яки тощо [13, 14, 25].

Протидія. Типовим методом протидії є застосування антивірусних засобів, що працюють в режимі реального часу (моніторів). Для виявлення троянських програм існує спеціалізоване програмне забезпечення.

2. Проблема забороненого контенту. Залежно від законодавства країни різні матеріали можуть вважатися нелегальними. У більшості країн заборонені: матеріали сексуального характеру за участю дітей і підлітків, порнографічний контент, описи насильства, в тому числі сексуального, екстремізм і розпалювання расової ненависті. В українському законодавстві кілька законів [18, 19, 21–24] регулюють питання надання інформації про фізичних та юридичних осіб, а саме: Закон України «Про інформацію» від 02.10.92, що регулює відносини щодо одержання і поширення інформації; Закон України «Про захист персональних даних» від 01.06.2010, що визначає захист і обробку персональних даних; Закон України «Про доступ до публічної інформації» від 13.01.2011, який надає право на отримання інформації, що знаходиться у володінні розпорядників.

Аналогічно з концепцією забезпечення комплексного захисту об’єкта інформатизації, можна сформувати повну множину функцій захисту від забороненої інформації. Під функцією захисту (ФЗ) розуміється сукупність однорідних в функціональному відношенні заходів, що регулярно здійснюються в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

Перелік повної множини функцій захисту від забороненої інформації в соціальних мережах:

1. Попередження умов виникнення забороненої інформації. Функція реалізується за допомогою нормативно-правових актів. Вона не може повністю виключити загрозу поширення забороненої інформації в соціальних мережах, так як в цілому ситуація з дотриманням законів незадовільна, а в інтернет-просторі загострюється через технічні складнощі.

2. Попередження безпосередньої прояви забороненої інформації. Функція реалізується за рахунок механізмів прогнозування поширення забороненої інформації в соціальній мережі.

3. Виявлення забороненої інформації, яка проявилася. Функція пов'язана з моніторингом ІТКМ на предмет забороненої інформації на сторінках абонентів. Як правило, для реалізації даного захисту використовується різні СОРМ (система оперативно-розшукових заходів). Дана ФЗ пов'язана з проблемами контекстного пошуку, а також необхідністю контролю над всією системою.

4. Попередження впливу на абонентів забороненої інформації, яка проявилася. Функція може бути реалізована за допомогою автоматичного пересилання повідомлення з попередженням про відповідальність за розповсюдження забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до керування системи та нелегітимними – при його відсутності (зламання акаунта). ФЗ ділиться на дві функції ($ФЗ_{4а}$ і $ФЗ_{4б}$). Перша пов'язана з попередженням абонентів, на сторінках яких була знайдена заборонена інформація, а друга – з розсилкою попереджень потенційним одержувачам забороненої інформації.

5. Виявлення впливу забороненої інформації на абонентів. Функція пов'язана безпосередньо з фіксацією процесу поширення забороненої інформації, може бути реалізована через контекстний аналіз повідомлень. Властиві такі ж недоліки, як і для $ФЗ_3$.

6. Локалізація, обмеження впливу забороненої інформації на абонентів. Функція реалізується через блокування абонентів, що поширюють заборонену інформацію ($ФЗ_{6а}$), або абонентів – потенційних розповсюджувачів ($ФЗ_{6б}$). Дана ФЗ спирається на попередні функції і для її ефективної реалізації необхідний контроль над системою.

7. Ліквідація наслідків виявленого впливу забороненої інформації на абонентів. Функція пов’язана з видаленням забороненої інформації з системи. Для реалізації даної функції також необхідний контроль над системою.

На рисунку 1.5 наведені всі поєднання подій, які потенційно можливі при здійсненні всіх ФЗ.

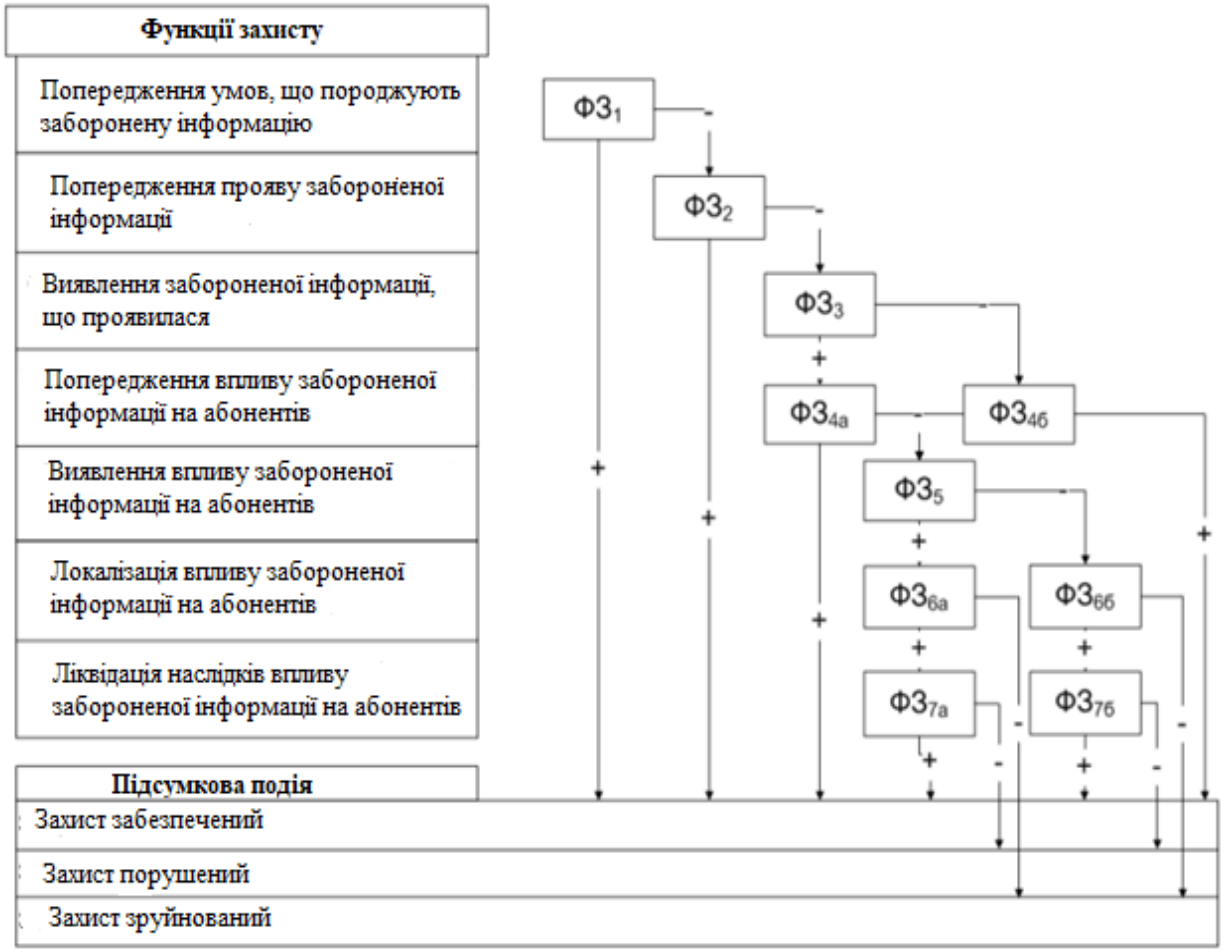


Рисунок 1.5 – Функції захисту від забороненої інформації в ІТКМ

Проаналізувавши функції захисту можна дійти висновку, що найбільш ефективні функції – це перші функції, оскільки вони забезпечують захист на початкових етапах. Наведені функції захисту мають свої недоліки. Найбільш перспективною ФЗ інженерно-технічного напряму є $ФЗ_2$. На даному етапі, маючи інформацію про топології ІТКМ і потенційних розповсюджувачів забороненої інформації, можливе прогнозування процесу її поширення.

Створення моделей та алгоритмів поширення загрози забороненої інформації – одна з ключових задач в даному напрямку. При її вирішенні

виникають проблеми, пов’язані з властивостями розглянутої інформаційно-телекомунікаційної системи, а саме [5]:

1. Відсутність перевірки достовірності даних про вузол системи. Дуже часто абоненти інформаційно-телекомунікаційних мереж (ІТКМ) вказують недостовірну інформацію про себе.

2. Закритість системи. Структура та інформація про управління системою є конфіденційною інформацією.

3. Проблема збору інформації. Неможливо отримати повну інформацію про топологію ІТКМ. Існує можливість для звичайного абонента збору інформації про структуру мережі (функції API), але ця можливість має багато обмежень (налаштування приватності, часовий інтервал).

Нас цікавить тільки обмін повідомленнями між абонентами, тому концептуальна математична модель інформаційної взаємодії представляється графом, вузлами якого є абоненти, а ребрами – зв’язки між ними. Перерахуємо властивості графа, принципові для справжнього дослідження:

1. Велика розмірність. Система містить мільйони елементів.

2. Гетерогенність. У графі, який відображає взаємозв'язок елементів в системі, вершини мають різну кількість прилеглих ребер.

3. Динаміка зв’язків. В системі протягом часу відбуваються зміни зв’язків.

4. Динаміка вузлів. Протягом часу змінюється кількість вузлів (елементів) системи.

5. Наявність груп вузлів, що мають велику кількість зв’язків всередині і невелику – між групами.

Граф, який представляє систему, володіє певною кластеризацією. Для таких систем характерно, що два вузли, які мають зв’язки до якого-небудь вузла, часто також мають зв’язок між собою.

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу. Таким

чином, ми приходимо до задачі моделювання ІТКМ за допомогою їх математичної моделі (графів).

1.3 Моделювання інформаційної взаємодії поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Моделювання є одним із основних способів вивчення інформаційно-телекомунікаційних мереж. Його прийнято розглядати в двох аспектах:

1. Моделювання топології інформаційно-телекомунікаційної мережі (структури інформаційних зв'язків між вузлами мережі)
2. Моделювання проблеми вивчення процесів інформаційної взаємодії в ІТКМ (загрози поширення забороненої інформації (ЗПЗІ)).

ІТКМ з точки зору топології відносять до складних мереж [34, 45]. Складні мережі (комплексні мережі, complex networks) – це існуючі в природі мережі, що володіють нетривіальними топологічними властивостями.

На рисунку 1.6 наведено класифікацію топологічних моделей мереж [29], яку здійснив Jasmin Leveille у [43]. В овалах вказані класи мереж, а в прямокутниках конкретні моделі-представники. Описуються їх характеристики: розподіл ступенів зв'язності вузлів мережі, кластерний коефіцієнт і середня довжина шляху мережі.

Тема випадкових графів (мереж) розкрита в роботах: Bela Bollobas [32], Erdos і Renyi [35]. В [36] описуються основні моделі мереж і їх основні характеристики. Проводиться дослідження топології популярних ІТКМ і здійснюється пошук найбільш адекватної топологічної моделі. Представлений огляд канонічних робіт [29, 32, 34–36, 39, 40, 43, 45] за даною тематики.

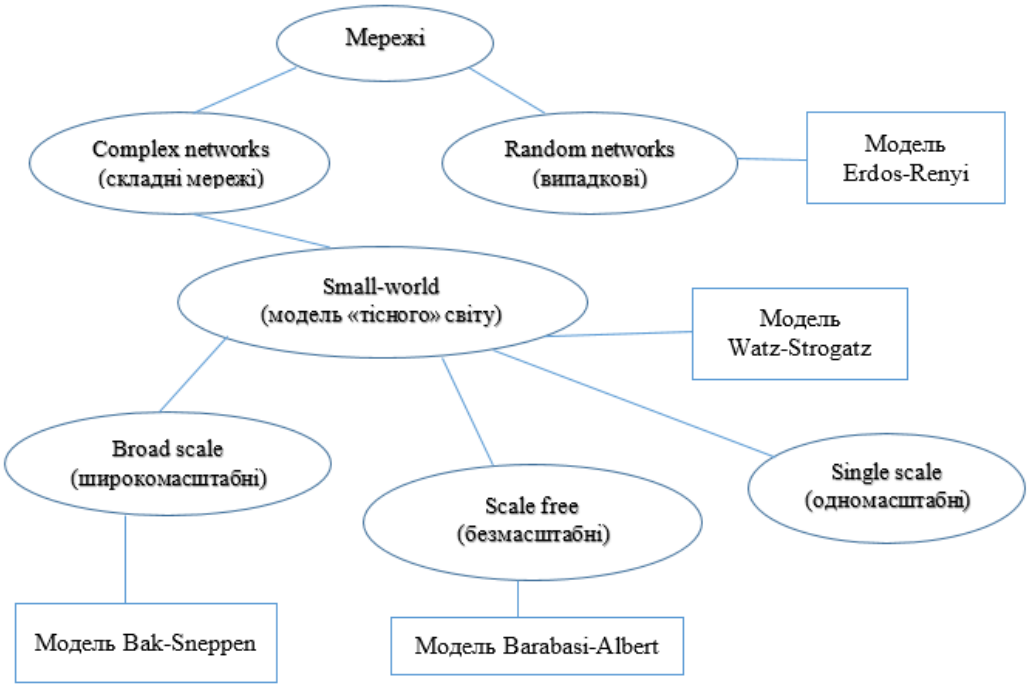


Рисунок 1.6 – Класифікація мереж

Виділено наступні головні сучасні тенденції в області аналізу топології ІТКМ:

1) вивчення топологічних характеристик ІТКМ;

2) дослідження еволюції ІТКМ;

3) вивчення і розробка методів для обчислення характеристик великомасштабних ІТКМ, рішення проблеми отримання репрезентативної вибірки з ІТКМ.

У [38, 48] розглянуті ІТКМ з точки зору маркетингових стратегій на їх основі. ІТКМ часто відносять до scale-free (SF) мереж. Перші роботи належать Barabasi і Albert та присвячені однойменій моделі. Порівнюють існуючі моделі і свою модель, детально її описують і приводять її сильні і слабкі сторони.

Dorogovtsev і Mendes у [34] узагальнюють модель Barabasi-Albert і знаходять її рішення. Тобто знаходять розподіл зв'язності вузлів і деякі інші пов'язані з ним параметри мережі, доводять, що виникаюча масштабованість дійсна не тільки для даної моделі, а і для широкого класу зростаючих мереж. Dorogovtsev і Mendes приводять отримані універсальні відношення масштабування, що описують властивості scale-free мереж, що розвиваються, scale-free мереж і вказують межі їх дії. Наведено доказ того, що основні

властивості SF мереж, що розвиваються, можуть бути описані в рамках аналітичної моделі, розглядають властивості перколяційного кластера.

Вчені Romualdo Pastor-Satorras and Alessandro Vespignani розглядали не тільки топологію ІТКМ як SF мережу, але аналізували процес поширення епідемії на таких мережах [38, 44, 46-48]. Вони отримали дані по комп'ютерним вірусам і виявляли такі їх параметри, як середня «тривалість життя» вірусу і стійкість до знищення, а також описали динамічну модель поширення інфекції в мережах, привели метод визначення наявності епідемічного порогу в мережі.

Ще однією точкою зору на тип топології ІТКМ є позиція таких дослідників як S.H. Strogatz, M.E.J. Newman, D.J. Watts і ряду інших вчених. Вони вважають, що ІТКМ топологічно є класом small-world мереж [43–48].

У [45] розглядається модель Watts-Strogatz, яка відноситься до класу small-world мереж, та імітує структуру ІТКС. Розглянута проблема перколяції вузлів на small-world мережах. Цей підхід дозволяє розглядати просту модель поширення захворювань (SIS) і отримати апроксимований вираз для порога перколяції. Всі аналітичні результати підтверджуються чисельними рішеннями моделі.

Small-world мережі розглядаються в багатьох роботах не тільки з точки зору топології мережі [45], а й як основа для епідеміологічних моделей [50].

Вид складних мереж, як Broad Scale мережі, де аналізується модель Bak-Sneppen, є найменш привабливий при моделюванні топології ІТКМ.

Аналіз наукових праць, в яких розглядаються різні підходи до моделювання топології ІТКМ, показує, що при вирішенні даної задачі, зазвичай, використовуються small-world і scale free мережі.

При розгляді питань, що стосуються моделювання процесів, що відбуваються в ІТКМ, основним підходом є застосування моделей впливу, інформаційного управління та протиборства [39]. У даній роботі розглядаються моделі впливу, так як вони найбільш адаптивні до розв'язуваних задач. На рисунку 1.7 зображена узагальнена класифікація

моделей впливу. Коротко охарактеризуємо представлені класи моделей впливу.

Порогової моделлю є будь-яка модель, в якій є порогове значення або набір порогових значень, використовуваних при зміні станів. Класичні моделі з порогами були розроблені Schelling, Axelrod і Granovetter для моделювання колективної поведінки [45].

Моделі незалежних каскадів (Independent Cascade Model) належать до категорії моделей так званих «систем взаємодіючих частинок» (Interacting Particle Systems). Вузол мережі (агент) визначається аналогічно до вищеописаної моделі. Коли агент i стає активним у деякий момент часу, він отримує шанс на перехід наступному (і тільки на наступному) кроці кожного зі своїх сусідів j з імовірністю p_{ji} (причому j можуть намагатися незалежно активувати і інші агенти) [45].

Моделі просочування і зараження є популярним способом вивчення поширення інформації та інновацій в соціальних системах.

Модель Ізінга – математична модель, що описує виникнення намагнічування матеріалу. Конформність або незалежність у великій соціальній групі може моделюватися за допомогою моделі Ізінга; вплив найближчих сусідів є визначальним, а аналогом температури є готовність групи мислити творчо, готовність прийняти нові ідеї. Зовнішнім полем для соціальної групи є вплив «авторитета» або керування. Більш складні моделі, які описують ІТКМ на термодинамічних аналогіях, розглядалися в [31].

Для опису процесів поширення інформації в ІТКМ останню можна розглядати як складну адаптивну систему, що складається з великої кількості агентів, взаємодія між якими призводить до масштабної, колективної поведінки, яку важко передбачити і аналізувати.

Рисунок 1.7– Класифікація моделей впливу

Для моделювання та аналізу таких складних систем іноді використовуються клітинні автомати. Клітинний автомат складається з набору об’єктів (в даному випадку агентів), що зазвичай утворюють регулярну решітку. Стан окремо взятого агента в кожен дискретний момент часу характеризується деякою змінною. Стани синхронно змінюються через дискретні інтервали часу відповідно до незмінними локальними ймовірнісними правилами, які можуть залежати від станів найближчих сусідніх агентів в околі даного агента, а також, можливо, від стану самого агента.

За допомогою моделі ланцюгів Маркова вивчається вплив в команді (групі агентів). Запропонована модель є динамічною Байєсовою мережею (Dynamic Bayesian Network – DBN) з дворівневою структурою: рівнем індивідів (моделюються дії кожного агента) і рівнем групи (моделюються дії групи в цілому).

Моделі взаємної інформованості [39]. Є агент, що входить в деяку соціальну мережу. Агент поінформований про поточну ситуаційну обстановку (діях і уявленнях інших агентів, параметрах середовища – так званому стані природи (state of nature) тощо). Ситуаційна обстановка впливає на наявний у агента набір цінностей, установок та уявлень, пов'язаних наступним чином: цінності впливають на установки, а ті, в свою чергу, призводять до схильності до уявлення того чи іншого рівня, до схильностей узгоджена знаходиться «в пам'яті» агента ієрархічна система уявлень про світ. Таким чином схильність до тих чи інших уявлень і ситуаційна обстановка (наприклад, дії інших агентів) призводять до формування нових або модифікації старих уявлень. Відповідно до цих уявлень і встановленої мети агент приймає рішення і виконує дію. Результати дій призводять до зміни як самої ситуаційної обстановки, так і внутрішніх цінностей, установок і уявлень.

Моделі узгоджених колективних дій. Ключове значення у цих моделях мають соціальні зв'язки. З одного боку, соціальні зв'язки можуть забезпечити ефективний локальний соціальний контроль для стимулювання участі в колективній дії (в силу тиску з боку своїх сусідів, довіри до них, соціального схвалення, необхідності збереження позитивних відносин і відповідності очікуванням, емоційної прихильності, збереження своєї репутації, ототожнення себе з сусідами тощо). Так, наприклад, поведінка сусідів агента вплине на його власну поведінку. З іншого боку, соціальні зв'язки забезпечують агента інформацією про наміри і дії інших агентів в мережі і формують його (неповні) уявлення, на основі яких агент приймає свої рішення. При цьому, в межах соціальних зв'язків агенти можуть прикладати спільні зусилля по створенню локального суспільного блага і спільно користуватися

ним. Тому структура ІТКМ створює сильний вплив на рішення агентів про прийняття участі в колективній дії.

У [49] ІТКМ розглядається як комунікаційна, за допомогою якої агенти повідомляють один одному про свою готовність взяти участь в коллективній дії. Кожен агент поінформований про готовність тільки своїх найближчих сусідів і на основі цього локального знання приймає рішення про участь, використовуючи правило прийняття рішень «я візьму участь, якщо береш участь ти» (механізм координації). А саме розглядається координаційна гра з неповною інформованістю. Комунікаційна мережа сприяє координації, і основний інтерес становить те, які властивості таких мереж, які допускають колективну дію. Розглядаються мінімально достатні мережі, які вибудовують агентів в ієрархію соціальних ролей / ступенів: «провідні» (initial adopters), «послідовники» (followers) і т.д. до «пізніших послідовників» (late adopters). Такі мережі сприяють координації наступним чином:

1) інформуючи кожну ступінь про більш ранні ступені;
2) формуючи загальне знання в межах кожного ступеня.

Тобто забезпечується розуміння ролі (локально) загального знання в колективну дію і співвідношення між структурою соціальної мережі і загальним знанням.

Рівновага стабільної мережі (stable network equilibrium) [45] – ситуація, в якій не існує агента, для якого будь-яка комбінація зміни його дії і зміни його зв’язків приведе до кращого результату. Тільки рівноваги з повною участю або повною неучастю є рівновагою стабільної мережі.

У [45] розглядаються моделі поширення інфекційних захворювань серед населення, проводиться їх математичний аналіз і застосування до конкретних захворювань. Розглядається класична епідеміологічна SIR модель Кермак-Маккендріка, MSEIR та SEIR ендемічні моделі.

Також існують епідеміологічні моделі поширення вірусів і боротьби з ними. Представлена нова модель, яка може бути використана для прогнозування процесу поширення шкідливих програм і оцінки ефективності

протидії їм. Показано, як застосовується модель для аналізу динаміки системи, інфекційних спалахів та інших процесів, пов’язаних з поширенням вірусів.

Вчені Kephart і White проводять аналогію між біологічними і комп’ютерними вірусами та розглядають адаптацію методів математичної епідеміології до вивчення комп’ютерних вірусів. Розглядаються стандартні епідеміологічні моделі на орієнтованому графі, використовується моделювання для вивчення поширення вірусів. Велика увага приділяється вивченню критичного порогу епідемії.

Вчені Pastor-Satorras і Vespignani в [48] представляють аналіз динаміки розвитку епідемії в складних гетерогенних мережах, приводять аналітичні та чисельні результати. Вченими розглядається вплив початкових умов і актуальність статистичних результатів дослідження, що стосується гетерогенних мереж. Автори вважають, що представлені теоретичні відомості становлять великий інтерес і можуть дати корисну інформацію для розробки стратегій, спрямованих на адаптивне стримування епідемії.

Вчені Leskovec, Adamic і Huberman розглядають вірусний маркетинг в ІТКМ. Вірусний маркетинг – загальна назва різних методів поширення реклами, що характеризуються поширенням в прогресії близькою до геометричної, де головним розповсюджувачем інформації є самі одержувачі інформації. Здійснюється даний підхід шляхом формування змісту повідомлення, таким чином, який здатний залучити нових одержувачів інформації за рахунок яскравої, творчої, незвичайної ідеї. Також ефективність повідомлення ґрунтується на використанні природних довірчих стосунків між одержувачем і відправником.

У межах вирішуваних задач для нас найбільш підходять оптимізаційні та імітаційні моделі. З них розглянемо моделі просочування і зараження (клас епідеміологічних моделей), так як дані моделі найбільш точно відображають специфіку розглянутих нами проблем. Даний клас моделей є дуже поширеним при дослідженнях процесів взаємодії в ІТКМ.

1.4 Постановка задачі

Після проведення аналізу предметної області в рамках даної роботи були поставлені такі завдання дослідження:

1. Створити імітаційну модель поширення загрози забороненої інформації в ІТКМ.

- розробити алгоритм загрози поширення забороненої інформації в ІТКМ;
- на основі розробленого алгоритму створити імітаційну модель загрози поширення забороненої інформації в ІТКМ;
- провести експериментальне дослідження імітаційної моделі загрози поширення забороненої інформації в ІТКМ.

2. Створити аналітичну модель поширення загрози забороненої інформації в ІТКМ.

- на основі експериментальних даних за імітаційною моделлю створити аналітичну модель загрози поширення забороненої інформації в ІТКМ;
- провести експериментальне дослідження аналітичної моделі, перевірити адекватність моделі.

3. Розробити методику формування топології ІТКМ

- алгоритму формування графа доступної частини мережі;
- алгоритму формування повного графа.

4. Змоделювати процес поширення загрози забороненої інформації на реальній великомасштабній ІТКМ.

- розробити методику формування топології великомасштабної ІТКМ;
- реалізувати методику у вигляді ПЗ;
- розробити ПЗ під розподілену обчислювальну систему для моделювання загрози поширення забороненої інформації на топології великомасштабної ІТКМ;
- провести експериментальне дослідження імітаційної моделі загрози поширення забороненої інформації на топології великомасштабної ІТКМ з використанням розробленого ПЗ;
- провести експериментальне дослідження з отриманими результатами.

2 МАТЕМАТИЧНІ МОДЕЛІ БЕЗПЕКИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

2.1 Алгоритм реалізації загроз поширення забороненої інформації на основі процесів, які протікають в реальних ІТКМ.

За результатами проведеного дослідження предметної області вставлено необхідність розробки імітаційної і аналітичної моделей поширення загрози забороненої інформації в ІТКМ. Імітаційна модель необхідна для отримання експериментальних результатів для синтезування аналітичної моделі. Необхідність створення аналітичної моделі обґрунтовується тим, що для імітаційного моделювання на топології існуючих ІТКМ (десятки мільйонів вузлів) необхідні великі витрати часу. Не враховуючи час на збір інформації про топології мережі, який може становити близько тижня, безпосередньо моделювання загрози поширення забороненої інформації (ЗПЗІ) займає кілька годин навіть при використанні розподілених обчислювальних ресурсів. Аналітична модель може дати прогноз загрозі поширення забороненої інформації майже миттєво. З її допомогою можна отримати актуальні дані (до того моменту, коли кількість атакуючих абонентів буде максимальною) за динамікою ЗПЗІ.

Процес ЗПЗІ характеризується наступними особливостями [4, 5]. У мережі існують вузли трьох типів. Перший тип – атакуючі вузли, це вузли, які розповсюджують заборонену інформацію. Другий тип – захищені вузли, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися. Третій тип – потенційно вразливі. Вузли такого типу не беруть участі в процесі поширення загрози, але можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію.

Постановка задачі

Дано:

N – кількість вузлів, яка дорівнює кількості абонентів мережі,

I_0 – кількість абонентів-зловмисників – початкових джерел загрози,

R_0 – кількість абонентів спочатку несприйнятливих до атакуючих дій,

β – параметр, що відображає силу загрози, ймовірність здійснення атаки,

γ – параметр, що відображає ступінь протидії загрозі, ймовірність захисту абонента (β і γ в даному дослідженні визначено як константи, але можуть бути виражені як функції, що залежать від психосемантичних профілів абонентів ІТКМ),

φ – коефіцієнт топологічної вразливості мережі, що відображає внутрішню властивість ІТКМ, засновану на характеристиках її топології, яке сприяє поширенню забороненої інформації,

t – час процесу (в умовних одиницях часу).

Потрібно розробити аналітичну модель динаміки атаки $I(t)$ та захисту вузлів $R(t)$

$$\begin{cases} I(t) = f(N, \beta, \gamma, \varphi. t) \\ R(t) = g(N, \beta, \gamma, \varphi. t) \end{cases} \quad (2.1)$$

Розробка аналітичної моделі включає в себе послідовність наступних дій:

1) формування імітаційної моделі для дослідження характеру і параметрів процесу ЗПЗІ;

2) синтез аналітичних залежностей параметрів процесу;

3) проведення експериментів з метою перевірки точності (адекватності) моделі.

Наведемо алгоритм реалізації ЗПЗІ, ґрунтуючись на описі процесів, що відбуваються в реальних ІТКМ. Схема реалізації загрози поширення забороненої інформаці в ІТКМ зображена на рисунку 2.1.

Алгоритм 1 – Загрози поширення забороненої інформації в ІТКМ

1. Поширення забороненої інформації (ЗІ) (далі процес «атаки») ініціює будь-який абонент-зловмисник (на рисунку 2.1 – вузол 1), поширюючи повідомлення з ЗІ (реалізує загрозу) за його списком контактів. Атаку може починати один зловмисник або група.

2. Абоненти-одержувачі (вузли 2, 3, 4), прийнявши повідомлення з ЗІ, читають його і включаються в процес атаки, поширюючи її далі по своєму списку контактів (вузол 3), або ігнорують або взагалі видаляють повідомлення (вузол 2), тобто в атаці не беруть участь. Процес атаки зазвичай йде лавиноподібно. Атакуючі абоненти не закінчують атаку, одного разу передавши повідомлення із забороненою інформацією. Вікно атаки, як правило, триває протягом досить значного проміжку часу і залежить від типу подачі ЗІ в повідомленні, зацікавленості абонента тощо.

3. Абоненти можуть перестати сприймати і, відповідно, поширювати ЗІ (вузол 5) (далі процес «захисту»), внаслідок впливу механізмів захисту (наприклад, попередження про неї), тому повідомлення з ЗІ від атакуючих абонентів будуть постійно відхилятися.

4. Процес триває поки в мережі є абоненти-зловмисники, або є потенційно вразливі вузли, якщо відсутній процес захисту.

Таким чином, ЗПЗІ в ІТКМ є складним динамічним процесом, що складається з двох протидіючих підпроцесів атаки і захисту вузлів мережі.

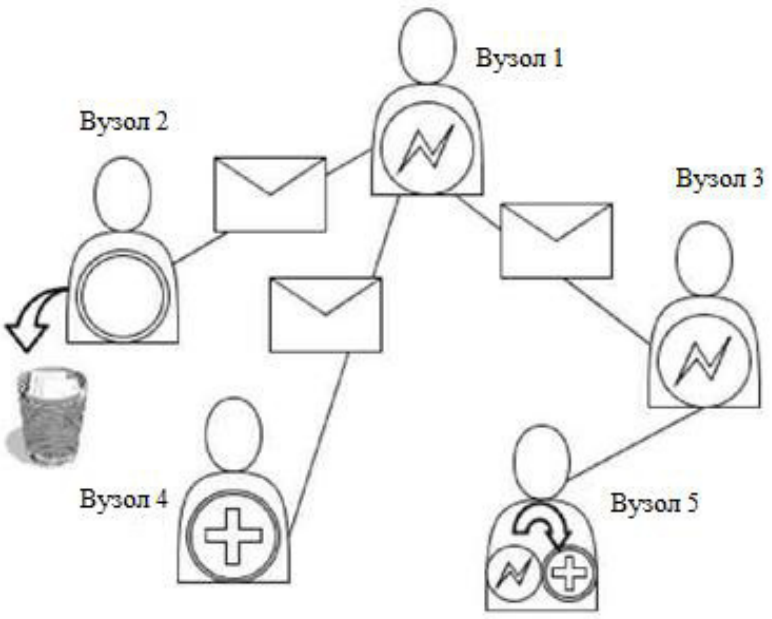


Рисунок 2.1 – Схема реалізації загрози поширення забороненої інформаці в ІТКМ

На основі описаного алгоритму була побудована імітаційна модель ЗПЗІ в ІТКМ, яка складається з розробленої програми ModelGraph і даних, які можуть бути згенеровані за допомогою ПЗ Pajek [2].

Імітаційна модель ЗПЗІ:

Вхідні дані: N, k – середній ступінь зв'язності вузлів, a – параметр, що відображає середню довжину шляху і рівень мережевої кластеризації, β, γ (в моделі вважається, що β та γ однакові для кожного абонента), I_0 – кількість абонентів-зловмисників – початкових джерел загроз, R_0 – кількість абонентів спочатку несприйнятливих до атакуючих дій.

Вихідні дані: $I(t)$, $R(t)$, $S(t)$ – чисельні масиви даних, що описують динамічний процес реалізації ЗПЗІ (кількості атакуючих, захищених і потенційно вразливих вузлів у кожну умовну одиницю часу відповідно).

1. Створення топології ІТКМ – графа $G_{SW} =< V, E >$, де G_{SW} – граф small-world мережі (на основі моделі Watts-Strogatz), $V = \{v_i\}$ – множина вершин, $E = \{e_{ij}\}$ – множина ребер, $i = \overline{1,N}$, $j = \overline{1,N}$. Даний крок здійснюється з використанням вільно розповсюджуваної програми Pajek,

адаптованої під цю задачу, за рахунок заданих топологічних параметрів N, k, a.

2. Сформувати множину $V = \{V^I, V^S, V^R\}$, де $V^I = \{v_i^I\}$ – множина атакуючих вузлів ($|V^I| = I_0$), $V^R = \{v_i^R\}$ – множина захищених вузлів ($|V^R| = R_0$), $V^S = \{v_i^S\}$ – множина потенційно вразливих вузлів ($|V^S| = N - I_0 - R_0$).

3. $\forall v_i^I$, якщо $\exists e_{ij}$ та $v_j \in V^S$ $j = \overline{1,N}$, то з ймовірністю β виконати: $V^S \backslash v_j$ та $V^I \cup v_j$; з ймовірністю γ виконати: $V^I \backslash v_i$, $V^R \cup v_i$.

4. Якщо $V^I = \emptyset$ або $\gamma = 0$ та $V^S = \emptyset$ y = 0, то кінець алгоритму, інакше перейти до п. 3.

ModelGraph – програма для імітаційного моделювання ЗПЗІ в ІТКМ. Даний програмний продукт є однопотоковим додатком. Програма складається з виконуваного файлу ModelGraph.exe і бібліотеки chartdir50.dll для побудови графіків. Після вибору типу мережі і введення її параметрів відбувається імітаційне моделювання за алгоритмом 1. Потім результати відправляються в функцію побудови графіків для виведення результатів в графічному вигляді. Програма написана в середовищі розробки Microsoft Visual Studio .NET 2017. Вихідними даними для гетерогенної мережі є файл формату .net, визначений у програмі Pajek.

ПЗ Pajek є програмою, для ОС MS Windows, призначеною для аналізу і візуалізації великих мереж. Дана програма знаходиться у вільному доступі і призначена для некомерційного використання. Pajek розроблений Vladimir Batagelj і Andrej Mrvar.

Проаналізуємо підпроцес атаки без захисту, провівши ряд експериментів (експеримент 1-3) з використанням імітаційної моделі (φ – коефіцієнт топологічної уразливості мережі).

1) Експеримент 1. Вплив сили атаки на процес.

Експерименти проводилися при наступних значеннях параметрів: N=1000, $\varphi = 20$, $I_0 = 1$, $\beta = 0{,}1..0{,}5$ (рисунок 2.2).

2) Експеримент 2. Вплив значення середнього ступеня зв’язності вузлів у мережі на процес.

Експерименти проводилися при наступних значеннях параметрів: N=1000, $\varphi = 0{,}5..60$, $I_0 = 1$, $\beta = 0{,}5$ (рисунок 2.3).

3) Експеримент 3. Вплив кількості спочатку атакуючих вузлів на процес.

Експерименти проводилися при наступних значеннях параметрів: $N = 1000$, $\varphi = 20$, $I_0 = 1..40$, $\beta = 0{,}5$ (рисунок 2.4).

Кожен з трьох типів експериментів проводився 100 разів, бралися усереднені значення.

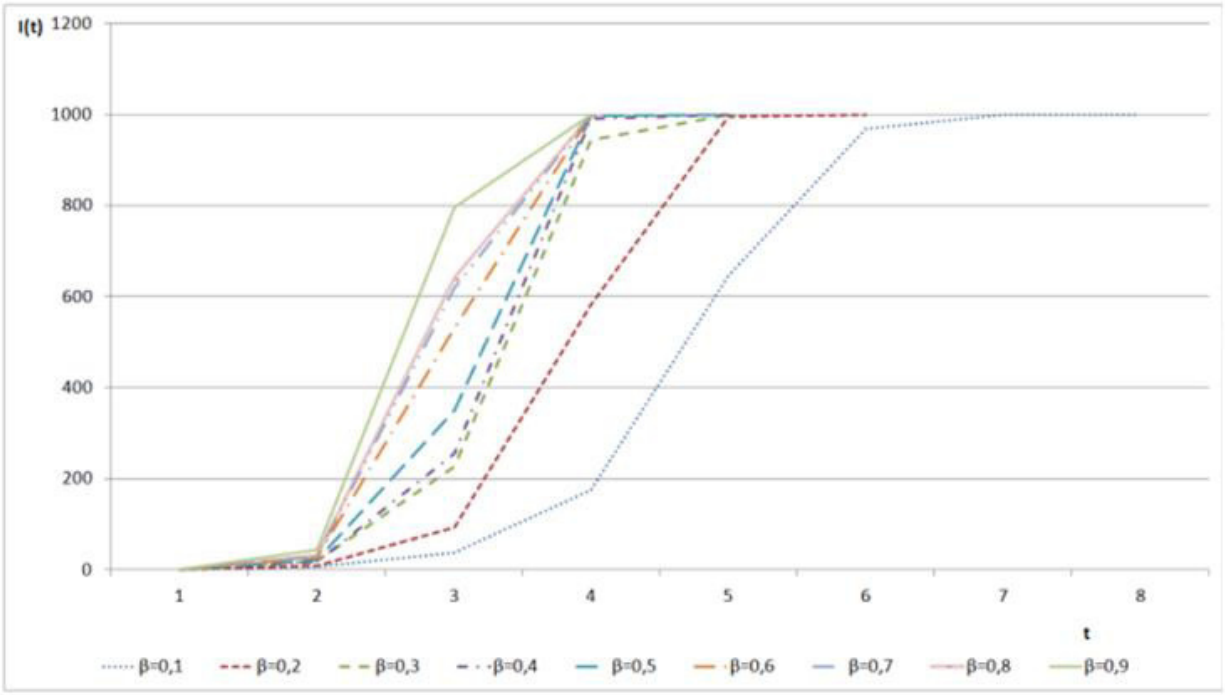


Рисунок 2.2 – Вплив β на процес атаки

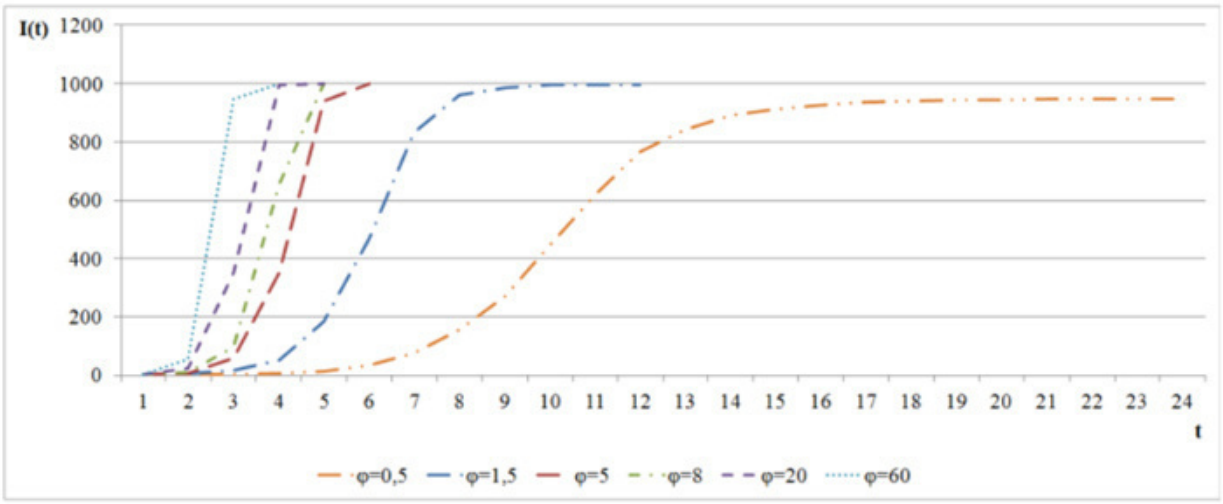


Рисунок 2.3 – Вплив φ на процес атаки

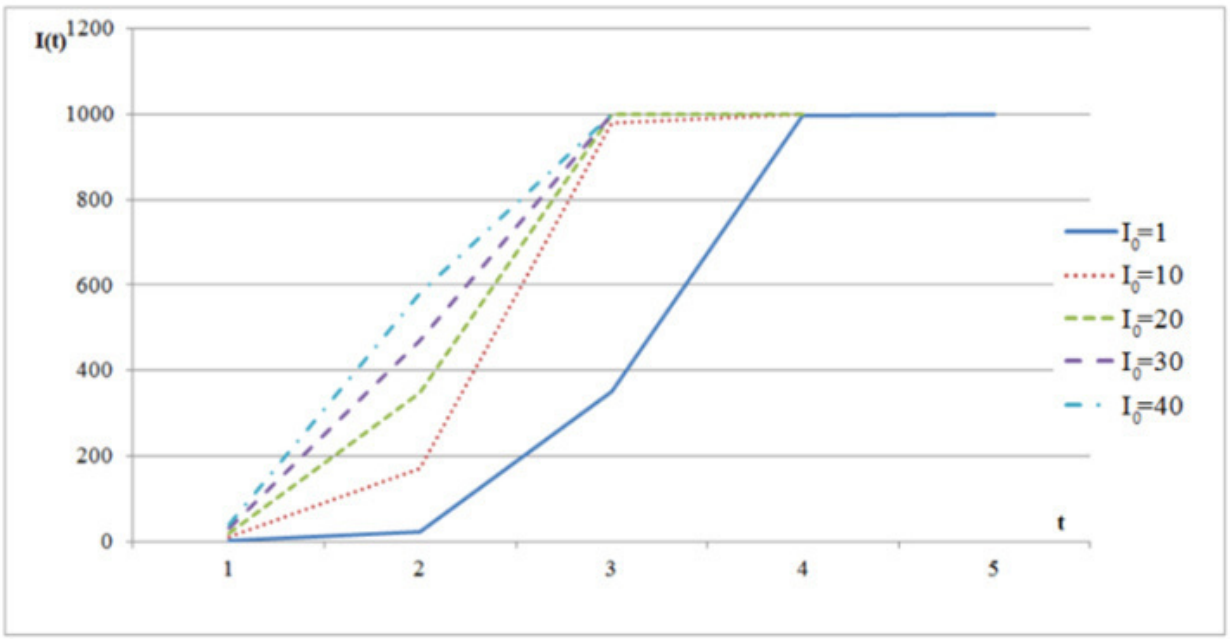


Рисунок 2.4 – Вплив I_0 на процес атаки

За результатами експериментів 1-3 можна зробити наступні висновки:

- процес атаки $I(t)$ має експоненціальну залежність (експеримент 1, 2, 3);

- при збільшенні значень φ, I_0, β зростає динаміка зараження вузлів (інтенсивність атаки) (експеримент 1,2,3);

- при зростанні ймовірності проведення атаки β від 0,1 до 0,9, час процесу знижується в два рази (з 8 до 4 умовних одиниць часу) (експеримент 1);

- коефіцієнт топологічної вразливості φ має найбільший вплив (в

порівнянні з I_0, β) на тривалість процесу. Наприклад, при $\varphi = 0{,}5$ (низька вразливість) атака триває 24 умовні одиниці часу, а при $\varphi = 60$ всього лише 4 (експеримент 2);

- велика кількість спочатку атакуючих вузлів I_0 знижує час, за який відбувається зараження всіх вузлів в мережі. Наприклад, при $I_0 = 40$ тривалість процесу становить 3 умовні одиниці часу (експеримент 3).

Ускладнимо умови експериментів, додавши підпроцес захисту, який залежить від початкової кількості захищених вузлів R_0 і ймовірності захисту γ.

4) Експеримент 4. Вплив ймовірності захисту.

Експерименти проводилися при наступних значеннях параметрів: $N = 1000$, $\varphi = 20$, $I_0 = 1$, $\beta = 0{,}5$, $\gamma = 0{,}1..0{,}9$, $R_0 = 0$ (рисунок 2.5).

5) Експеримент 5. Вплив початкового кількості захищених вузлів

Експерименти проводилися при наступних значеннях параметрів:

$N = 1000$, $\varphi = 20$, $I_0 = 1$, $\beta = 0{,}5$, $\gamma = 0{,}5$, $R_0 = 0..200$ (рисунок 2.6).

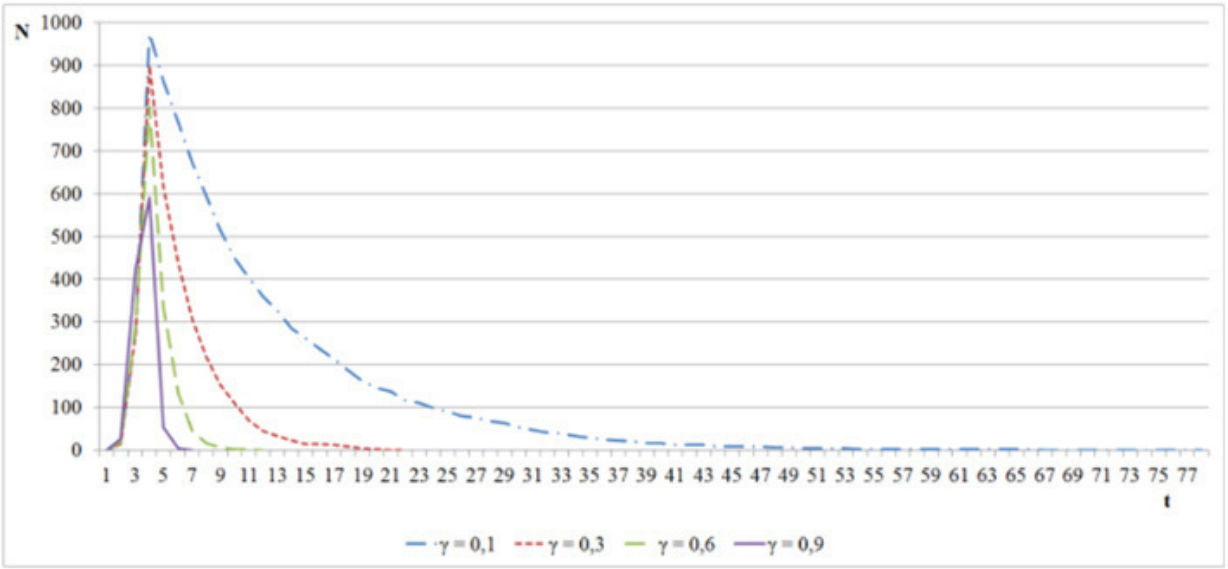


Рисунок 2.5 – Вплив γ на процес атаки

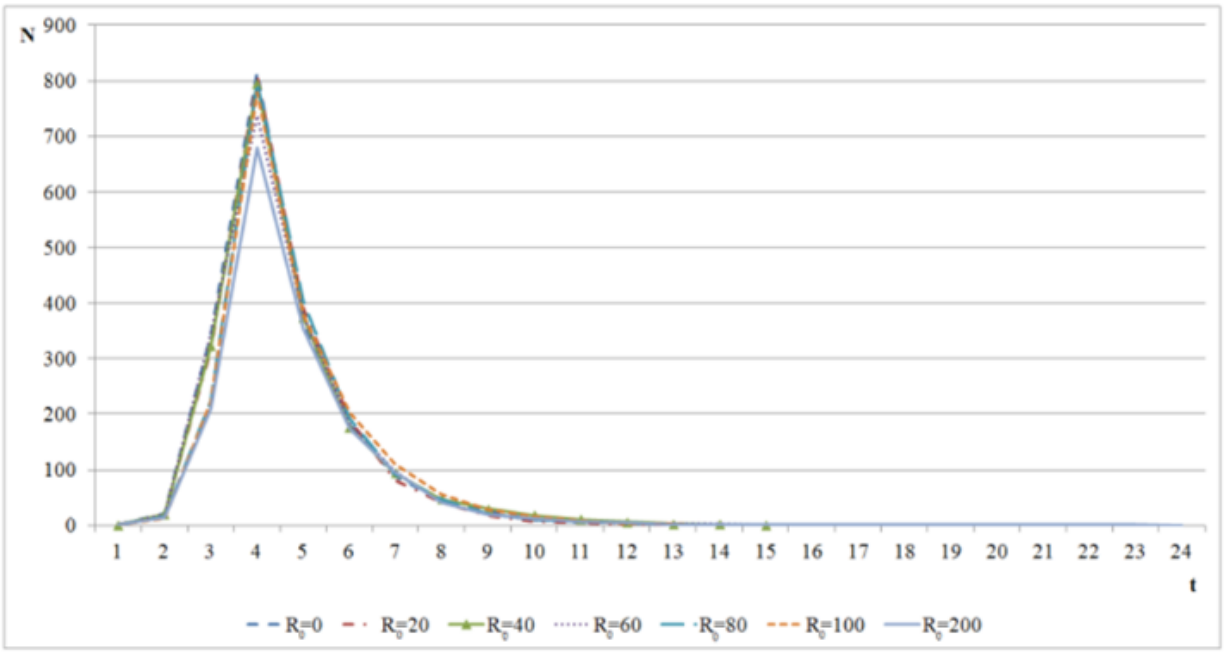


Рисунок 2.6 – Вплив R_0 на процес атаки

За результатами експериментів 4 і 5 можна зробити наступні висновки:

- введення підпроцеса захисту збільшує час всього процесу ЗПЗІ (експеримент 4, 5);
- при невеликих значеннях ймовірності захисту ($\gamma < 0{,}3$) загроза реалізується практично на всіх вузлах в мережі (експеримент 4);
- при невеликих значеннях ймовірності захисту ($\gamma < 0{,}3$) час процесу становить понад 50 умовних одиниць часу (експеримент 4);
- при великій ймовірність захисту (≈0,9) процес триває ≈7 умовних одиниць часу, і максимальна кількість атакуючих вузлів знижується в залежності від ймовірності проведення атаки (експеримент 4);
- при випадковому виборі від початку захищених вузлів картина процесу атаки практично не змінюється (експеримент 5);
- при високій топологічній вразливості зростає тривалість процесу ЗПЗІ (експеримент 5).

2.2 Математичні модель інформаційної взаємодії абонентів при поширенні забороненої інформації в інформаційно-телекомунікаційних мережах

Аналізуючи процес інформаційної взаємодії абонентів при поширенні забороненої інформації в ІТКМ, можна зробити наступні висновки. Маємо справу з трьома типами абонентів: атакуючі абоненти, які поширюють заборонену інформацію, захищені абоненти, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися, і потенційно вразливі абоненти, які можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію. При цьому ми спостерігаємо два протиборчих підпроцеси атаки і захисту абонентів мережі. Для моделювання таких явищ часто застосовують епідеміологічні моделі [43, 45], зокрема нашому опису точно відповідає SIR-модель Кермак-Маккендріка [46, 47]. Характер графіків, отриманих у результаті імітаційного моделювання (рисунок 2.7), подібний з результатами, що дає дана модель. Виходячи з вищесказаного, приходимо до висновку, що дана модель є найбільш релевантною для цього дослідження

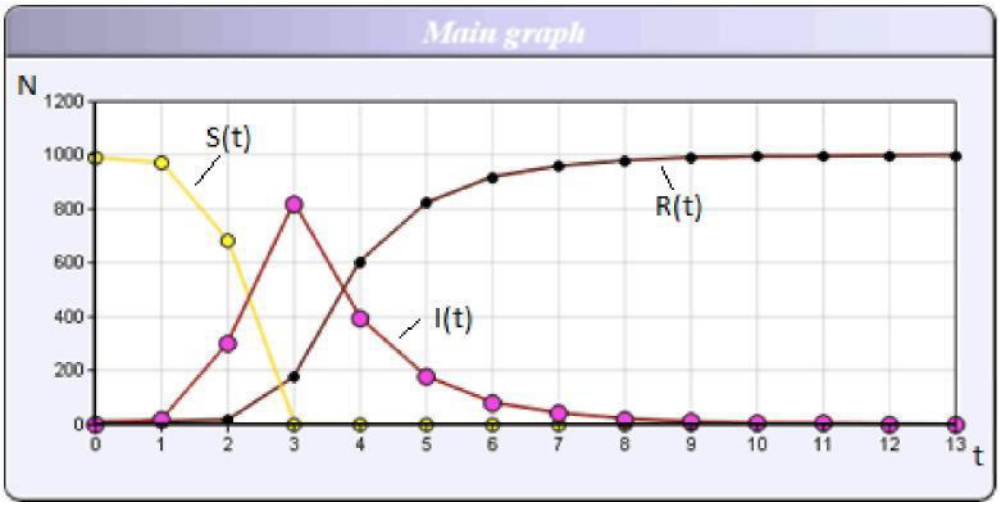


Рисунок 2.7 – Імітаційне моделювання ($N = 1000$, $\varphi = 20$, $I_0 = 1$, $\beta = 0{,}5$, $\gamma = 0{,}5$, $R_0 = 10$), $S(t)$ – кількість схильних до атаки вузлів

SIR (від англ. Susceptibles – Infectives – Removed with immunity) – епідеміологічна модель, що спрощено описує поширення захворювання, які передається від одного індивіда до іншого, яка розглядає суб'єктів з точки зору трьох можливих станів: сприйнятливий, інфікований, імунізований.

Система диференціальних рівнянь, що описують SIR-модель, має вигляд [37]:

$$\begin{cases} \frac{dI}{dt} = \beta \cdot \frac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \frac{dR}{dt} = \gamma \cdot I(t) \\ \frac{dS}{dt} = -\beta \cdot \frac{S(t) \cdot I(t)}{N} \end{cases} \quad (2.2)$$

де $I(t)$ – кількість заражених (інфікованих) особин, $S(t)$ – кількість сприятливих особин, $R(t)$ – кількість «виключених з імунізацією» (Removed with immunity) особин, $N = I(t) + S(t) + R(t)$ – кількість особин у популяції, γ – коефіцієнт відновлення / смерті, β – коефіцієнт зараження (інфікування), t – час. Дана система є надлишковою – будь-яке рівняння з трьох рівнянь можна виключити.

При використанні системи (2.2) для аналізу ЗПЗІ в ІТКМ отримуємо результати у вигляді графіків (рисунок 2.8), які хоча і правильно описують характер процесу, але не дають потрібної точності прогнозу.

Була висунута гіпотеза про те, що система (2.2) не дає потрібної точності в зв'язку з тим, що в моделі, яку вона описує, не враховуються топологічні особливості мережі. У зв'язку з цією гіпотезою була поставлена задача адаптування системи (2.2) під прогнозування ЗПЗІ в ІТКМ шляхом інтегрування в неї параметра топологічної уразливості мережі φ.

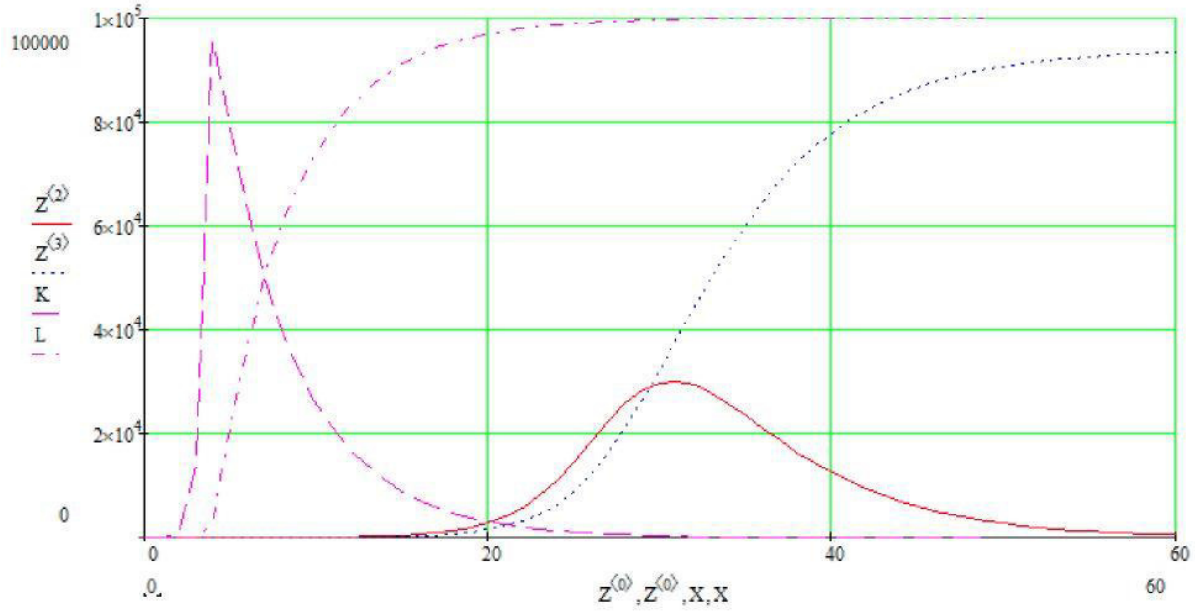


Рисунок 2.8 – Результати імітаційного моделювання (N=100000, $\varphi = 150$, $I_0 = 1,\ \beta = 0{,}3,\ \ \gamma = 0{,}2,\ R_0 = 0$) та аналітичного рішення ($Z^{<2>}, Z^{<3>}$ – аналітичне рішення для процесу атаки та захисту відповідно, K, L – результати імітаційного моделювання для процесів атаки та захисту відповідно).

Проаналізувавши графіки, отримані за результатами імітаційного моделювання та аналітичного рішення системи (2.2), і простеживши фізичний зміст рівнянь в даній системі [10], можна прийти до наступного висновку. Процес захисту не залежить від топології мережі, тому «змінювати» $R(t)$ не маємо права. А ось процес атаки залежить від структури зв'язків між абонентами в мережі. Параметр топологічної уразливості φ може впливати на $I(t)$ через коефіцієнт β. У загальному вигляді адаптовану систему (2.2) можна представити в наступному вигляді

$$\begin{cases} \frac{dI}{dt} = C \cdot \beta \cdot \frac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \frac{dR}{dt} = \gamma \cdot I(t) \\ \frac{dS}{dt} = -C \cdot \beta \cdot \frac{S(t) \cdot I(t)}{N} \end{cases} \quad (2.3)$$

де C – коефіцієнт, що залежить від параметра φ.

Зауважимо, що в [10] вже пропонувався аналогічний підхід, при цьому зазначалося, що коефіцієнт C може бути виражений функцією або апроксимувати константою.

Аналіз топологій великомасштабних ІТКМ показав, що типові значення параметра φ для них знаходяться в діапазоні від 100 до 600. Результати серії експериментів з імітаційного моделювання ЗПЗІ в ІТКМ (рисунки 2.9, 2.10) дозволили отримати залежність параметра C від φ у вигляді $2 * \ln \varphi$. Апроксимація проводилася методом найменших квадратів з використанням пакета MathCAD.

Підсумкова система має вигляд:

$$\begin{cases} \frac{dI}{dt} = 2 \cdot \ln \varphi \cdot \beta \cdot \frac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \frac{dR}{dt} = \gamma \cdot I(t) \\ \frac{dS}{dt} = -2 \cdot \ln \varphi \cdot \beta \cdot \frac{S(t) \cdot I(t)}{N} \end{cases} \quad (2.4)$$

Система диференціальних рівнянь (2.4) дозволяє отримати прогноз ЗПЗІ у великомасштабної ІТКМ ($N = 10^5..10^8$) з похибкою до 18%.

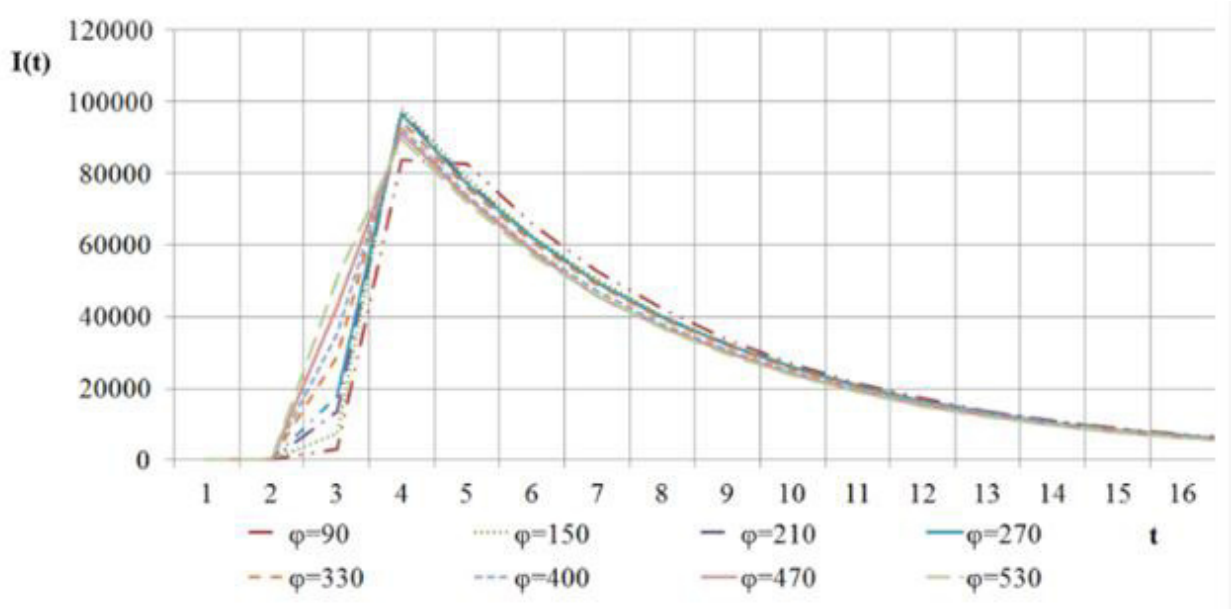


Рисунок 2.9 – Результати імітаційного моделювання ($N = 10^5$, $I_0 = 1$, $\beta = 0{,}3, \gamma = 0{,}2, R_0 = 0$)

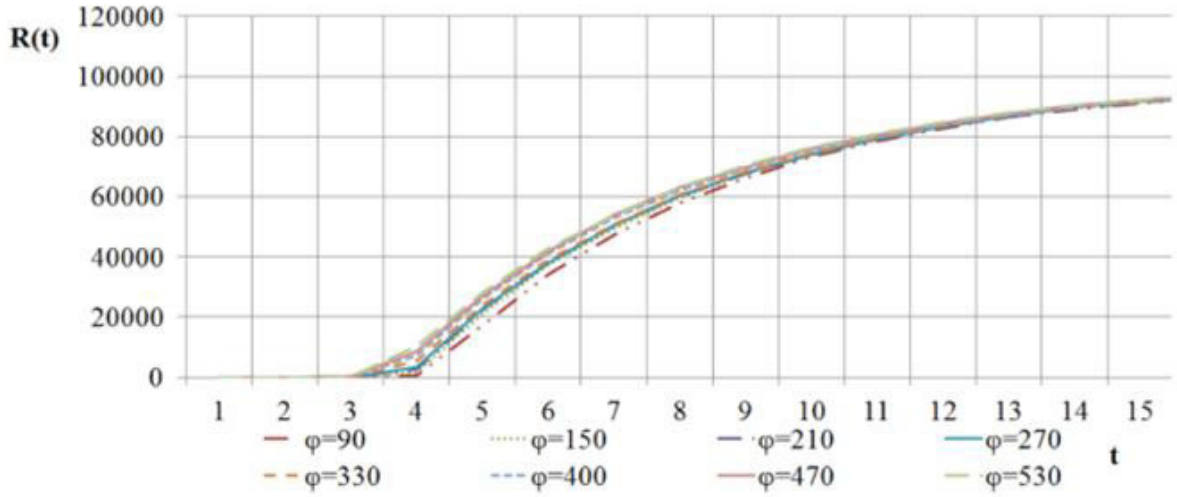


Рисунок 2.10 – Результати імітаційного моделювання ($N = 10^5$, $I_0 = 1$, $\beta = 0{,}3, \gamma = 0{,}2, R_0 = 0$)

2.3 Дослідження адекватності математичної моделі інформаційної взаємодії абонентів при поширенні забороненої інформації в інформаційно-телекомунікаційних мережах

Результати аналітичної моделі порівнювалися з результатами імітаційного моделювання процесу ЗПЗІ на топології реальної мережі.

Експеримент 1. На рисунку 2.11 наведені результати імітаційного моделювання та аналітичного розв'язку для β = 0,5, γ = 0,51, $R_0 = 0$, $I_0 = 1$.

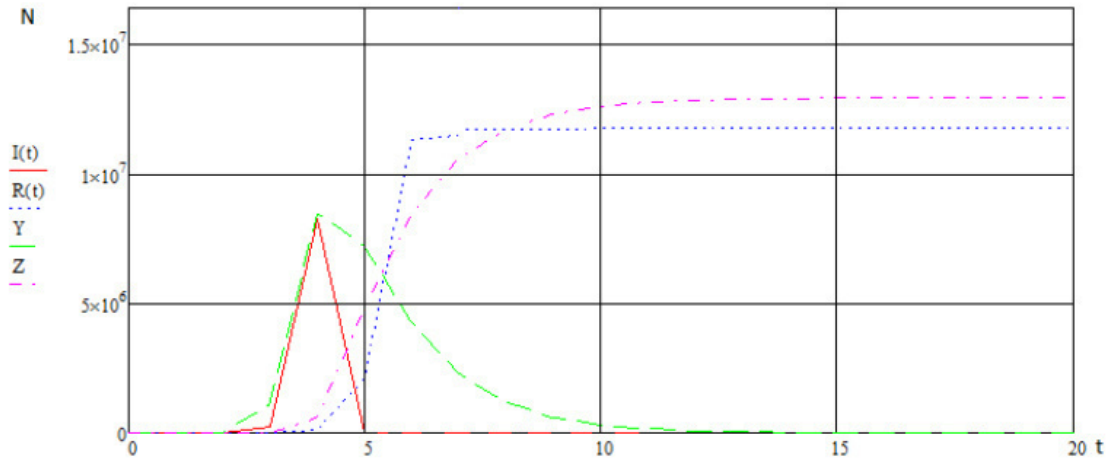


Рисунок 2.11 – Результати аналітичної та імітаційної моделі (I та R – аналітичний розв'язок, Y та Z – результати імітаційної моделі). β = 0,5, γ = 0,51, $R_0 = 0$, $I_0 = 1$.

Експеримент 2. На рисунку 2.12 наведені результати імітаційного моделювання та аналітичного розв'язку для $\beta = 0{,}5$, $\gamma = 0{,}51$, $R_0 = 0$, $I_0 \approx 24000$

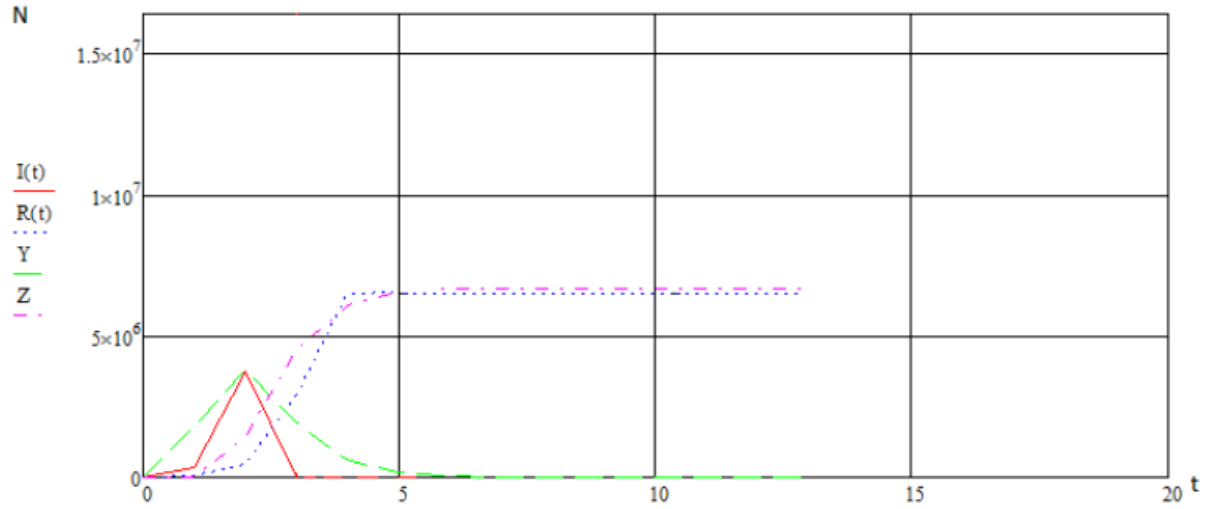


Рисунок 2.12 – Результати аналітичної та імітаційної моделі (I та R – аналітичний розв'язок, Y та Z – результати імітаційної моделі). $\beta = 0{,}5$, $\gamma = 0{,}51$, $R_0 = 0$, $I_0 \approx 24000$.

Експеримент 3. На рисунку 2.13 наведені результати імітаційного моделювання та аналітичного розв'язку для $\beta = 0{,}5$, $\gamma = 0{,}51$, $R_0 \approx 4 \cdot 10^6$, I_0=1.

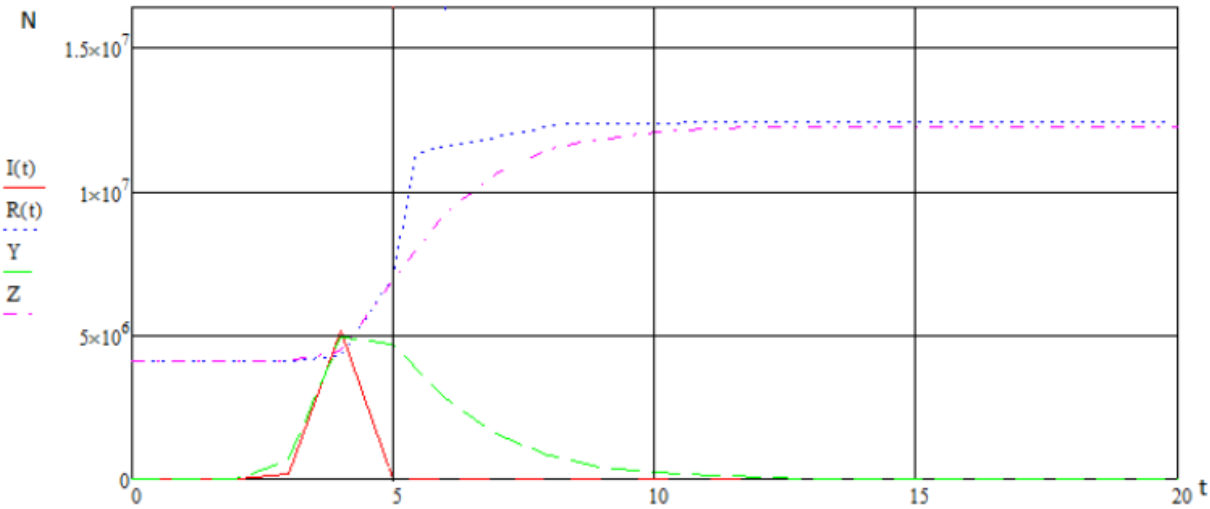


Рисунок 2.13 – Результати аналітичної та імітаційної моделі (I та R – аналітичний розв'язок, Y та Z – результати імітаційної моделі). $\beta = 0{,}5$, $\gamma = 0{,}51$, $R_0 \approx 4 \cdot 10^6$, $I_0 = 1$.

За результатами експериментів можна зробити наступні висновки:

- результати аналітичного рішення підходять для апроксимації імітаційних результатів, при цьому похибка апроксимації для процесу захисту $R(t)$ становить не більше 10%, для процесу атаки $I(t)$ – не більше 15% (експеримент 1, 2, 3);
- при середніх значеннях сили атаки і захисту ($\beta, \gamma \in [0{,}3; 0{,}7]$) похибка залишається в тому ж діапазоні ($\Delta_{R(t)} < 10\%$, $\Delta_{I(t)} < 15\%$), при сильній атаки і слабкому захисті і навпаки – може складати близько 20%.
- при моделюванні з великою кількістю спочатку атакуючих вузлів (I_0>>1) похибка складає: $\Delta_{R(t)} < 10\%$, $\Delta_{I(t)} < 15\%$ (експеримент 2);
- при додаванні в мережу великої кількості спочатку захищених вузлів (≈4 *10^6) аналітичне рішення також дає результат з похибкою $\Delta_{R(t)} < 10\%$, $\Delta_{I(t)} < 15\%$ (експеримент 3);
- порівнюючи дані результати з результатом застосування вихідної системи диференціальних рівнянь (2.2), можна говорити про значне збільшенні точності прогнозування процесу ЗПЗІ в ІТКМ за рахунок врахування впливу на процес топологічної уразливості мережі

2.4 Висновки

Розроблено алгоритм реалізації ЗПЗІ в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

Створена імітаційна модель ЗПЗІ в ІТКМ, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі.

Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з

використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

Приклади ефективного апробування механізмів прогнозування ЗПЗІ в ІТКМ дають підставу констатувати адекватність і функціональність основних теоретичних побудов і розроблених на їх основі алгоритмічних і інструментальних засобів

3 РОЗРОБКА МЕТОДИКИ ФОРМУВАННЯ ТОПОЛОГІЇ ВЕЛИКОМАСШТАБНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Під топологією будемо розуміти структуру інформаційних зв'язків між вузлами мережі. Топологічні характеристики, такі як середня ступінь зв'язності вузлів, розподіл ступенів зв'язності вузлів, кластерний коефіцієнт мережі, середня довжина шляху мережі, в роботі розглядаються як основні технічні уразливості ІТКМ до реалізацій загроз. Інші уразливості: використання неліцензійного ПЗ в вузлах, некоректно налаштовані міжмережеві екрани тощо, відображені в різних працях [6, 8, 17, 31] в даній роботі не розглядаються.

Для моделювання ЗПЗІ необхідно мати топологію реального об'єкту. Пряме отримання цієї інформації ускладнено в зв'язку з наступним протиріччям. Для підвищення точності результатів моделювання необхідно мати топологію всієї мережі. Отримати таку інформацію без прав адміністратора не є можливим. При зборі даних з правами абонента ІТКМ маємо справу з двома типами вузлів: відкритими і закритими. Якщо в ході збору даних ми отримуємо ідентифікатори (id) вузла і суміжних з ним вузлів, то такий вузол називаємо відкритим. Якщо ж отримуємо тільки id вузла (абонент за допомогою налаштувань приховав інформацію про свої контакти), то такий вузол називаємо закритим. Також в мережі можуть існувати вузли, які з'єднані тільки з закритими вузлами. При цьому неможливо отримати навіть ідентифікатор вузла. Таких вузлів в мережі незначна частина. Емпірично показано [43], що закритих вузлів на порядок більше, ніж відкритих, тому при зборі даних втрачається значна частина даних.

Особливості практичної реалізації:

1) частота запитів абонента про зв'язки вузла обмежена адміністраторськими заходами (наприклад, для соціальної мережі Facebook це значення приблизно становить 10 запитів в секунду). Це обмеження

призводить до того, що, з огляду на масштабність ІТКМ (десятки мільйонів вузлів), отримання інформації про топології мережі перетворюється в тривалий процес (наприклад, для соціальної мережі Facebook отримання інформації про $16*10^6$ вузлів зайняло близько 20 діб). З огляду на те, що час сесії обмежений (наприклад, для соціальної мережі Facebook це значення дорівнює одній добі), дана особливість повинна враховуватися при практичній реалізації.

2) відомі засоби (наприклад, Tictrac) для вирішення завдання збору інформації про зв'язки вузлів в ІТКМ неефективні, оскільки безпосередньо не призначені для досягнення цієї мети і мають безліч недоліків.

3) топологія реальної ІТКМ постійно змінюється (абоненти реєструються, додають зв'язку, видаляють зв'язку та облікові записи). У зв'язку з цим, необхідно постійно отримувати актуальну інформацію про ІТКМ для більш точного моделювання ЗПЗІ.

Топологія мережі рекомендується графом $G = \{V, E\}$, де V (множина вершин графа) – множина вузлів-абонентів, а E (множина ребер) – інформаційні зв'язки між вузлами.

Будемо вважати, що граф є неорієнтованим, тобто всі зв'язки – двонаправлені. Будь-які дві вершини графа можуть бути пов'язані не більше ніж одним ребром. Для спрощення досліджень граф вважається не виваженим, тобто сила інформаційних зв'язків не відображається на ваги відповідних ребер. Вузол є людино-машиною системою, на одному комп'ютері не може перебувати кілька вузлів.

У запропонованій моделі вузол $v_i = \{id_i, flag_i\}$ зберігає унікальний ідентифікатор абонента мережі (id) і прапор (flag). Змінна flag визначає статус вузла: відкритий ($flag = 1$) або закритий ($flag = 0$).

У розділі розробляється методика формування топології ІТКМ, яка складається з послідовності кроків:

• збір даних про топології доступною частини мережі

• формування повного графа мережі з урахуванням додавання

недоступної частини на основі обчислених прогнозованих топологічних характеристик (розподіл ступенів зв'язності, середня довжина шляху).

- формування вектору топологічної уразливості вузлів ІТКМ.

3.1. Збір даних про топології доступної частини мережі

Введемо визначення.

Визначення 1. Граф доступної частини мережі – граф, що містить відкриті і закриті вузли і зв'язки між ними.

Визначення 2. Повний граф мережі – граф, що містить відкриті вузли та закриті вузли, що перейшли в стан відкритих, і зв'язки між ними.

Визначення 3. Сусідні вузли (суміжні вузли) – вузли, які мають зв'язки з даним вузлом.

Постановка завдання: потрібно скласти граф доступної частини мережі $G(V, E)$, де

V – множина вершин, що включає два підмножини:

$W = \{w_i\}$ – підмножина відкритих вершин;

$U = \{u_i\}$ – підмножина закритих вершин;

E – множина зв'язків між вузлами ($e_{ij} = e_{ji}$ – зв'язок між i-м та j-м вузлами);

A – масив, що містить id пройдених вузлів (a_i – елементи масиву).

Блок-схема алгоритму формування графа доступної частини мережі зображена на рисунку 3.1.

Змінні, що використовуються в алгоритмі:

k – лічильник вузлів;

$Z = \{z_i\}$ – множина сусідніх вузлів k-го вузла;

flag – прапор, який визначає статус вузла (*flag* = 1 – відкритий, *flag* = 0 – закритий);

n – поточне значення довжини масиву A;

i – лічильник сусідніх вузлів

X – тимчасова множина.

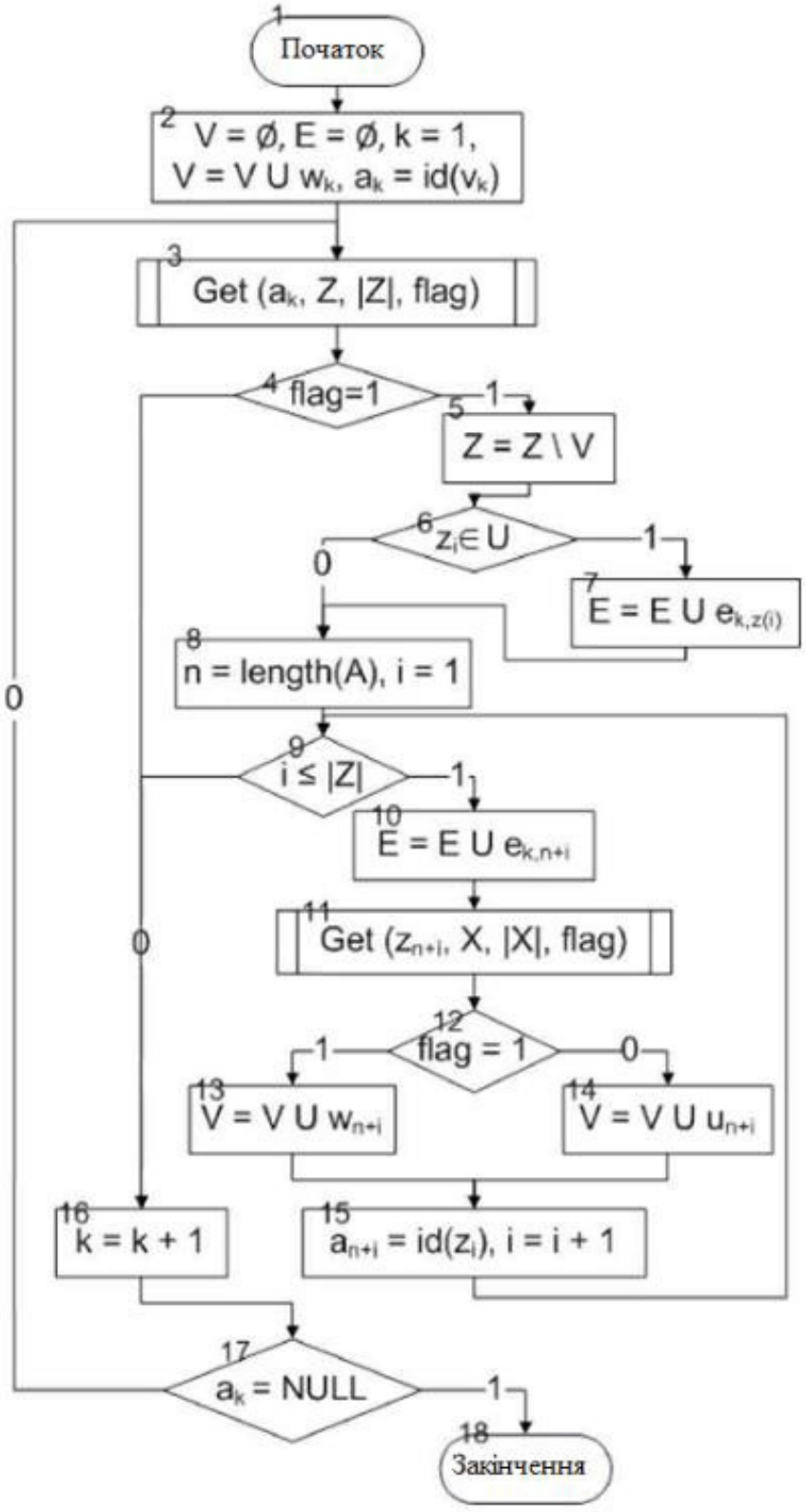


Рисунок 3.1. – Блок-схема алгоритму формування графа доступної частини мережі

Алгоритм 2 – Алгоритм формування графа доступної частини мережі

Крок 1 (блок 2). Початкова установка. Обнулити множини вершин $V = \emptyset$ і зв'язків $E = \emptyset$. Ініціалізувати лічильник вузлів (k = 1). Додати вершину v_1 в множину V ($V = V \cup v_1$), зробити її поточною. Виконати $a_k = id(v_k)$.

Крок 2 (блоки 3,4). Виконати функцію *Get*(a_k, Z, |Z|, *flag*) отримання множини Z сусідніх вузлів k-го вузла, де a_k – ідентифікатор k-го вузла, Z – множина, що повертається, |Z|– її потужність, *flag* – прапор, який визначає статус вузла (відкритий/закритий). Якщо *flag* =1 (вузол відкритий), перейти до кроку 3, інакше (*flag* = 0) – до кроку 5.

Крок 3 (блок 5-7). Для $\forall z_i \in Z$ (i = 1, .., |Z |) якщо $z_i = v_k$, то $Z = Z \backslash z_i$ і якщо $z_i \in U$, то $E = E \cup e_{k,z(i)}$.

Крок 4 (блоки 8-15). Визначити довжину масиву A (n = *length*(A)). Для $\forall z_{n+i} \in Z$ (i = 1, .., |Z|) додати ребро з до k–ою вершиною $E = E \cup e_{k,n+i}$. Виконати функцію *Get*(z_{n+i}, X, |X|, *flag*). Якщо *flag* = 1, то $V = V \cup w_{n+i}$, інакше (*flag* = 0) $V = V \cup u_{n+i}$. Виконати $a_{n+i} = id(z_i)$.

Крок 5 (блоки 16,17). Перейти до наступного вузла $k = k+ 1$. Якщо $a_k = NULL$, то кінець алгоритму, інакше перейти до кроку 2.

Розглянемо приклад поетапної реалізації алгоритму 2.

Етап 1. Виконуємо початкові установки згідно першого кроку алгоритму: k = 1, $V = \{w_1\}$, A[12].

Етап 2. Виконуємо функцію *Get*(12, Z, |Z|, *flag*). Отримуємо Z = {43, 36, 39, 78}, |Z| = 4, *flag* = 1. Переходимо до третього кроку алгоритму.

Етап 3. Перевіряємо множину Z на наявність вузлів, вже доданих до множини V, і при наявності таких, видаляємо їх. Отримуємо Z = {43, 36, 39, 78}, |Z| = 4.

Етап 4. Визначаємо довжину масиву A (n = 1). Додаємо ребра, що зв'язують першу вершину з вузлами з множини Z. Отримуємо $E = \{e_{1,2}, e_{1,3}, e_{1,4}, e_{1,5}\}$. Виконуємо функцію *Get* для всіх вузлів з множини Z і додаємо їх до

відповідних підмножин множини V. Отримуємо $W = \{w_1, w_2\}$, $U = \{u_3, u_4, u_5\}$. Записуємо ідентифікатори вузлів в масив A. Отримуємо A[12, 43, 36, 39, 78].

Етап 5. Збільшуємо лічильник $k = 1 + 1 = 2$. Другий елемент масиву $A(a_2)$ існує, отже, переходимо до другого кроку алгоритму.

Після виконання перших п’яти етапів отримуємо граф, зображений на рисунку 3.2, на якому закриті вузли виділені сірим кольором, а відкриті – білим.

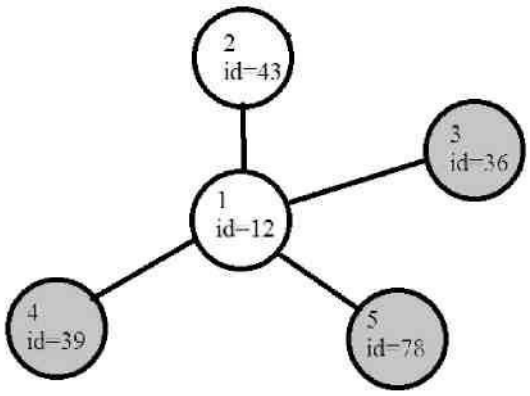


Рисунок 3.2 – Результат роботи алгоритму (1-5 етапи)

Етап 6. Виконуємо функцію *Get*(43, Z, $|Z|$, *flag*). Отримуємо $Z = \{12, 16, 25, 4\}$, $|Z| = 4$, *flag* = 1. Переходимо до третього кроку алгоритму.

Етап 7. Перевіряємо множину Z на наявність вузлів, вже доданих у множину V, і при наявності таких, видаляємо їх. Отримуємо $Z = \{16, 25, 4\}$, $|Z|=3$.

Етап 8. Визначаємо довжину масиву A (n=5). Додаємо ребра, що зв’язують другу вершину з вузлами із множини Z. Отримуємо $E = \{e_{1,2}, e_{1,3}, e_{1,4}, e_{1,5}, e_{2,6}, e_{2,7}, e_{2,8}\}$. Виконуємо функцію *Get* для всіх вузлів з множини Z і додаємо їх до відповідних підмножин множини V. Отримуємо $W = \{w_1, w_2, w_8\}$, $U = \{u_3, u_4, u_5, u_6, u_7\}$. Записуємо ідентифікатори вузлів в масив A. Отримуємо A[12, 43, 36, 39, 78, 16, 25, 4].

Етап 9. Збільшуємо лічильник $k = 2 + 1 = 3$. Третій елемент масиву $A(a_3)$ існує, отже, переходимо до другого кроку алгоритму.

Після виконання етапів 6-9 отримуємо граф, зображений на рисунку 3.3.

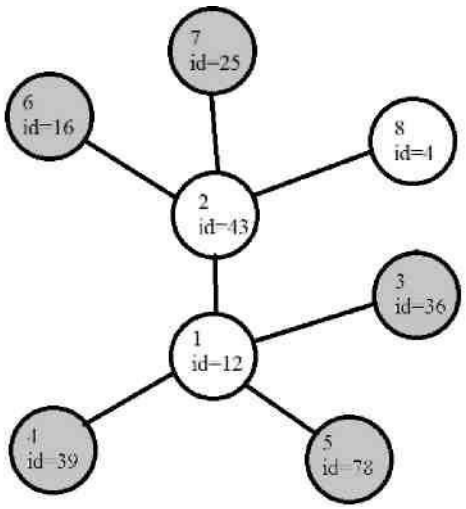


Рисунок 3.3 – Результат роботи алгоритму (1-9 етапи)

Етап 10. Виконуємо функцію *Get*(36, Z, |Z|, flag). Отримуємо $Z = Ø$, $|Z| = 0$, $flag = 0$. Переходимо до п’ятого кроку алгоритму.

Етап 11. Збільшуємо лічильник $k = 3 + 1 = 4$. Четвертий елемент масиву $A(a_4)$ існує, отже, переходимо до другого кроку алгоритму.

Етап 12. Виконуємо функцію *Get*(39, *Z*, |*Z*|, *flag*). Отримуємо $Z = Ø$, $|Z|=0$, $flag = 0$. Переходимо до п’ятого кроку алгоритму.

Етап 13. Збільшуємо лічильник $k = 4 + 1 = 5$. П’ятий елемент масиву $A(a_5)$ існує, отже, переходимо до другого кроку алгоритму.

Етап 14. Виконуємо функцію *Get*(78, *Z*, |*Z*|, *flag*). Отримуємо $Z = Ø$, $|Z|=0$, $flag = 0$. Переходимо до п’ятого кроку алгоритму.

Етап 15. Збільшуємо лічильник $k = 5 + 1 = 6$. Шостий елемент масиву $A(a_6)$ існує, отже, переходимо до другого кроку алгоритму.

Етап 16. Виконуємо функцію *Get*(16, *Z*, |*Z*|, *flag*). Отримуємо $Z = Ø$, $|Z|=0$, $flag = 0$. Переходимо до п’ятого кроку алгоритму.

Етап 17. Збільшуємо лічильник $k = 6 + 1 = 7$. Сьомий елемент масиву $A(a_7)$ існує, отже, переходимо до другого кроку алгоритму.

Етап 18. Виконуємо функцію *Get*(25, *Z*, |*Z*|, *flag*). Отримуємо $Z = Ø$, $|Z|=0$, $flag = 0$. Переходимо до п’ятого кроку алгоритму.

Етап 19. Збільшуємо лічильник $k = 7 + 1 = 8$. Восьмий елемент масиву $A(a_8)$ існує, значить, переходимо до другого кроку алгоритму

Етап 20. Виконуємо функцію *Get*(8, *Z*, |*Z*|, *flag*). Отримуємо $Z = \{43, 36\}$, $|Z| = 2$, $flag=1$. Переходимо до третього кроку алгоритму.

Етап 21. Перевіряємо множину Z на наявність вузлів, вже доданих в множину V, і при наявності таких, видаляємо їх. Отримуємо $Z = \varnothing$, $|Z| = 0$, $E = \{e_{1,2}, e_{1,3}, e_{1,4}, e_{1,5}, e_{2,6}, e_{2,7}, e_{2,8}, e_{8,3}\}$.

Етап 22. На даному етапі нічого не змінюється, так як $Z = \varnothing$.

Етап 23. Збільшуємо лічильник $k = 8 + 1 = 9$. Дев'ятого елемента масиву $A(a_9)$ існує, отже, робота алгоритму завершена.

Сформований в результаті алгоритму граф доступної ІТКМ зображений на рисунку 3.4.

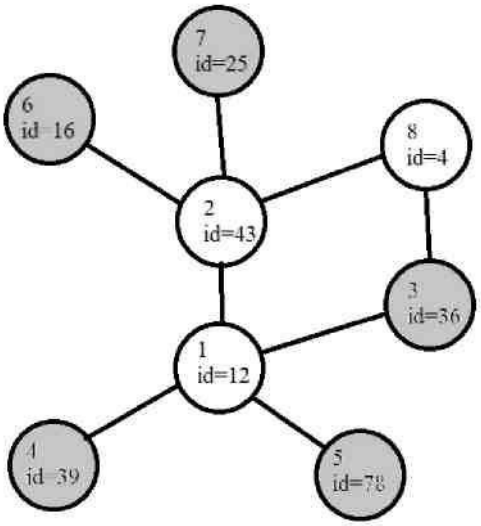


Рисунок 3.4 – Підсумковий результат роботи алгоритму

Результат роботи після кожного етапу відображені в таблиці 3.1.

Таблиця 3.1 – Поетапні результати роботи алгоритму

№	*V*	*E*	*A*	*Z*	*K*	*N*
1	w_1	Ø	12	Ø	1	0
2	w_1	Ø	12	43, 36, 39, 78	1	0
3	w_1	Ø	12	43, 36, 39, 78	1	0
4	w_1, w_2, u_3, u_4, u_5	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$	12, 43, 36, 39, 78	43, 36, 39, 78	1	1
5	w_1, w_2, u_3, u_4, u_5	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$	12, 43, 36, 39, 78	43, 36, 39, 78	2	1
6	w_1, w_2, u_3, u_4, u_5	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$	12, 43, 36, 39, 78	12, 16, 25, 4	2	1
7	w_1, w_2, u_3, u_4, u_5	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$	12, 43, 36, 39, 78	16, 25,4	2	1
8	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16 ,25, 4	16, 25, 4	2	5
9	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	16,25,4	3	5
10	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	3	5
11	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	4	5
12	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	4	5
13	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	5	5
14	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	5	5
15	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	6	5
16	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	6	5
17	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	7	5
18	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12 ,43, 36, 39, 78, 16, 25, 4	Ø	7	5
19	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	8	5
20	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$	12, 43, 36, 39, 78, 16, 25, 4	43, 36	8	5
21	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$, $e_{8,3}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	8	5
22	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$, $e_{8,3}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	8	8
23	w_1, w_2, w_8, u_3, u_4, u_5, u_6, u_7	$e_{1,2}$, $e_{1,3}$, $e_{1,4}$, $e_{1,5}$, $e_{2,6}$, $e_{2,7}$, $e_{2,8}$, $e_{8,3}$	12, 43, 36, 39, 78, 16, 25, 4	Ø	9	8

Розглянутий приклад показує коректність алгоритму 2.

3.2 Формування повного графа мережі з урахуванням недоступної частини

Розроблено алгоритм формування повного графа мережі, який враховує топологічні характеристики доступної частини мережі (розподіл ступенів зв’язності, середня довжина шляху).

Обчислення середнього ступеня зв’язності мережі.

Ступінь зв’язності вузла (degree) – кількість суміжних з ним вузлів.

Середній ступінь зв’язності мережі (average degree) – середнє арифметичне ступеня зв’язності по всій мережі.

Використаний алгоритм обчислення середнього ступеня зв’язності ґрунтується на обчисленні ступенів зв’язності у відкритих вузлів з урахуванням їх зв'язків з закритими. Середнє значення береться з відкритих вузлів.

Отримання розподілу ступенів зв’язності вузлів у мережі

Розподіл ступенів зв’язності вузлів – статистична характеристика, що показує кількість вузлів з кожним значенням зв’язності в мережі [36].

Облік відкритих і закритих вузлів при отриманні розподілу ступенів зв’язності ведеться аналогічним чином з підходом обчислення середнього ступеня зв’язності.

Обчислення кластерного коефіцієнта мережі

Кластерний коефіцієнт вузла – це характеристика, що показує «щільність» зв’язків навколо вузла [36]. Кластерний коефіцієнт вузла обчислюється як відношення числа існуючих зв’язків між суміжними вузлами до значення загальної кількості можливих таких зв’язків:

$$C_i = \frac{2n_i}{k_i \cdot (k_i - 1)}$$

де k_i – ступінь зв’язності вузла, n_i – кількість зв’язків між суміжними вузлами.

Розглянемо приклад обчислення кластерного коефіцієнта для вузла 1 (рисунок 3.5). Суцільними лініями показані існуючі зв’язки, пунктирними –

потенційні. Ступінь зв’язності $k = 4$. Кількість можливих зв’язків між його суміжними вузлами рівно $k \cdot (k-1)/2 = 4 \cdot (4-1) = 6$. Кількість існуючих зв’язків – 2. Кластерний коефіцієнт $C = 2/6 = 1/3$.

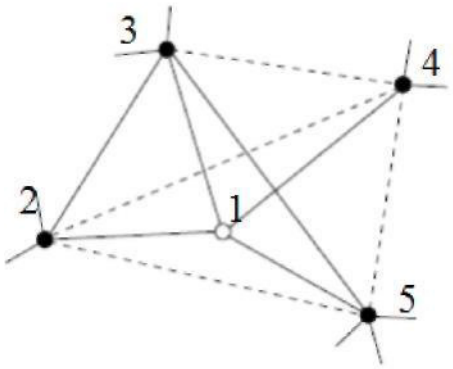


Рисунок 3.5 – Схематичний рисунок для визначення кластерного коефіцієнта

Алгоритм обчислення коефіцієнта кластеризації мережі полягає в підрахунку кластерного коефіцієнта кожного вузла і знаходження середнього значення. Обчислення кластерних коефіцієнтів здійснюється тільки для відкритих вузлів з підрахунком клік утворених і відкритими і закритими вузлами. Середнє значення розраховується за відкритими вузлами.

Алгоритм обчислення середньої довжини шляху мережі

Середня довжина шляху вузла – середнє арифметичне найкоротших шляхів від заданого вузла до всіх інших.

Середня довжина шляху мережі – середнє арифметичне середніх довжин шляху всіх вузлів мережі.

Обчислення середньої довжини шляху в графі здійснюється тільки за відкритими вузлами. Закриті вузли при цьому «віддалялися» з мережі, так як вони не несуть корисної інформаційного навантаження для даної топологічної характеристики. Даний алгоритм полягає в обчисленні суми середніх довжин шляху для кожного відкритого вузла, поділених на їх загальну кількість.

Блок-схема алгоритму формування повного графа мережі з урахуванням недоступної частини зображена на рисунку 3.6.

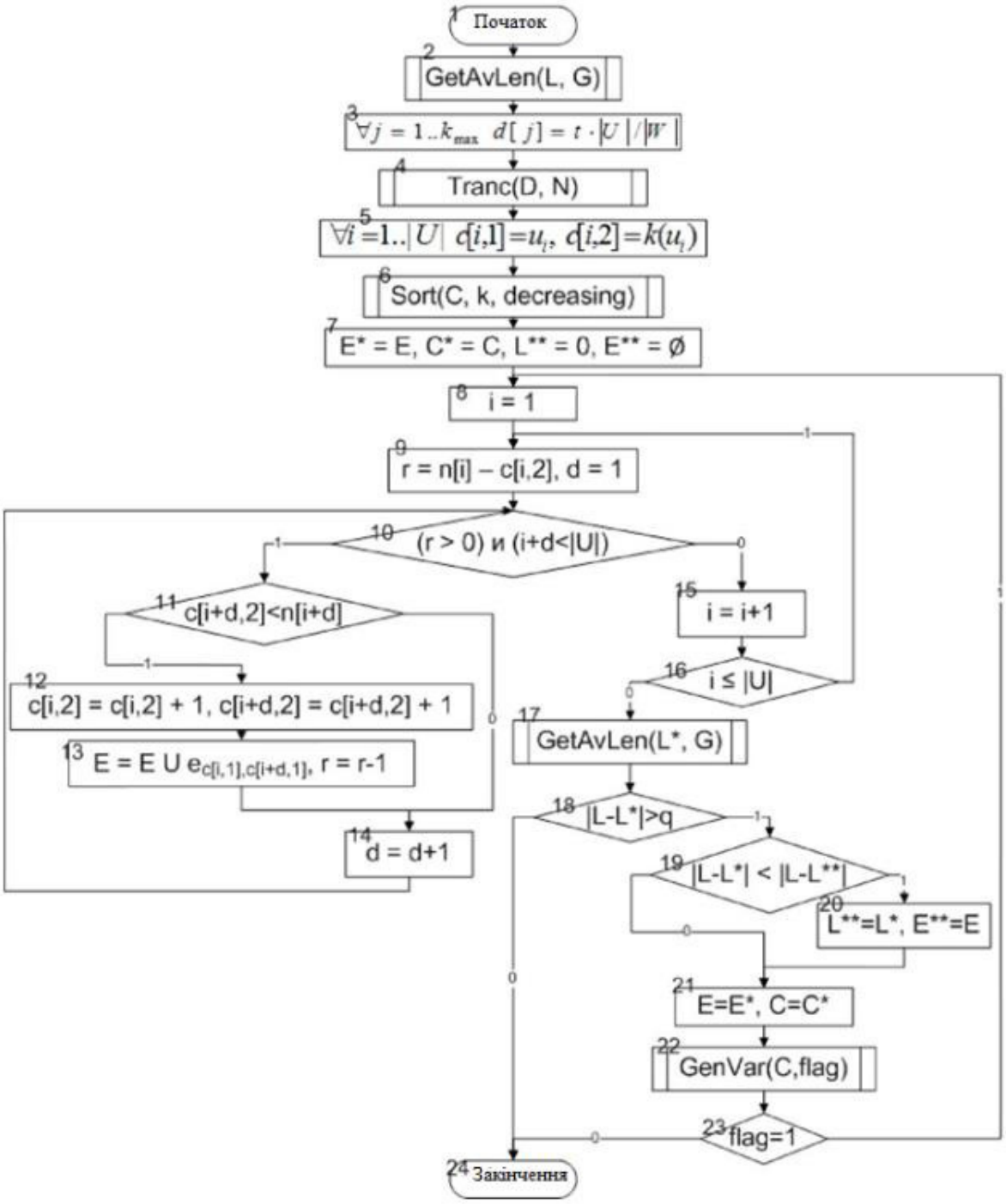


Рисунок 3.6 – Алгоритм генерації недоступної частини мережі

Алгоритм 3 – Алгоритм формування повного графа мережі

Крок 1 (блок 2). Обчислити середню довжину шляху L в графі G.

Крок 2 (блок 3). Отримати прогнозований розподіл (гістограму) ступенів зв'язності за закритими вузлів: масив $D = \|d[j]\|$, $d[j] = t \cdot |U|/|W|$, де t –

кількість вершин зі ступенем зв'язності j (j=1..k_{max}; $k_{max} = \max\{k_1..k_{|V|}\}$; k – ступінь зв'язності вузла).

Крок 3 (блок 4). Сформувати масив $N = \|n[i]\|$, $i = 1 .. |U|$ за правилом: в масив включаються значення j з масиву D d_j разів. Відсортувати N за спаданням.

Крок 4 (блоки 5,6). Сформувати двовимірний масив C=‖c[i]‖ за правилом: $\forall i = 1..|U| \quad c[i,2] = u_i, \quad c[i,2] = k(u_i)$. Відсортувати C за значенням k в порядку спадання.

Крок 5 (блок 7). Зберегти вихідну конфігурацію мережі: $E^* = E$, $C^* = C$. Ініціалізувати змінну $L^{**} = 0$ і множину $E^{**} = Ø$.

Крок 6 (блоки 8-16). Отримати нову конфігурацію мережі: Ініціалізувати лічильник вузлів $i = 1$. Для $\forall i = 1..|U|$ визначити кількість зв'язків, що додаються, для i-го вузла $r = n[i] - c\ [i, 2]$, $d = 1$. Поки $r > 0$ та $i + d \le |U|$, знайти вузол для зв'язку: якщо він існує $c[i + d, 2] < n[i + d]$, то додати зв'язок $c[i, 2] = c[i, 2] + 1$, $c[i + d, 2] = c[i + d, 2] + 1$, $E = E \cup e_{c[i,1],c[i+d.1]}$, $r = r - 1$; $d = d + 1$.

Крок 7 (блок 17). Обчислити середню довжину шляху L^* для графа мережі з новою конфігурацією.

Крок 8 (блок 18). Якщо значення L^* задовольняє заданій точності q ($|L - L^*| < q$), то кінець алгоритму.

Крок 9 (блоки 19-21). Якщо значення L^* поточної конфігурації ближче до L, ніж значення L^{**} з попередніх конфігурацій ($|L - L^*| < |L - L^{**}|$), то зберегти кращу конфігурацію ($L^{**} = L^*$, $E^{**} = E$). Відновити вихідну конфігурацію мережі ($E = E^*$, $C = C^*$).

Крок 10 (блоки 22,23). Згенерувати новий варіант розстановки вузлів в масиві C. Якщо варіантів більше немає, то кінець алгоритму, інакше перейти до кроку 6.

Розглянемо приклад поетапної реалізації алгоритму 3.2. На рисунку 3.7 зображений граф доступної частини вихідної мережі (білим відзначені відкриті, а сірим – закриті вузли). Задача – отримати повний граф ІТКМ з точністю середньої довжини шляху 0,15.

Етап 1. Обчислюємо середню довжину шляху – *GetAvLen*(*L*,*G*). Отримуємо $L = 2{,}85$.

Етап 2. Отримуємо розподіл ступенів зв'язності за закритими вузлами відповідно до кроку 2 алгоритму. Отримуємо масив D, який представлений в таблиці 3.2.

Таблиця 3.2 – Розподіл ступенів зв'язності за закритими вузлів

k	1	2	3	4	5	6	7
Кількість вузлів	1	2	3	2	2	1	1

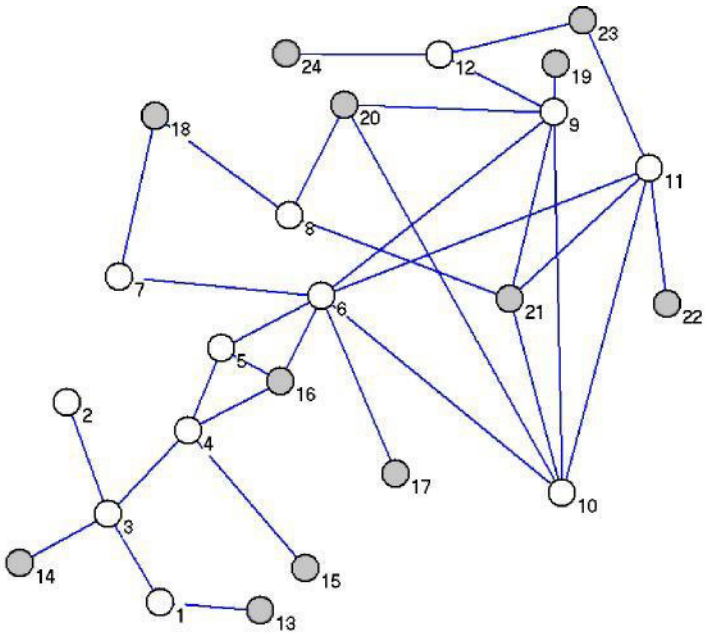


Рисунок 3.7 – Граф вихідної мережі

Етап 3. Формуємо масив *N* і сортуємо його відповідно до кроку 3 алгоритму. Отримуємо $N = \{7, 6, 5, 5, 4, 4, 3, 3, 3, 2, 2, 1\}$.

Етап 4. Формуємо двовимірний масив *C* відповідно до кроку 4 алгоритму. Отримуємо масив *C*, який представлений в таблиці 3.3.

Таблиця 3.3 – Двовимірний масив *C*

№ вузла	21	20	16	18	23	13	24	**22**	19	17	15	14
Поточне значення *k*	4	3	3	2	2	1	1	1	1	1	1	1

Етап 5. Зберігаємо поточну конфігурацію відповідно до кроку 5 алгоритму. Отримуємо множину E^*, що містить всі зв'язки вихідного графа мережі, і масив C^*, рівний C. Ініціалізувавши змінну $L^{**} = 0$ та множину $E^{**}=Ø$.

Етап 6. Отримуємо нову конфігурацію мережі відповідно до кроку 6 алгоритму.

Результат роботи етапу представлений в таблиці 3.4.

На першому кроці для вузла 21, щоб отримати зв'язність 7, потрібно додати 3 зв'язки (7 – 4 = 3). Додаємо зв'язки до наступних вузлів ($e_{21,20}$, $e_{21,16}$, $e_{21,18}$) і збільшуємо у них поточний ступінь зв'язності.

Крок 2 – додаємо два зв'язки ($e_{20,16}$, $e_{20,18}$) для вузла 20. У вузла 16 стає потрібна ступінь 5, переходимо до наступного вузла.

Крок 3 – додаємо один зв'язок ($e_{18,23}$) для вузла 18.

Крок 4 – додаємо один зв'язок ($e_{23,13}$) для вузла 23.

Крок 5 – додаємо два зв'язки ($e_{13,24}$, $e_{13,22}$) для вузла 13.

Крок 6 – додаємо один зв'язок ($e_{24,22}$) для вузла 24.

Крок 7 – додаємо два зв'язки ($e_{19,17}$, $e_{19,15}$) для вузла 19.

Таблиця 3.4 – Результати роботи 6 етапу

№ вузла	21	20	16	18	23	13	24	**22**	19	17	15	14
Поточне значення *k*	4	3	3	2	2	1	1	1	1	1	1	1
Потрібне значення *k*	**7**	**6**	**5**	**5**	**4**	**4**	**3**	**3**	**3**	**2**	**2**	**1**
Крок 1	*7*	4	4	3	2	1	1	1	1	1	1	1
Крок 2	*7*	*6*	*5*	4	2	1	1	1	1	1	1	1
Крок 3	*7*	*6*	*5*	*5*	3	1	1	1	1	1	1	1
Крок 4	*7*	*6*	*5*	*5*	*4*	2	1	1	1	1	1	1
Крок 5	*7*	*6*	*5*	*5*	*4*	*4*	2	2	1	1	1	1
Крок 6	*7*	*6*	*5*	*5*	*4*	*4*	*3*	*3*	1	1	1	1
Крок 7	*7*	*6*	*5*	*5*	*4*	*4*	*3*	*3*	*3*	*2*	*2*	*1*

Етап 7. Обчислюємо середню довжину шляху L^* (*GetAvLen*(*L*,*G*)). Отримуємо $L^* = 2{,}7$.

Етап 8. Порівнюємо значення L і L^*: q=2,85 – 2,7 = 0,15. Отримане значення середньої довжини шляху задовольняє умові завдання, отже, кінець алгоритму.

На рисунку 3.8 зображений повний граф ІТКМ, отриманий в результаті роботи алгоритму

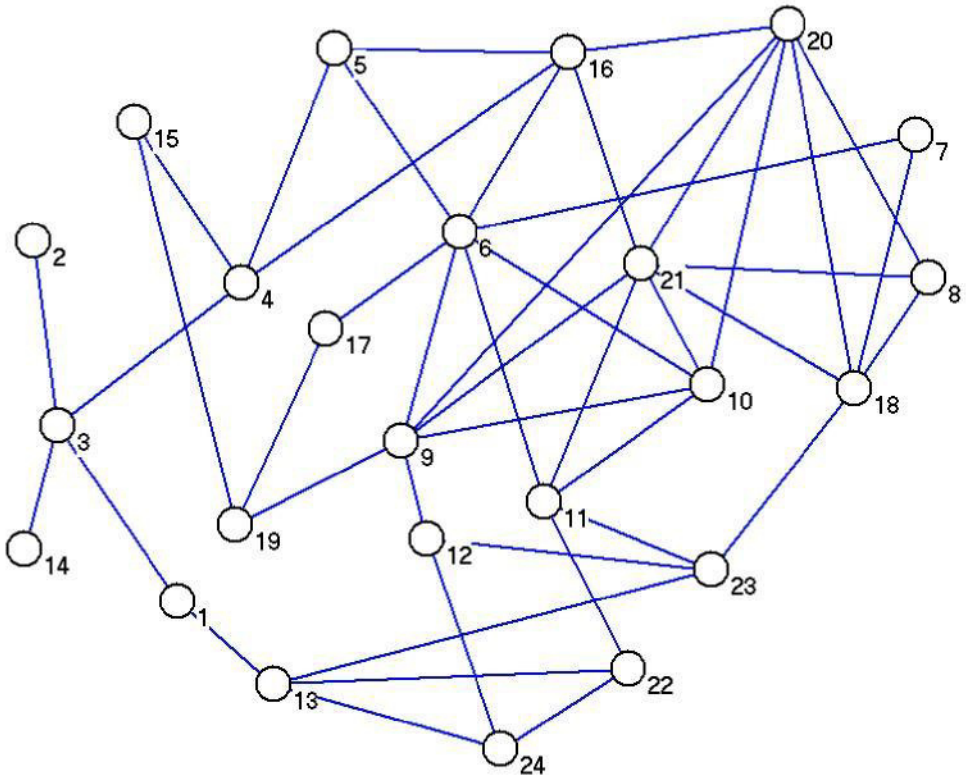


Рисунок 3.8 – Повний граф ІТКМ

3.3 Формування вектору топологічної уразливості повного графа мережі

Топологічна вразливість ІТКМ – внутрішня властивість ІТКМ, заснована на характеристиках її топології, яке сприяє поширенню загрози забороненої інформації.

Топологічною вразливістю вузла мережі назвемо показник φ, який обчислюється за формулою:

$$\varphi_i = \frac{k_i \cdot (C_i + 1)}{L_i} \qquad (3.1)$$

де k_i – ступінь зв'язності вузла, C_i – кластерний коефіцієнт вузла, L – середня довжина шляху вузла.

Дана характеристика показує, наскільки вразливий до атак з точки зору розташування в мережі певний вузол.

Накладається умова для застосування формули (3.1) – в мережі має бути більше одного вузла.

Властивості коефіцієнта φ:

1) $1 \leq \varphi \leq 2 \cdot (N-1)$, де N – кількість вузлів в мережі.

Крайній випадок (максимальне значення) – повнозв'язний граф. У ньому $k_i = N - 1$ та середня довжина шляху дорівнює одиниці $L_i = 1$. Кластерний коефіцієнт має властивість $0 \leq C \leq 1$ і в повнозв'язну графі $C_i = 1$. Отже, в цьому випадку $\varphi_i = 2 \cdot (N-1)$.

Крайній випадок (мінімальне значення) – граф з двох вузлів. При цьому $k_i = 1$, $L_i = 1$, $C_i = 0$. Отже, в цьому випадку $\varphi_i = 1$.

2) Зі збільшенням φ, зростає вразливість вузла.

Підрахунок коефіцієнта топологічної уразливості для всієї мережі здійснюється за формулою:

$$\varphi = \frac{k \cdot (C+1)}{L}, \tag{3.2}$$

де k – середній ступінь зв'язності вузлів в мережі, C – середній кластерний коефіцієнт мережі, L – середня довжина шляху мережі.

При дослідженні топологій реальних великомасштабних ІТКМ (10^5 – 10^8), можна виділити основні значущі положення:

1) середня ступінь зв'язності вузлів в таких мережах становить 100–1000;

2) середня довжина шляху визначається теорією шести рукостискань: в глобальних масштабах дорівнює 6, в реальних мережах становить значення 3–5;

3) коефіцієнт кластеризації, як правило, варіюється в значних від 0,01 до 0,2.

Виходячи з перерахованого вище і отриманих експериментальних результатів, маємо типове значення коефіцієнта топологічної уразливості в діапазоні від 100 до 500.

Практичне застосування:

1. Використовуючи коефіцієнт φ можна оцінити топологічну вразливість конкретної реальної мережі за формулою (3.2).

У ході роботи були проаналізовані соціальні мережі Facebook і ВКонтакте. Для мережі Facebook $\varphi \approx 70$, ВКонтакте – $\varphi \approx 200$. Для мережі Facebook отримали не зовсім типове значення, пов'язане це з методом вибірки, застосованої американськими дослідниками, а також тим, що дана мережа найбільша і, дійсно, в цілому менш вразлива, ніж мережа ВКонтакте. У другому розділі магістерської роботи топологічна вразливість φ використовувалися для створення аналітичної моделі поширення забороненої інформації як інтегральна складова топологічних параметрів мережі.

2. При аналізі топологічних характеристик мережі можна підрахувати коефіцієнти уразливості для кожного вузла в мережі (вектор топологічної уразливості вузлів ІТКМ).

Вектор топологічної уразливості вузлів ІТКМ – вектор виду:

№ вузла	значення φ
Вузол 1	φ_1
.....	.....
Вузол N	φ_N

Отриманий вектор можна використовувати при прогнозуванні загрози поширення забороненої інформації. З одного боку, можна класифікувати за небезпекою атакуючі вузли, а з іншого боку, можна вибудувати найбільш ефективну стратегію протидії загрозі.

3.4 Особливості розробки програмного інструментарію

Розроблена методика формування топології ІТКМ реалізована у вигляді програмного комплексу.

Перша програма призначена для отримання доступної частини мережі. Хоча ці програми орієнтовані на соціальну мережу «ВКонтакте», їх легко можна переробити під іншу ІТКМ. Робота програми заснована на алгоритмі обходу в ширину. Додаток написано на мові програмування Python. Для зберігання топології використовується об’єктно-орієнтована база даних ZODB. Отримання інформації здійснюється за допомогою API ВКонтакте. Програма збирає дані до настання одного з наступних подій: отримана інформація про всі відкриті вузлах в мережі, збір даних перерваний користувачем.

На початку роботи програми необхідно авторизуватись під акаунтом абонента, з якого почнеться збір інформації. Вихідними дані додатка є текстовий файл, в якому в кожному рядку записаний ідентифікатор вузла, і через пробіл перераховані ідентифікатори суміжних з ним вузлів.

В результаті роботи програми була отримана частина топології соціальної мережі ВКонтакте, яка містить 118 834 відкритих вузли і 16270504 закритих. Фрагмент вихідного файлу представлений на рисунку 3.9.

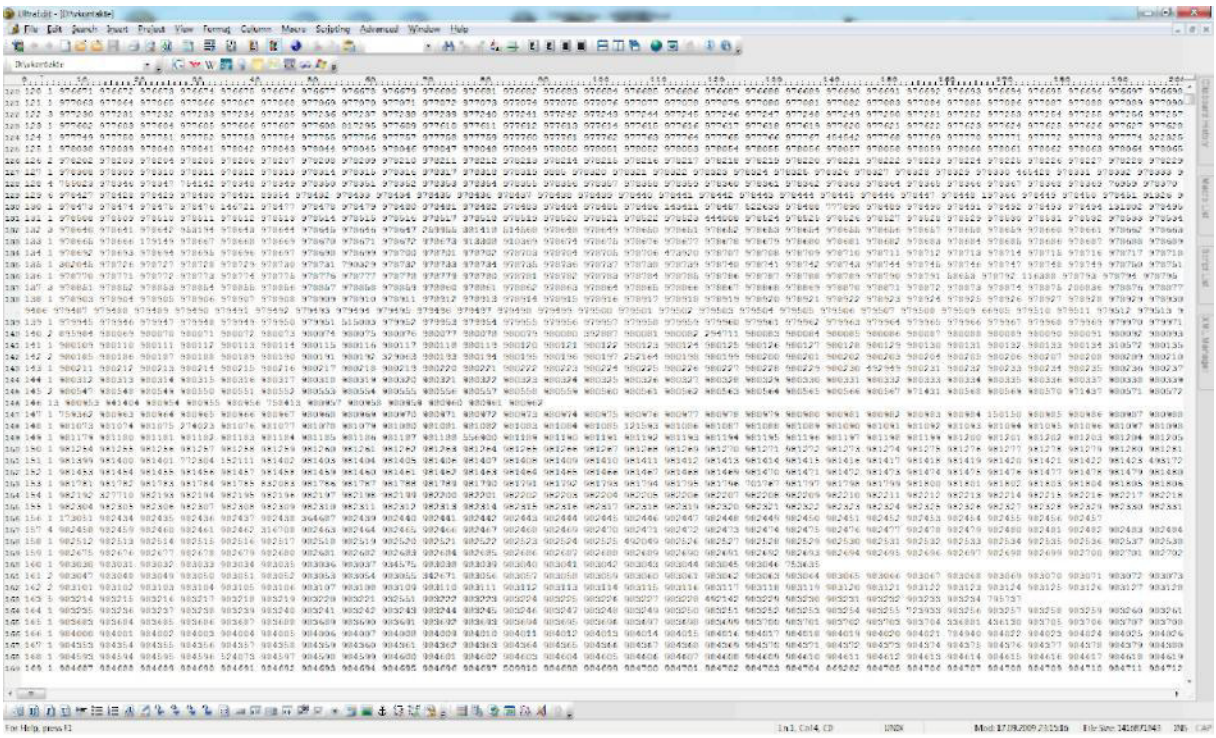


Рисунок 3.9 – Фрагмент вихідного файлу програми

На рисунку 3.10 показаний фрагмент (1000 вузлів) отриманої топології, побудований за допомогою ПЗ Pajek.

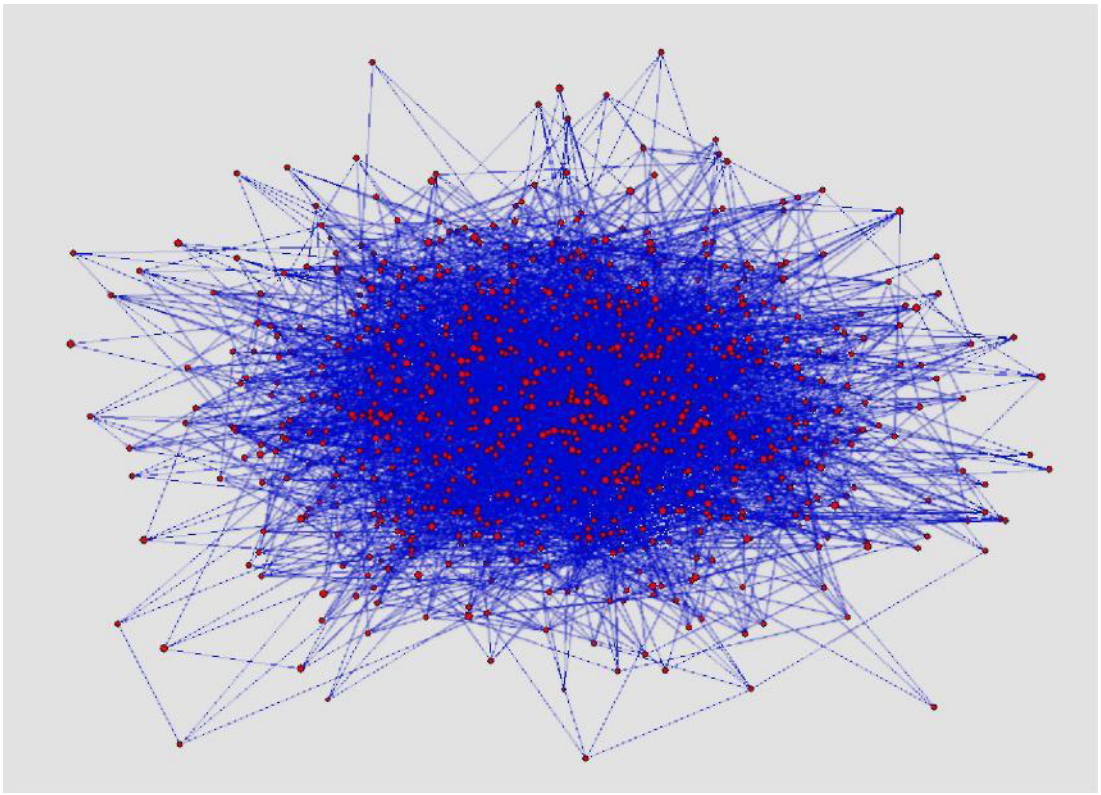


Рисунок 3.10 – Візуалізований фрагмент топології

Друга програма призначена для формування повного графа ІТКМ на основі обчислених прогнозованих топологічних характеристик і формування

його вектору топологічної уразливості. ПЗ створено для використання на супер-ЕОМ з використанням розподілених обчислювальних ресурсів. Програма написана в середовищі програмування Microsoft Visual Studio. Інтерфейсом взаємодії між процесами в додатку є MPI. В деяких випадках додатково використовувалося багатопотокове програмування. Для представлення графа в пам'яті обчислювальної системи використовувалося два підходи: нерозподілений (локальний, використовувалася бібліотека Boost Graph Library) і розподілений (Parallel Boost Graph Library).

Формат вихідних даних аналогічний першій програмі – текстовий файл, в якому в кожному рядку записаний ідентифікатор вузла, і через пробіл перераховані ідентифікатори суміжних з ним вузлів (топологія повного графа мережі). Другий вихідний файл – файл з вектором топологічної уразливості мережі.

У додатку А наведений фрагмент коду з файлу DistributedGraph_main.cpp та фрагмент коду з файлу aux_types.h.

3.5 Висновки

Розроблено методику формування топології ІТКМ, яка враховує основні топологічні характеристики доступною частини мережі і працює в умовах недостатньої репрезентативності вибірки вихідних даних. Запропонована методика складається з послідовності розроблених алгоритмів.

Створено алгоритм формування вихідних даних про топологію мережі (множини вершин і зв'язків між ними доступною частини мережі), який враховує обмеження зі збору даних і реалізований у вигляді розробленого програмного забезпечення.

Розроблено алгоритм формування повного графа мережі з урахуванням додавання недоступної частини на основі обчислених прогнозованих топологічних характеристик. Алгоритм реалізований у вигляді розробленого програмного забезпечення.

Введена оцінка топологічної уразливості мережі (вектор топологічної уразливості), що враховує такі параметри: середню довжину шляху мережі, коефіцієнт кластеризації мережі, середній ступінь зв'язності мережі і загальна кількість вузлів в мережі.

4 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ. ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ

Моделювання ЗПЗІ на великомасштабній ІТКМ є трудомістким завданням. Його рішення в прийнятні терміни і отримання актуальних результатів можливо тільки при використанні розподілених обчислювальних ресурсів. При проведенні експериментальних досліджень в даній роботі була використана супер-ЕОМ.

Експериментальні дослідження проводилися на двох фрагментах ІТКМ. Перший (фрагмент соціальної мережі «ВКонтакте») отримано в межах даної магістерської роботи (розділ 3), а другий (фрагмент з 16163521 вузла соціальної мережі «Facebook») отримано незалежно американськими вченими Maciej Kurant, Minas Gjoka і ін.

4.1 Розподілене моделювання загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Експериментальне дослідження ЗПЗІ в ІТКМ здійснювалося на основі імітаційної моделі, що детально розглянута у другому розділі роботи.

Імітаційна модель реалізована у вигляді розробленого програмного забезпечення на розподілену обчислювальну систему. Для реалізації паралельних обчислень на графі була використана бібліотека Parallel Boost Graph Library [7]. Бібліотека є вільно розповсюджуваної і за своїми функціональними можливостями не має альтернатив.

Parallel Boost Graph Library (PBGL) надає гнучку і ефективну реалізацію концепції графів. Входить до зібрання бібліотек boost, що розширюють функціональність C ++, які вільно поширюються за ліцензією Boost Software License разом з вихідним кодом.

Бібліотека дозволяє вибрати подання графа, тип даних і алгоритм з великого набору алгоритмів, серед яких:

- пошук в ширину;
- пошук в глибину;
- алгоритм Беллмана-Форда;
- алгоритм Дейкстри;
- алгоритм Прима;
- алгоритм Краскала;
- знаходження компонент зв'язності графа;
- задача про максимальний потік;
- зворотний алгоритм Катхілла-Маккі;
- алгоритм топологічної сортування тощо.

Розроблена програма створена для використання на супер-ЕОМ, загальна характеристика якого представлена в таблиці 4.1.

Таблиця 4.1 – Загальна характеристика супер-ЕОМ

Пікова продуктивність	4771 Tflops / s
Продуктивність на Linpack	3756 Tflops / s (78.7% від пікової)
Кількість процесорів / ядер в системі	128/512
Модель процесора	Intel Xeon 5345 2.33 GHz
Об’єм оперативної пам’яті	512 Гбайт
Дискова пам'ять вузлів	10Тб
Кількість стійок / обчислювальних	4/2
Кількість обчислювальних вузлів	64
Виробник	Т-Платформи

Групи обчислювальних вузлів: student (4 вузли, 2 процесора, ОП 8 Гб, HDD 160 Гб), short (14 вузлів, 2 процесора, ОП 8 Гб, HDD 160 Гб), long (14 вузлів, 2 процесора, ОП 8 Гб, HDD 160 Гб), work (32 вузла, 2 процесора, ОП 8 Гб, HDD 160 Гб).

Всі вузли в супер-ЕОМ пов’язані двома незалежними мережами: системна мережа: InfiniBand DDR (Fat Tree: 6x12 порту; латентність на рівні

MPI: 1.3-1.95 мкс; швидкість обміну на рівні MPI: 1540 Мбайт/с) і допоміжна/ керуюча мережа: GigabitEthernet (2x (44 портів + 4x10G)).

Програмне забезпечення:

- Операційна система Suse Linux Enterprise Server v 10 sp 1
- Система черги завдань Torque
- Система моніторингу вузлів Ganglia
- Компілятори GNU gcc, Intel C / C ++ Compiler.
- Дод. Бібліотеки MPI (mpich), ANSYS, ScaLAPACK, lapack, blas

Інфраструктура суперкомп'ютера. Суперкомп'ютер має унікальну інформаційно-обчислювальної та інженерною інфраструктурою, необхідною для надійної цілодобової роботи комплексу. Розроблене ПЗ написано в середовищі програмування Microsoft Visual Studio. Інтерфейсом взаємодії між процесами в додатку є MPI. У деяких випадках додатково використовувалося багатопотокове програмування. Для представлення графа в пам'яті обчислювальної системи використовувався розподілений підхід з використанням бібліотеки Parallel Boost Graph Library.

Формат вхідних даних – текстовий файл, в якому в кожному рядку записаний ідентифікатор вузла, і через пробіл перераховані ідентифікатори суміжних з ним вузлів (топологія повного графа мережі). У вихідному файлі фіксуються дані про динаміку ЗПЗІ, представлені списками атакуючих і захищених вузлів за кожен квант часу.

У додатку А наведено частину коду програми

4.2 Аналіз результатів експериментальних досліджень

4.2.1 Аналіз результатів моделювання загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Запропонований алгоритм розподіленого моделювання був апробований на двох представлених вище топологічних фрагментах мереж, після застосування до них алгоритму формування повного графа мережі.

Експерименти проводилися з різними початковими умовами. Спочатку було проаналізовано вплив параметрів β і γ на характер процесу, результати експериментів наведені на рисунках 4.1 та 4.2 («ВКонтакте»).

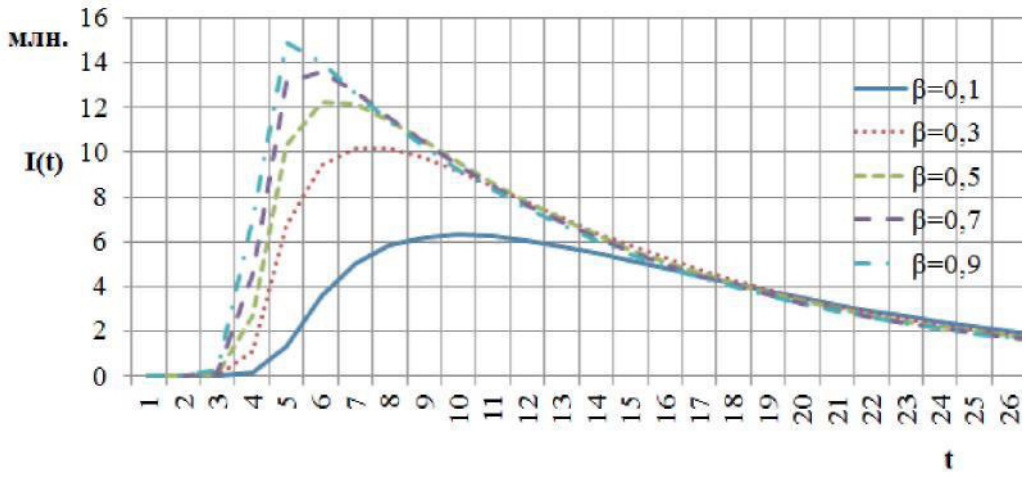


Рисунок 4.1 – Результати моделювання з параметрами γ = 0,1, $I_0 = 1$, $R_0 = 0$

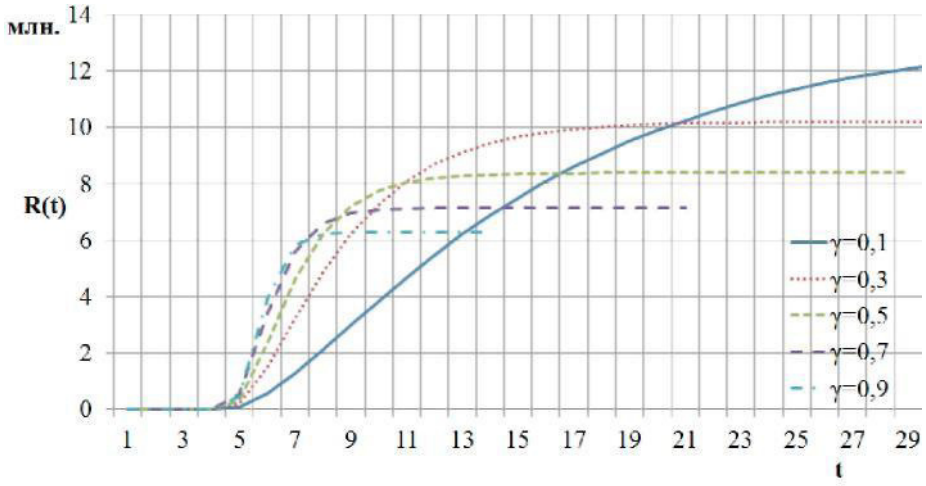


Рисунок 4.2 – Результати моделювання з параметрами β = 0,2, $I_0 = 1$, $R_0 = 0$

У ході роботи в другому розділі була отримана аналітична модель ЗПЗІ в ІТКМ. В рамках даної моделі передбачені два випадки: β ≠ γ та β = γ, тому при моделюванні використовувалися наступні окремі випадки: β = 0,2 та γ=0,8, β = 0,5 та γ=0,5. Кількість спочатку атакуючих вузлів I_0, розглядалося виходячи з того факту, що це може бути одна людина, або декілька. Як декількох розповсюджувачів вибиралося близько 0,1% вузлів випадковим чином. При розгляді такої умови як кількість спочатку захищених вузлів R_0, виходимо з таких міркувань. По-перше, таких вузлів може і не бути, по-друге, їх може бути достатня кількість (розглядалося 25% від загальної кількості вузлів в мережі), і, по-третє, такі вузли складають основну частину мережі

(розглядалося 75% від загального кількості вузлів в мережі). Вузли, схильні до атаки (S_0), визначаються: $S_0 = N - I_0 - R_0$, де N – загальна кількість вузлів в мережі.

Графіки результатів проведеного моделювання поширення забороненої інформації на топологічному фрагменті соціальної мережі «ВКонтакте» наведені на рисунках 4.4-4.15. На рисунку 4.3 представлена загальна легенда.

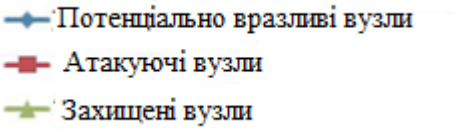


Рисунок 4.3 – Легенда

Експеримент 1 (рисунок 4.4): $\varphi = 200$, $\beta = 0{,}2$, $\gamma = 0{,}8$, $I_0 = 1$, $R_0 = 0$

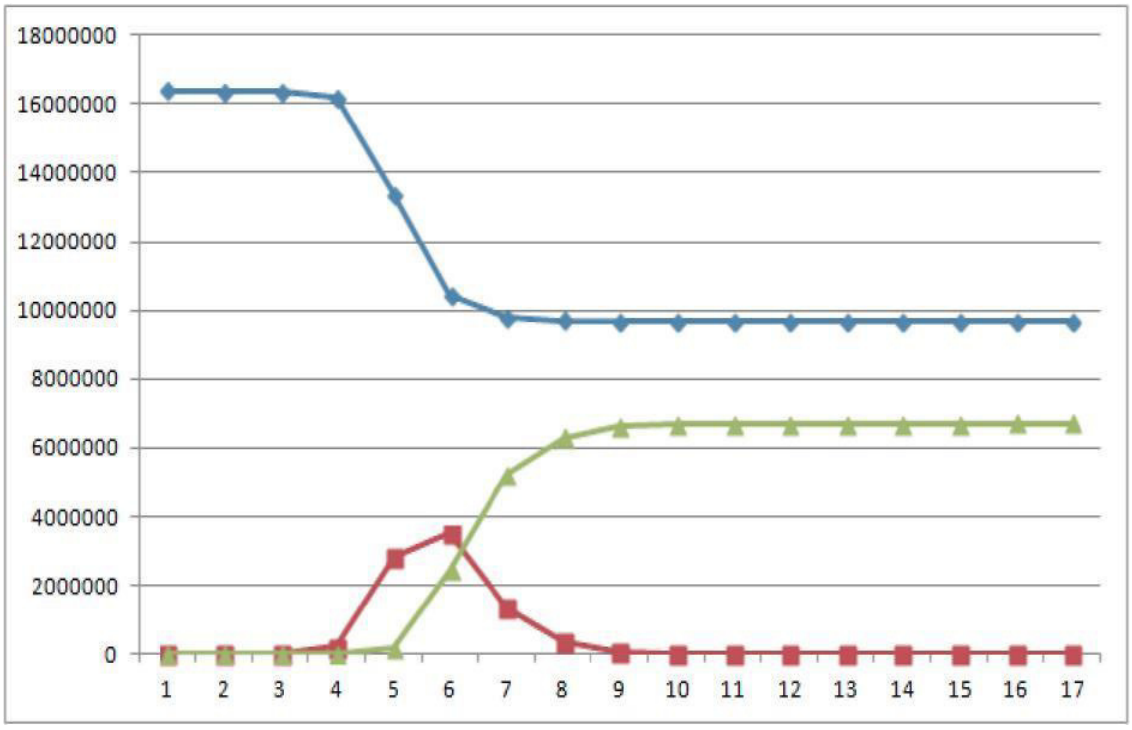


Рисунок 4.4 – Результати експерименту 1

Експеримент 2 (рисунок 4.5): $\varphi = 200$, $\beta = 0{,}2$, $\gamma = 0{,}8$, $I_0 = 1$, $R_0 = 0{,}25N$.

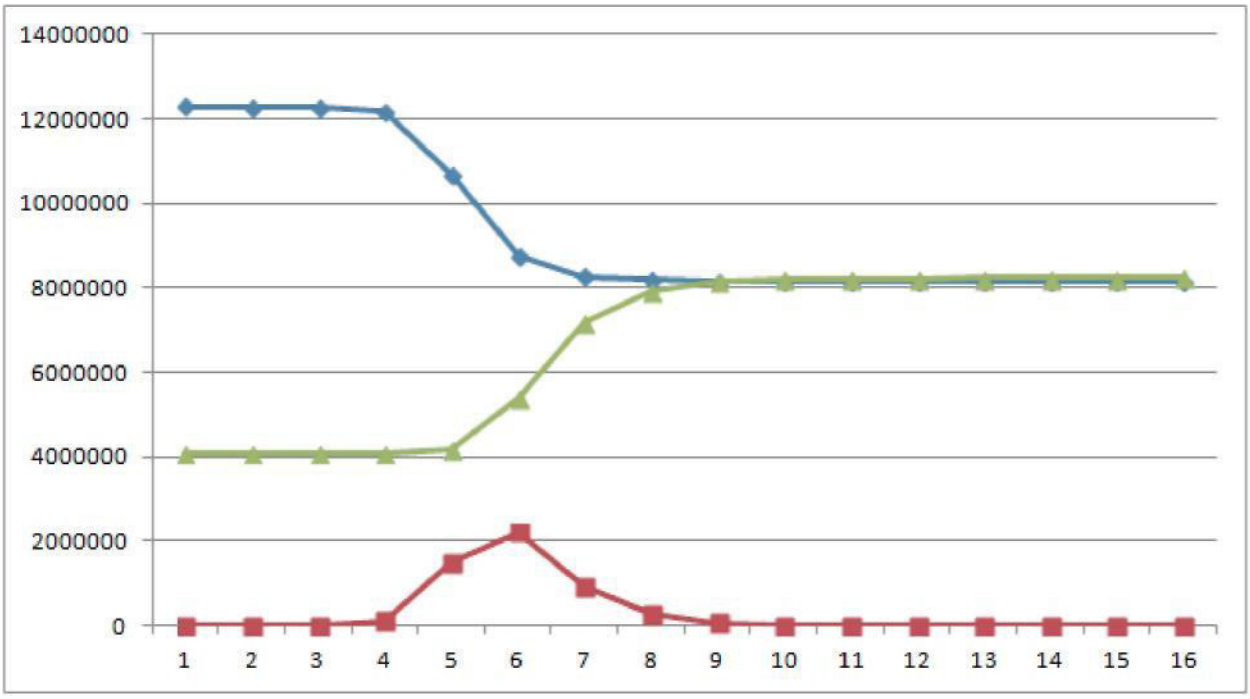


Рисунок 4.5 – Результати експерименту 2

Експеримент 3 (рисунок 4.6): $\varphi = 200$, $\beta = 0{,}2$, $\gamma = 0{,}8$, $I_0 = 1$, $R_0 = 0{,}75N$.

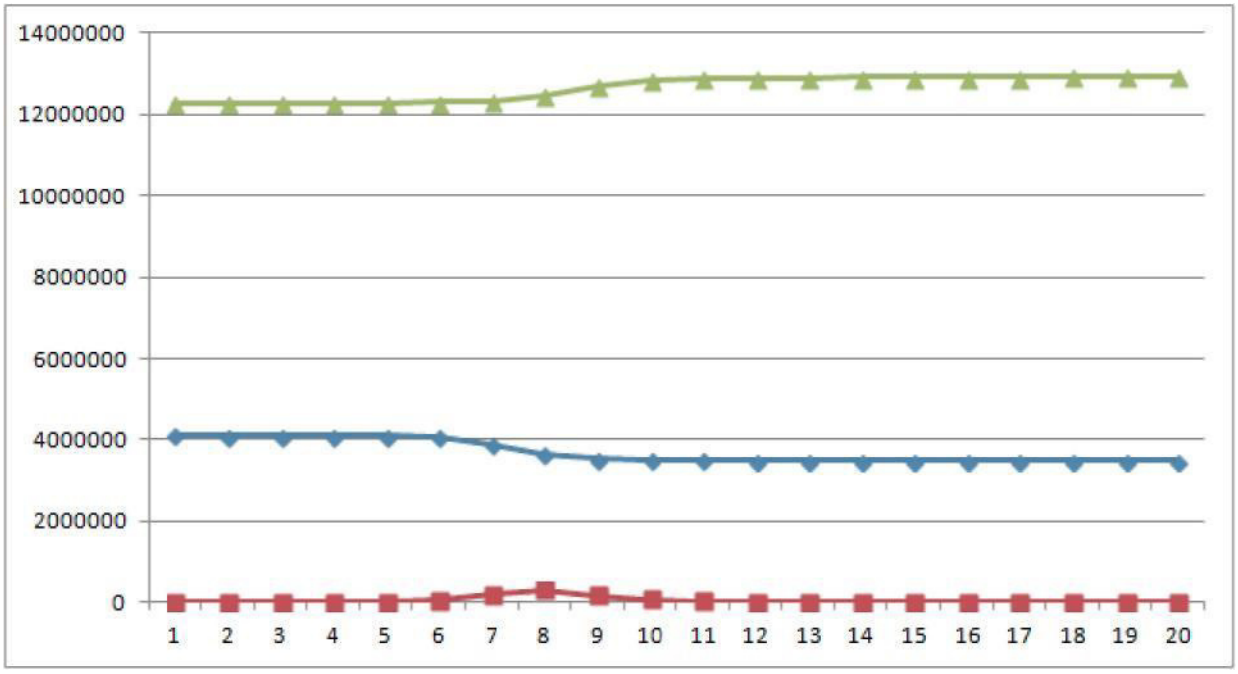


Рисунок 4.6 – Результати експерименту 3

За результатами перших трьох експериментів можна зробити наступні висновки:

1. Уже один атакуючий вузол може викликати «спалах» в мережі, навіть при великому значенні ймовірності захисту.

2. З ростом кількості спочатку захищених вузлів, максимальне число атакуючих вузлів падає.

Експеримент 4 (рисунок 4.7): $\varphi = 200$, $\beta = 0{,}2$, $\gamma = 0{,}8$, $I_0 = 0{,}001N$, $R_0 = 0$.

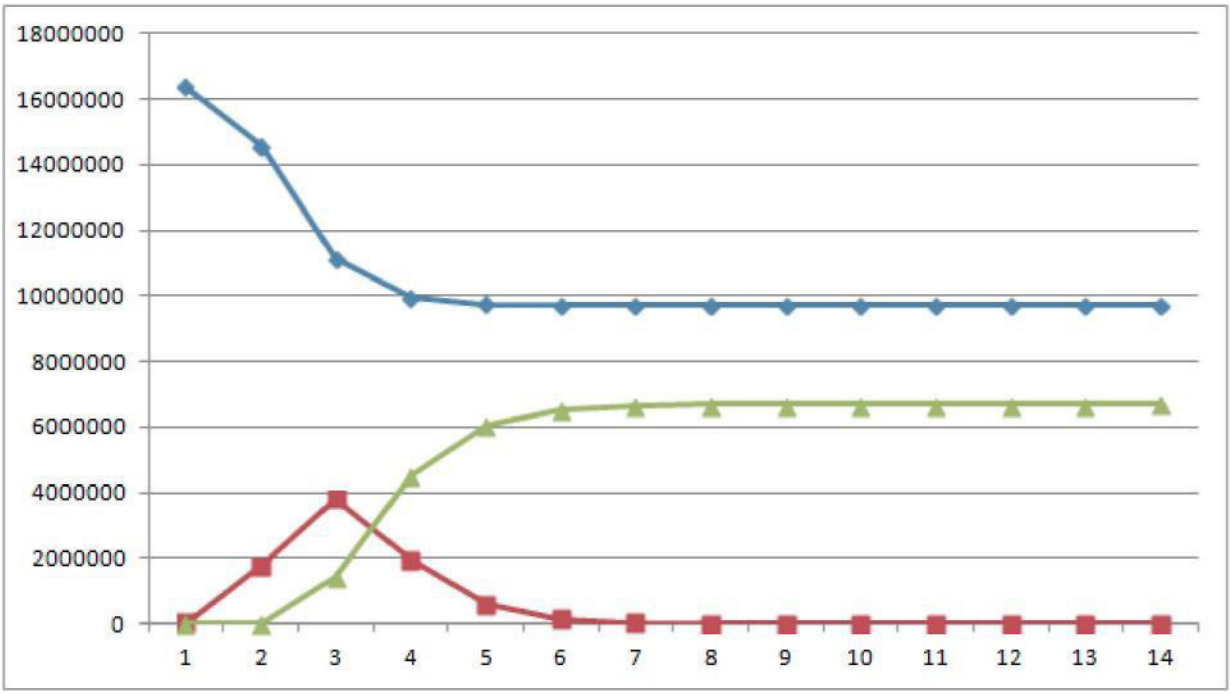


Рисунок 4.7 – Результати експерименту 4

Експеримент 5 (рисунок 4.8): $\varphi = 200$, $\beta = 0{,}2$, $\gamma = 0{,}8$, $I_0 = 0{,}001N$, $R_0 = 0{,}25N$

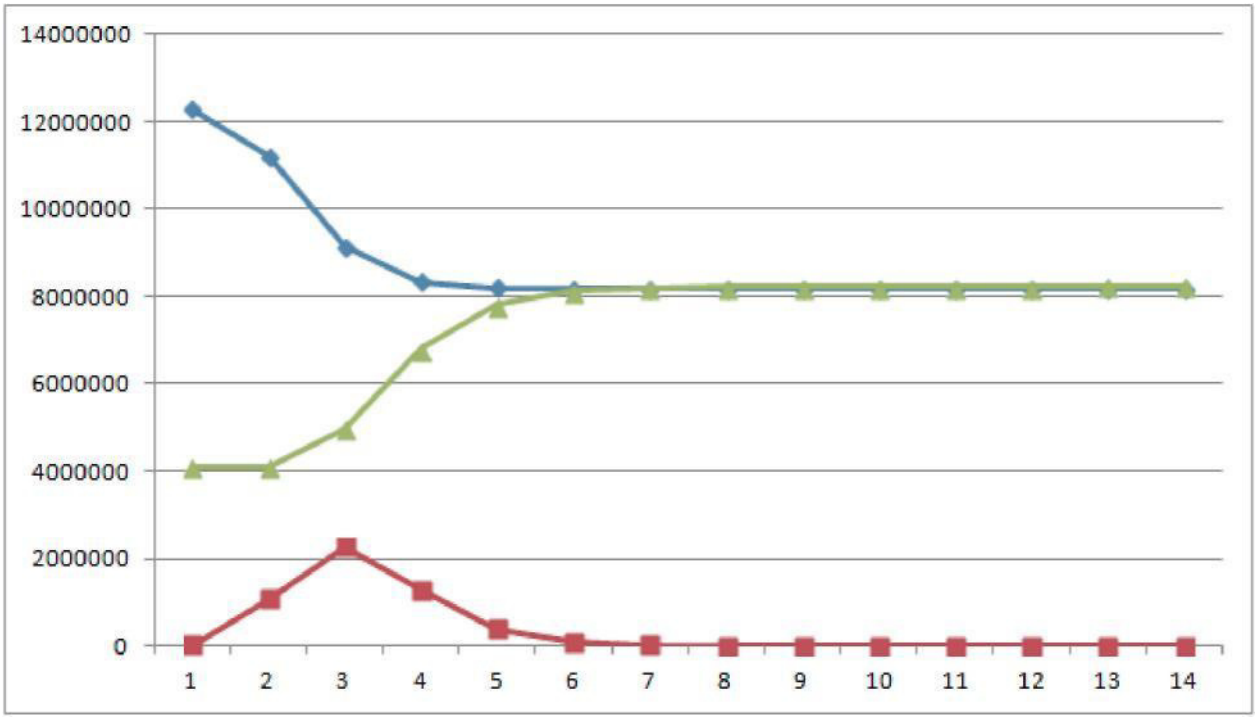
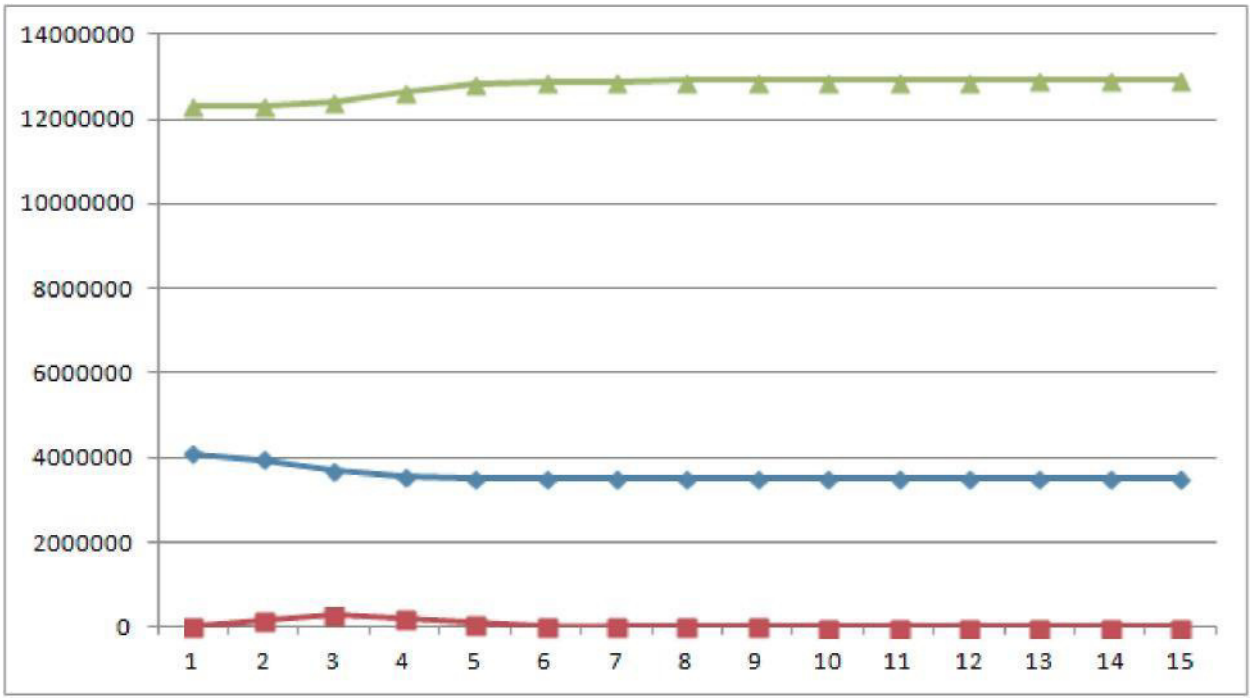


Рисунок 4.8 – Результати експерименту 5

Експеримент 6 (рисунок 4.9): $\varphi = 200, \beta = 0{,}2, \gamma = 0{,}8, I_0 = 0{,}001N, R_0 = 0{,}75N$



Рисунокк 4.9 – Результати експерименту 6

За результатами експериментів 4-6 можна зробити наступні висновки:

1. При зростанні кількості спочатку атакуючих вузлів спостерігається «спалах» вже на перших етапах (1-6 тіки).

2. Параметр R_0 впливає на пік також як і в 1-3 експериментах.

Експеримент 7 (рисунок 4.10): $\varphi = 200, \beta = 0{,}5, \gamma = 0{,}5, I_0 = 1, R_0 = 0.$

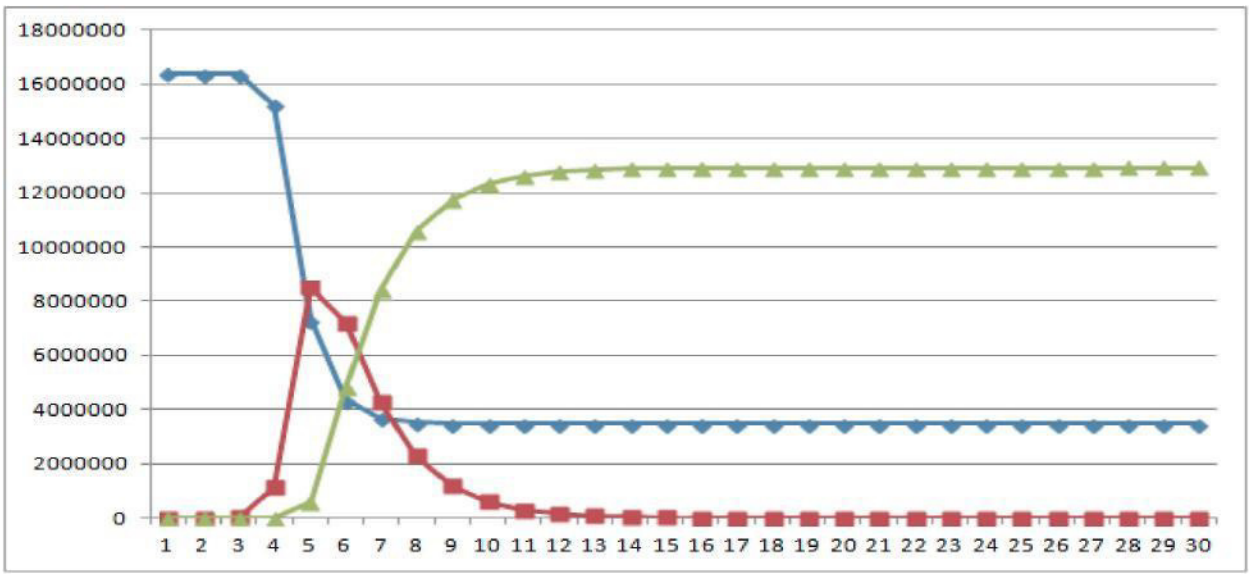


Рисунок 4.10 – Результати експерименту 7

Експеримент 8 (рисунок 4.11): $\varphi = 200, \beta = 0{,}5, \gamma = 0{,}5, I_0 = 1, R_0 = 0{,}25N.$

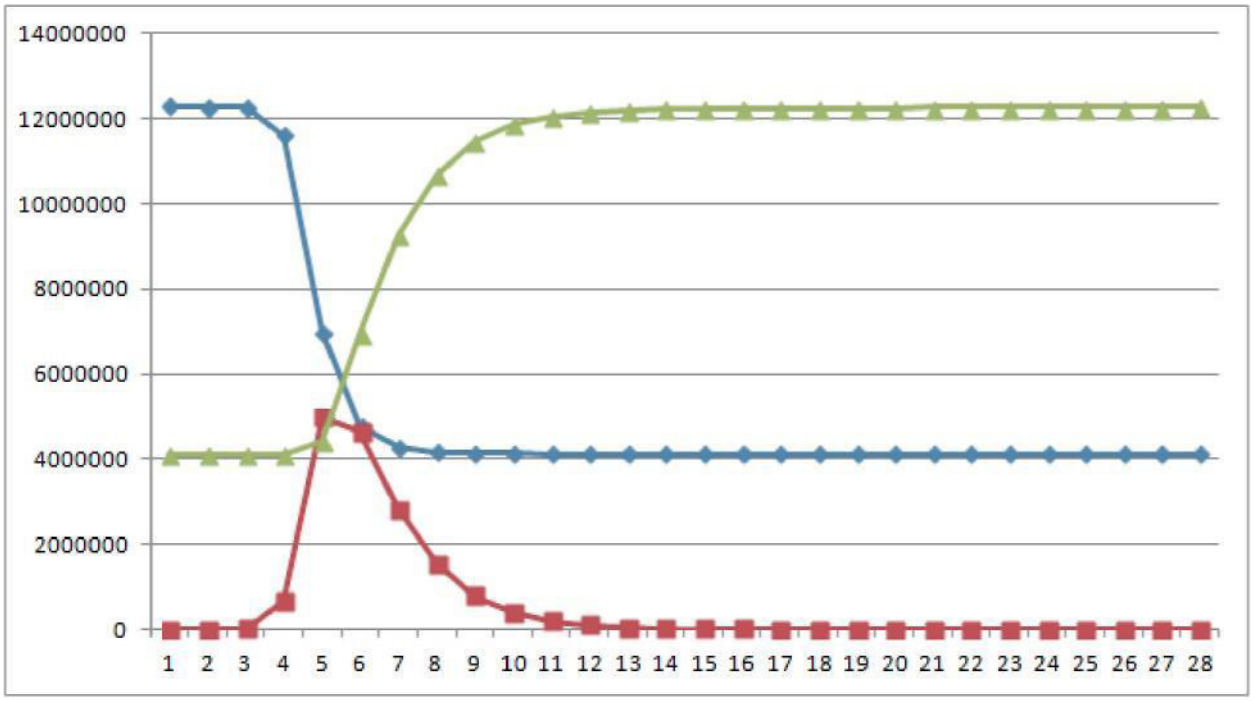


Рисунок 4.11 – Результати експерименту 8

Експеримент 9 (рисунок 4.12): $\varphi = 200$, $\beta = 0{,}5$, $\gamma = 0{,}5$, $I_0 = 1$, $R_0 = 0{,}75N$.

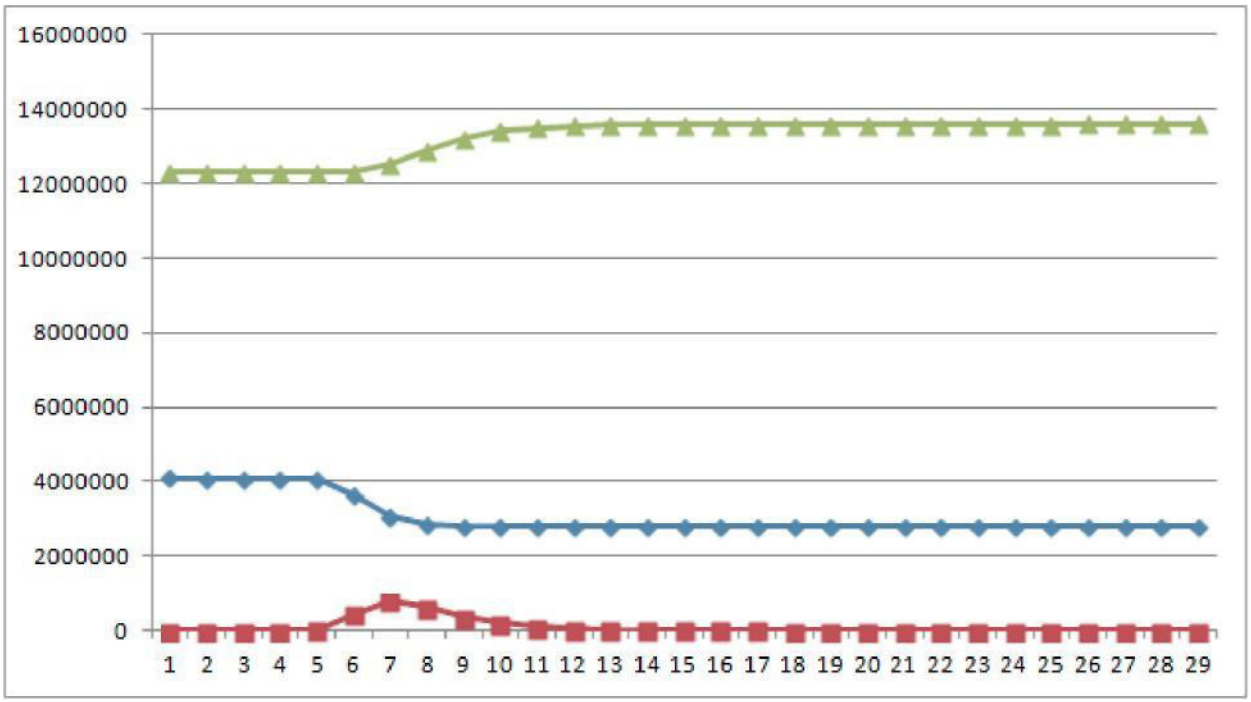


Рисунок 4.12 – Результати експерименту 9

За результатами експериментів 7-9 можна зробити наступні висновки:

1. При зміні параметрів β і γ різко змінюється характер ЗПЗІ.

2. При збільшенні ймовірності атаки і зменшенні ймовірності захисту загроза приймає глобальний характер навіть при одному первісному атакуючому вузлі (пік атакуючих вузлів збільшується більш ніж в два рази).

3. Процес ЗПЗІ збільшується за часом в два рази (з 15 тиків до 30).

4. Вплив числа спочатку захищених вузлів залишається таким же, як і в експериментах 1-3.

Експеримент 10 (рисунок 4.13): $\varphi = 200$, $\beta = 0{,}5$, $\gamma = 0{,}5$, $I_0 = 0{,}001N$, R_0=0.

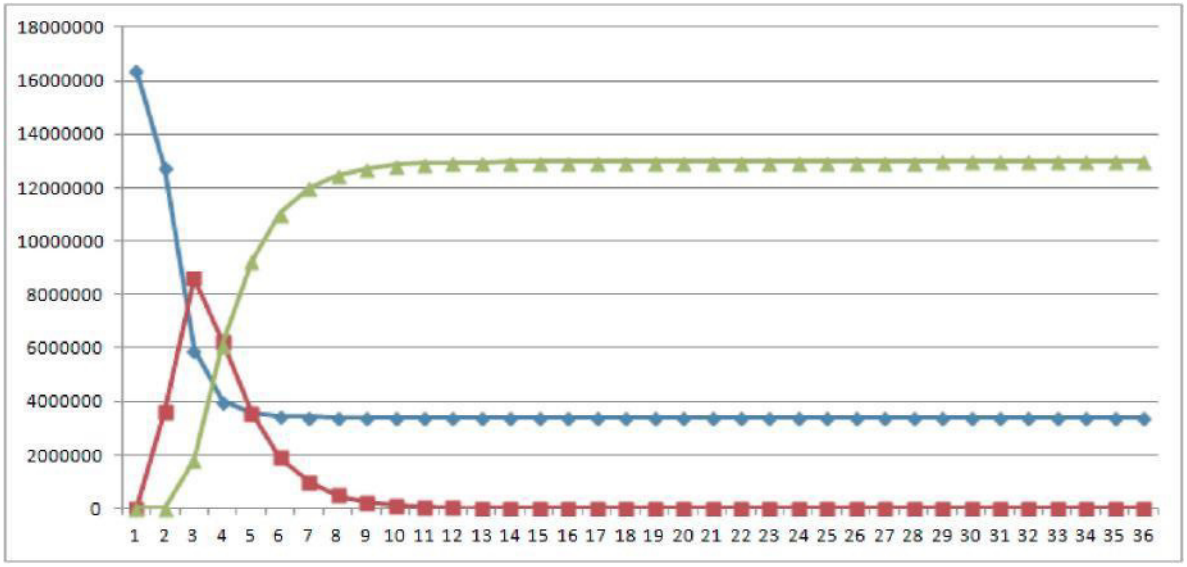


Рисунок 4.13 – Результати експерименту 10

Експеримент 11 (рисунок 4.14): φ=200, $\beta = 0{,}5$, $\gamma = 0{,}5$, $I_0 = 0{,}001N$, $R_0 = 0{,}25N$

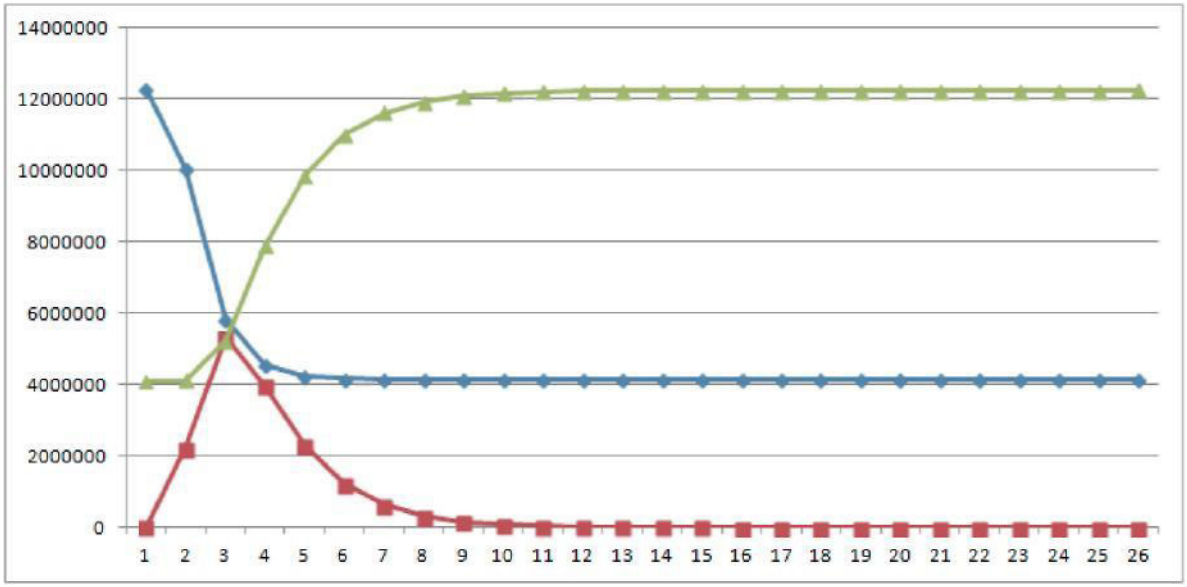


Рисунок 4.14 – Результати експерименту 11

Експеримент 12 (рисунок 4.15): $\varphi = 200$, $\beta = 0{,}5$, $\gamma = 0{,}5$, $I_0 = 0{,}001N$, R_0=$0{,}75N$

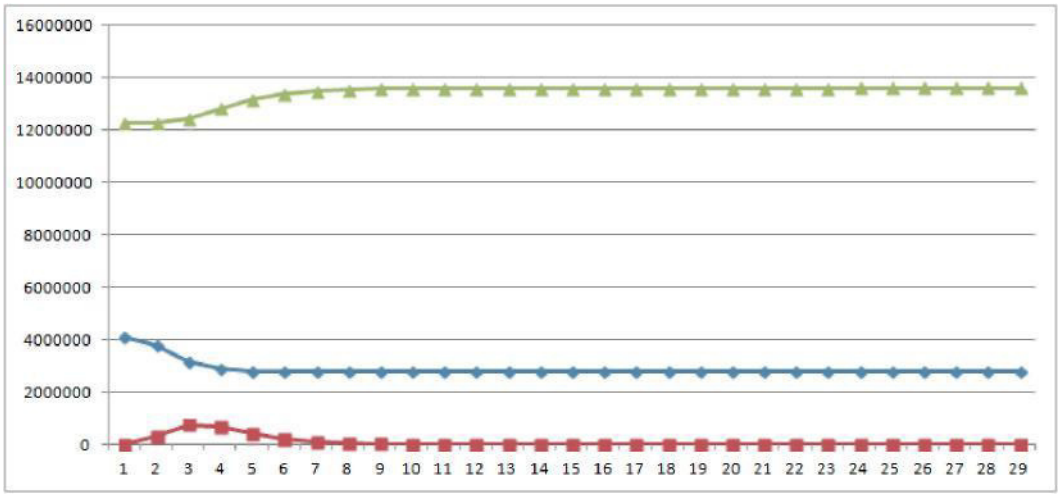


Рисунок 4.15 – Результати експерименту 12

За результатами експериментів 10-12 можна дійти такого висновку: в цілому, тенденції, що простежуються в попередніх експериментах, не змінюють свій характер.

Характер процесу поширення забороненої інформації у мережі Facebook такий же, як і на мережі ВКонтакте. Це факт вказує на те, що різні соціальні мережі мають схожу топологію.

4.2.2 Аналіз результатів експериментальних досліджень топології інформаційно-телекомунікаційних мереж

В ході експериментальних досліджень були отримані результати, що стосуються топології ІТКМ.

У таблиці 4.2 [10] представлені основні топологічні характеристики для випадкових графів і двох видів складних мереж (complex networks), які були розглянуті в першому розділі магістерської роботи.

Після проведення експериментів можна порівняти результати з представленими даними і зробити висновок про належність соціальних мереж до певного типу, виходячи з отриманих топологічних характеристик. Знаючи топологічні характеристики ІТКМ, можна генерувати на їх основі мережі з такими ж параметрами будь-яких масштабів, що допоможе вивчати процеси, що відбуваються в них з використанням моделювання.

Таблиця 4.2 – Основні топологічні характеристики

Параметр	Випадкові графи	Small world	Scale-Free
Середня довжина шляху L	$\frac{\ln N}{\ln k}$	$\frac{\ln N}{\ln k}$	$m = 1 : l \sim \ln N$; $m \geq 2 : \ l_{BA}^{a>3} \approx \ln N$; $l_{BA}^{a=3} \approx \ln N / \ln lnN$; $l_{BA}^{2<a<3} \approx \ln \ln N$.
Кластерний коефіцієнт C	$\frac{k}{N}$	$C_{p\to 1} \sim \frac{k}{N}$, $C_{p>0} >> C_{p\to 1}$	$5\frac{k}{N}$
Розподіл ступенів вершин	Закон Пуассона	Закон Пуассона	Степеневий закон

Розподіл ступенів зв’язності вузлів

Розглянемо результати обчислення середнього ступеня зв’язності за топологичічним фрагментом мережі ВКонтакте. Експерименти проводилися з використанням двох підходів. При першому підході використовувався алгоритм, що враховує всі вузли. Результат зображений на рисунку 4.16, на ньому показано розподіл ступенів зв’язності вузлів. Для інформативності дані представлені на логарифмованій шкалі. При цьому підході середня ступінь зв’язності на всіх вузлах вийшла рівною 8,387. При другому підході враховувалися тільки відкриті вузли. Розподіл показано на рисунку 4.17. Середній ступінь зв’язності склала 631,685.

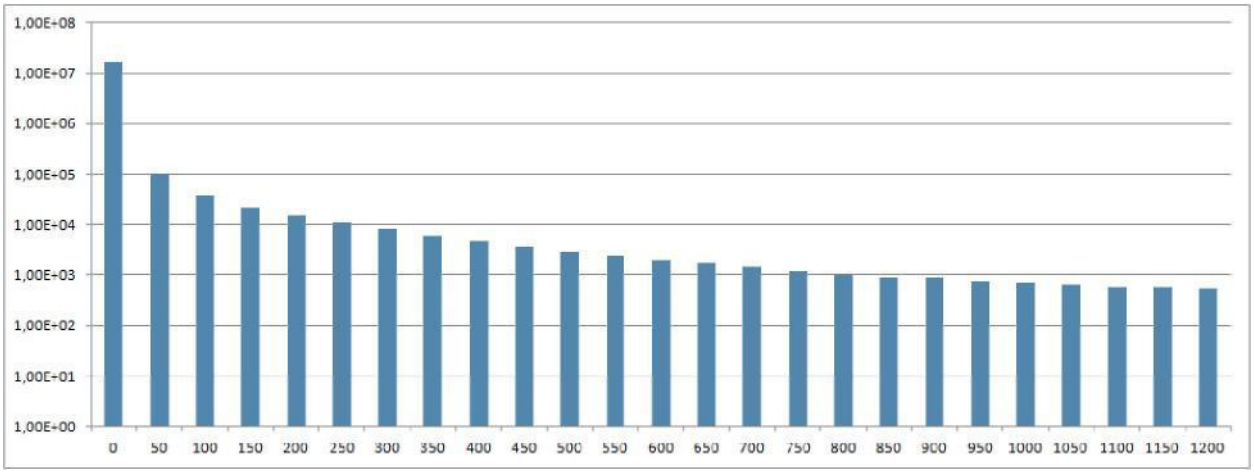


Рисунок 4.16 – Розподіл ступенів звязності по всіх вузлах (ВКонтакті)

Підхід, що враховує тільки відкриті вузли, є більш коректним. Обґрунтовується це тим, що за закритими вузлів у нас немає повної

інформації і, отже, ступінь зв’язності у них маленька, також їх на два порядки більше, ніж відкритих, тому вони значно змінюють характер розподілу.

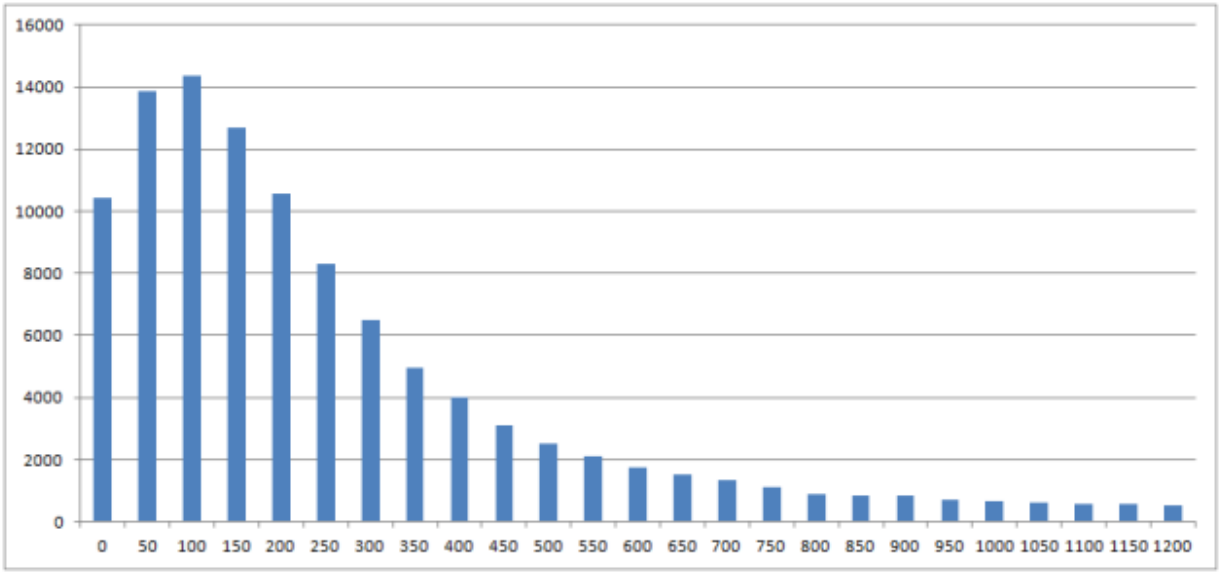


Рисунок 4.17 – Розподіл ступенів зв’язності за відкритими вузлів (ВКонтакте)

В ході аналізу даних по розподілу середнього ступеня зв’язності були отримані наступні результати. Можна бачити, що представлений розподіл, показаний на рисунку 4.4, не можна апроксимувати ні пуассоновским, ні степеневим розподілом. Добре підходить гамма-розподіл, щільність ймовірності якого має вигляд:

$$f(x) = \begin{cases} x^{k-1} \cdot \frac{e^{-x/\theta}}{\Gamma(k)\cdot\theta}, & x \geq 0 \\ 0, & x < 0 \end{cases} \qquad (4.1)$$

де $\Gamma(k)$ – гамма-функція Ейлера.

Для отриманих експериментальних даних за допомогою програмного продукту Microsoft Office Excel були підраховані математичне сподівання і мода. Далі, використовуючи формули математичного сподівання і моди (формули (4.2) і (4.3) відповідно) для гамма-розподілу, були обчислені значення параметрів k та θ. Після підстановки цих значень в формулу 4.1, був отриманий апроксимуючий розподіл, представлений на рисунку 4.18. Похибка апроксимації дорівнює $2{,}2 \cdot 10^{-4}$, що становить приблизно 10%. Слід зазначити,

що до висновку про те, що розподіл ступенів зв’язності вузлів соціальної мережі відмінно від пуасонівского і степеневого, приходили і інші дослідники.

$$M = k\theta \tag{4.2}$$

$$Mo = (k-1)\cdot\theta \tag{4.3}$$

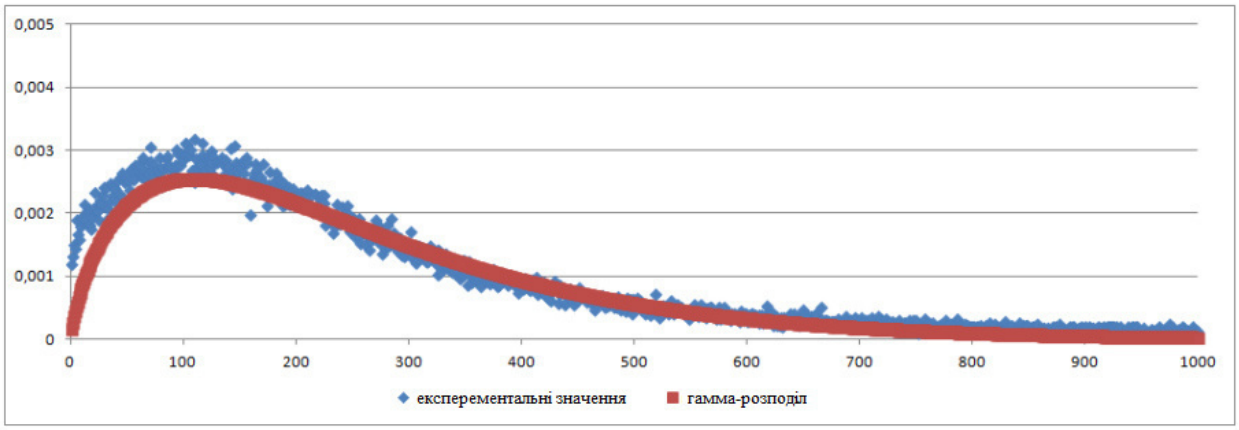


Рисунок 4.18 – Експериментальний та апроксимуючий розподіл середнього ступеня зв’язності (ВКонтакті)

Розглянемо результати обчислення середнього ступеня зв’язності за топологічним зрізом соціальної мережі Facebook. Експерименти проводилися також з використання двох підходів. При першому підході середня ступінь зв’язності по всіх вузлах вийшла рівною 4,15377. Результат представлений на рисунку 4.19. При другому середня ступінь зв’язності склала 295,677. Розподіл показано на рисунку 4.20.

Аналогічно з мережею ВКонтакті отримано апроксимуючий розподіл для зрізу Facebook, яке представлено на рисунку 4.21. Похибка апроксимації вийшла рівною $2 \cdot 10^{-4}$ (≈10%).

Аналізуючи результати моделювання розподілу ступенів зв’язності за двома мережами, можна зробити наступні висновки. В цілому характер розподілу однаковий для обох зрізів. А середні значення у мережі Facebook в два рази менше, ніж у мережі ВКонтакте. Цей факт вказує на те, що російська аудиторія більш комунікабельна, ніж користувачі соціальних мереж всієї планети в цілому.

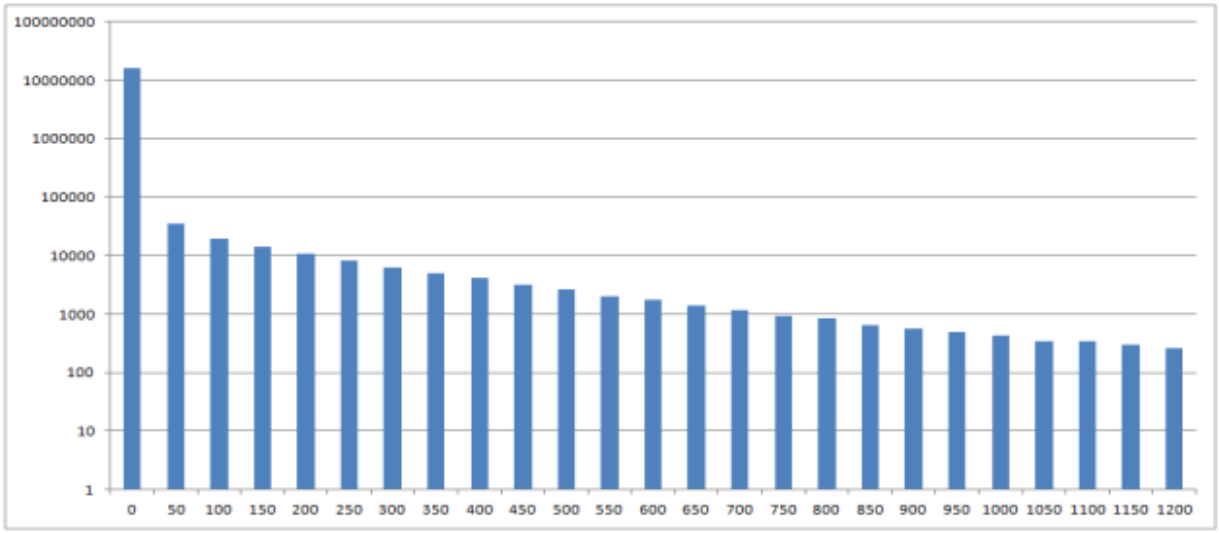


Рисунок 4.19 – Розподіл ступенів зв’язності по всіх вузлах (Facebook)

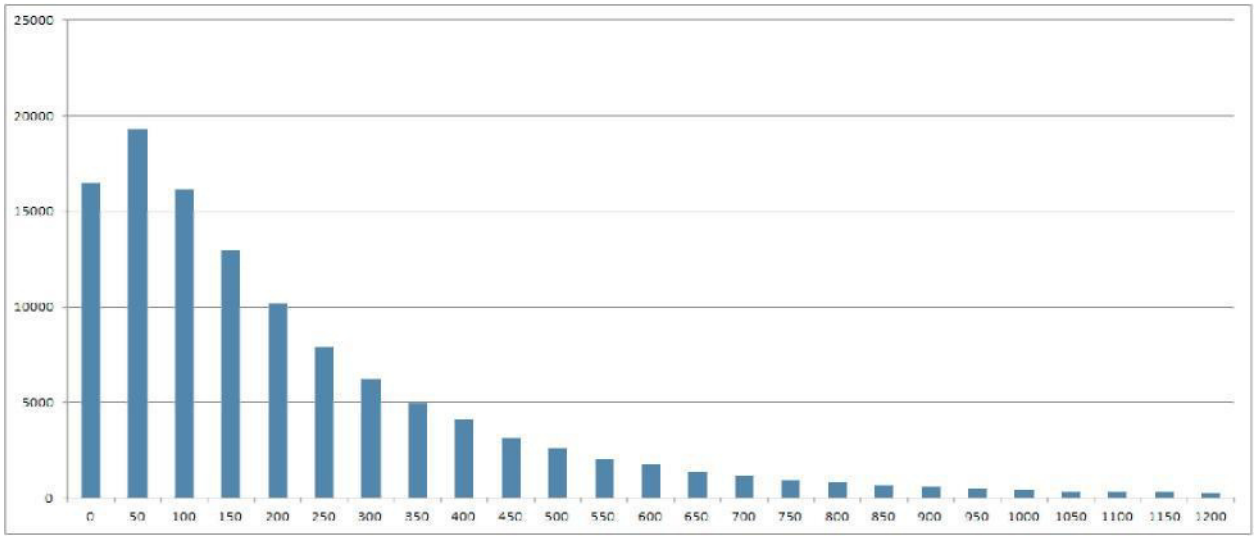


Рисунок 4.20 – Розподіл ступенів зв’язності за відкритими вузлами (Facebook)

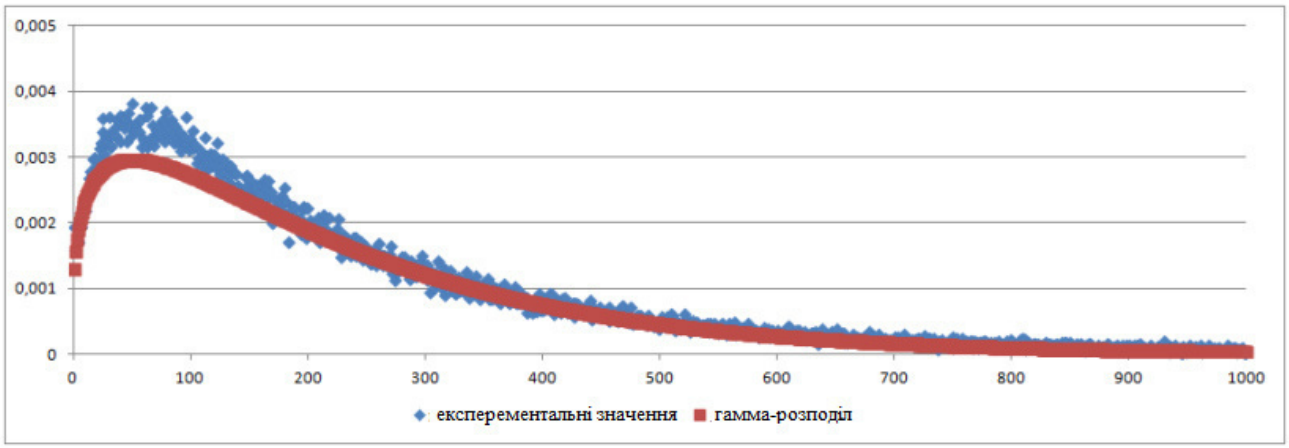


Рисунок 4.21 – Експериментальний і апроксимуючий розподіл середнього ступеня зв’язності (Facebook)

Кластерний коефіцієнт мережі

Розглянемо результати обчислення кластерного коефіцієнта за топологічним фрагментом мережі ВКонтакті. Значення середнього кластерного коефіцієнта мережі вийшло рівним 0,048087. Докладні дані у вигляді діапазонів значення коефіцієнта і кількості вузлів, що потрапляють в відповідні інтервали, наведені в таблиці 4.3. На рисунку 4.22 зображено розподіл значень кластерного коефіцієнта (на логарифмічній шкалі).

Таблиця 4.3 – Кластерний коефіцієнт (ВКонтакті)

Кластерний коефіцієнт (інтервал)	Кількість вузлів
[0; 0,1)	104810
[0,1; 0,2)	9094
[0,2; 0,3)	2423
[0,3; 0,4)	1198
[0,4; 0,5)	587
[0,5; 0,6)	332
[0,6; 0,7)	188
[0,7; 0,8)	67
[0,8; 0,9)	39
[0,9; 1)	8
1	88

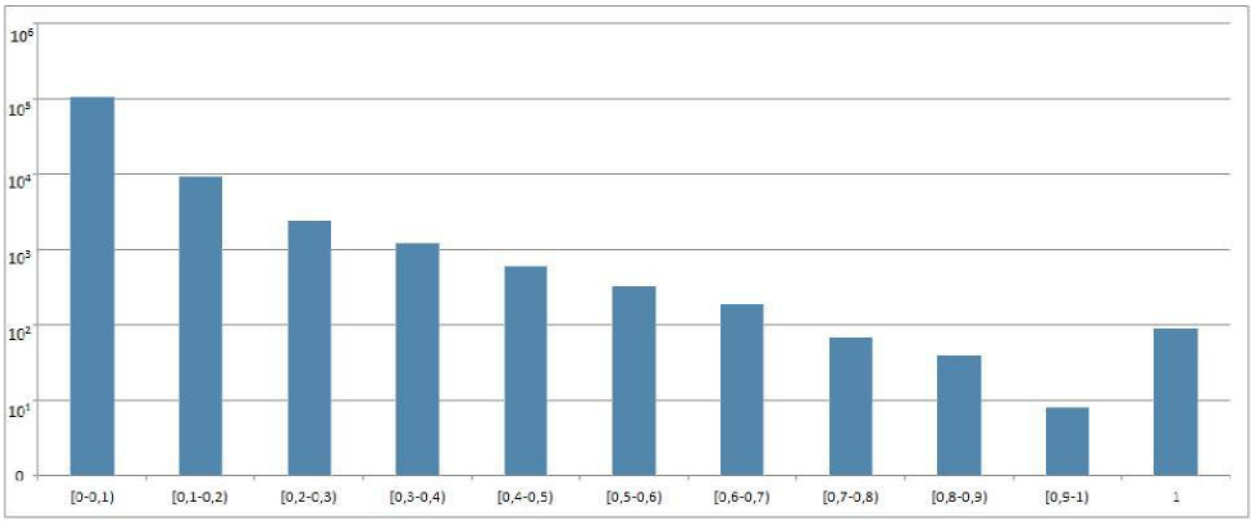


Рисунок 4.22 – Розподіл кластерного коефіцієнта (ВКонтакті)

Аналізуючи отримані дані, можна зробити наступні висновки. Більшість вузлів мають кластерний коефіцієнт в інтервалі [0; 0,1), що свідчить про низьку ступінь кластеризації розглянутого фрагмента мережі. Проте, присутня група вузлів з коефіцієнтом рівним одиниці, яка вибивається із залежності – чим більше значення кластерного коефіцієнта, тим менше вузлів. Фізичний зміст цього явища можна пояснити наступним чином. У нашій вибірці ми захопили групи користувачів, які підтримують тісні зв'язки між собою, наприклад, в зв'язку із сферою діяльності. Захоплення, в свою чергу, таких груп визначається використаним методом вибірки – обходом в ширину.

Розглянемо результати обчислення кластерного коефіцієнта за топологічним фрагментом мережі Facebook. Значення середнього кластерного коефіцієнта мережі вийшло рівним 0,040362. Це трохи менше, ніж за зрізом мережі ВКонтакті (0,048087). Докладні дані у вигляді діапазонів значення коефіцієнта і кількості вузлів, що потрапляють у відповідні інтервали, наведені в таблиці 4.4. На рисунку 4.23 представлено розподіл значень кластерного коефіцієнта (на логарифмічній шкалі).

Таблиця 4.4 – Кластерний коефіцієнт (Facebook)

Кластерний коефіцієнт (інтервал)	Кількість вузлів
[0; 0,1)	105481
[0,1; 0,2)	8006
[0,2; 0,3)	2738
[0,3; 0,4)	1155
[0,4; 0,5)	518
[0,5; 0,6)	306
[0,6; 0,7)	178
[0,7; 0,8)	49
[0,8; 0,9)	44
[0,9; 1)	17
1	122

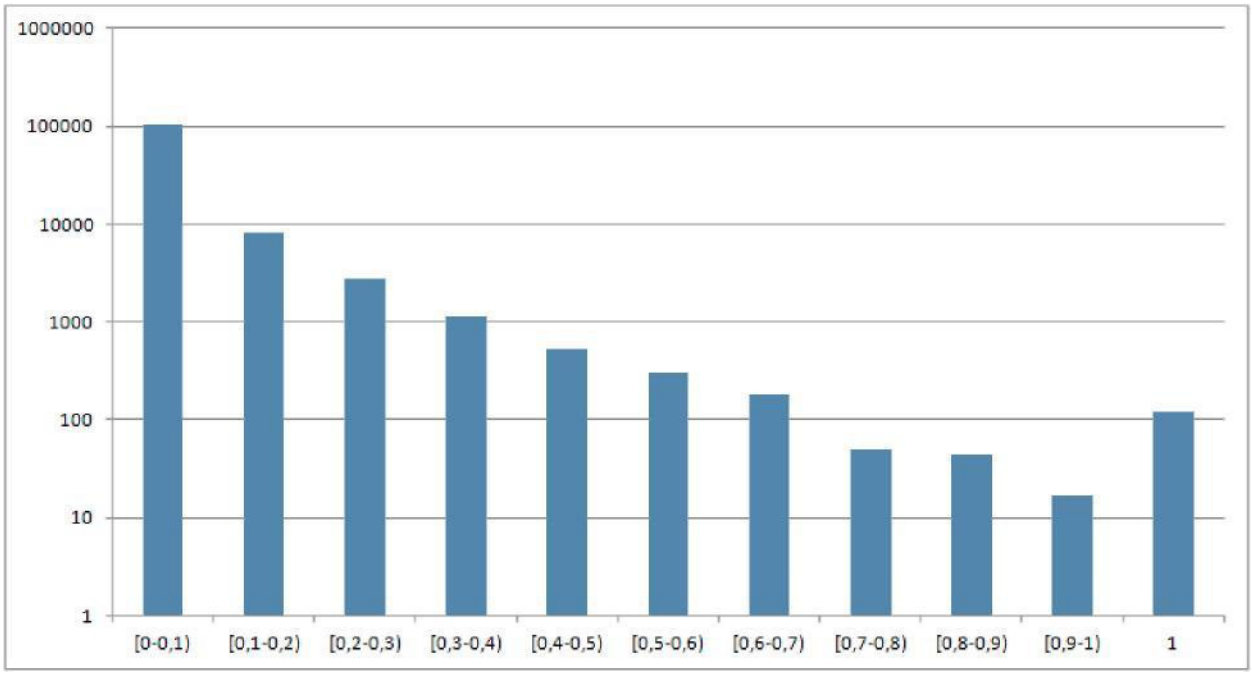


Рисунок 4.23 – Розподіл кластерного коефіцієнта (Facebook)

Результати моделювання на зрізі Facebook аналогічні результатам по мережі ВКонтакті, отже, характер кластеризації для розглянутих мереж однаковий. Якщо ми застосуємо формули для обчислення кластерного коефіцієнта для різних типів мереж з таблиці 4.2, то побачимо, що жодна з них не дає правильного результату для наших випадків.

Середня довжина шляху мережі

Значення середньої довжини шляху для «ВКонтакте» вийшло рівним 3,32, а для «Facebook» – 4,48. Міланський університет і Facebook, проводячи спільне дослідження теорії шести рукостискань, отримали значення 4,74. Розбіжність в значеннях пояснюється кількістю вузлів у вибірці. Для «ВКонтакті» також були проведені незалежні дослідження за підрахунком середньої довжини шляху. Ланцюжки виявляються коротше (3-4 людини), що відповідає отриманим даними в цій роботі. Таке значення пояснюється тим, що аудиторія «ВКонтакті» обмежена (Росія і країни СНД). Наведені дані дозволяють нам при дослідженні великомасштабних ІТКМ використовувати фіксоване значення середньої довжини шляху.

Порівнюючи отримані результати з топологічним характеристиками і дані в таблиці 4.2, можна стверджувати, що представлені зрізи не належать до

жодного з типів складних мереж. У даному випадку можна говорити про новий тип, який володіє отриманими властивостями і є представниками топології інформаційних зв’язків абонентів ІТКМ.

4.3 Особливості реалізації автоматизованої системи протидії загрозі поширення забороненоїінформації

При наявності адміністративного ресурсу можна реалізувати автоматизовану систему протидії загрозі поширення забороненої інформації. Узагальнений алгоритм роботи такої системи представлений на рисунку 4.24. Розглянуті функції реалізуються за допомогою типових засобів.

Крок 1. Введення даних – типове повідомлення, що містить інформацію, заборонену до поширення. База даних таких повідомлень формується з федерального списку екстремістських матеріалів (рисунок 4.25) і єдиного реєстру доменних імен, покажчиків сторінок сайтів в мережі «Інтернет» і мережевих адрес, що дозволяють ідентифікувати сайти в мережі «Інтернет», що містять інформацію, поширення якої в Україні заборонено (рисунок 4.26).

Крок 2. Виявлення «маркерів», тобто слів і словосполучень, що мінімально змінюються в ході переформулювання.

Крок 3. Синтез формального опису «маркерів» з використанням регулярних виразів або контекстно-вільної граматики.

Далі робота алгоритму розбивається на дві, що паралельно виконуються процедури попередження і усунення наслідків загрози.

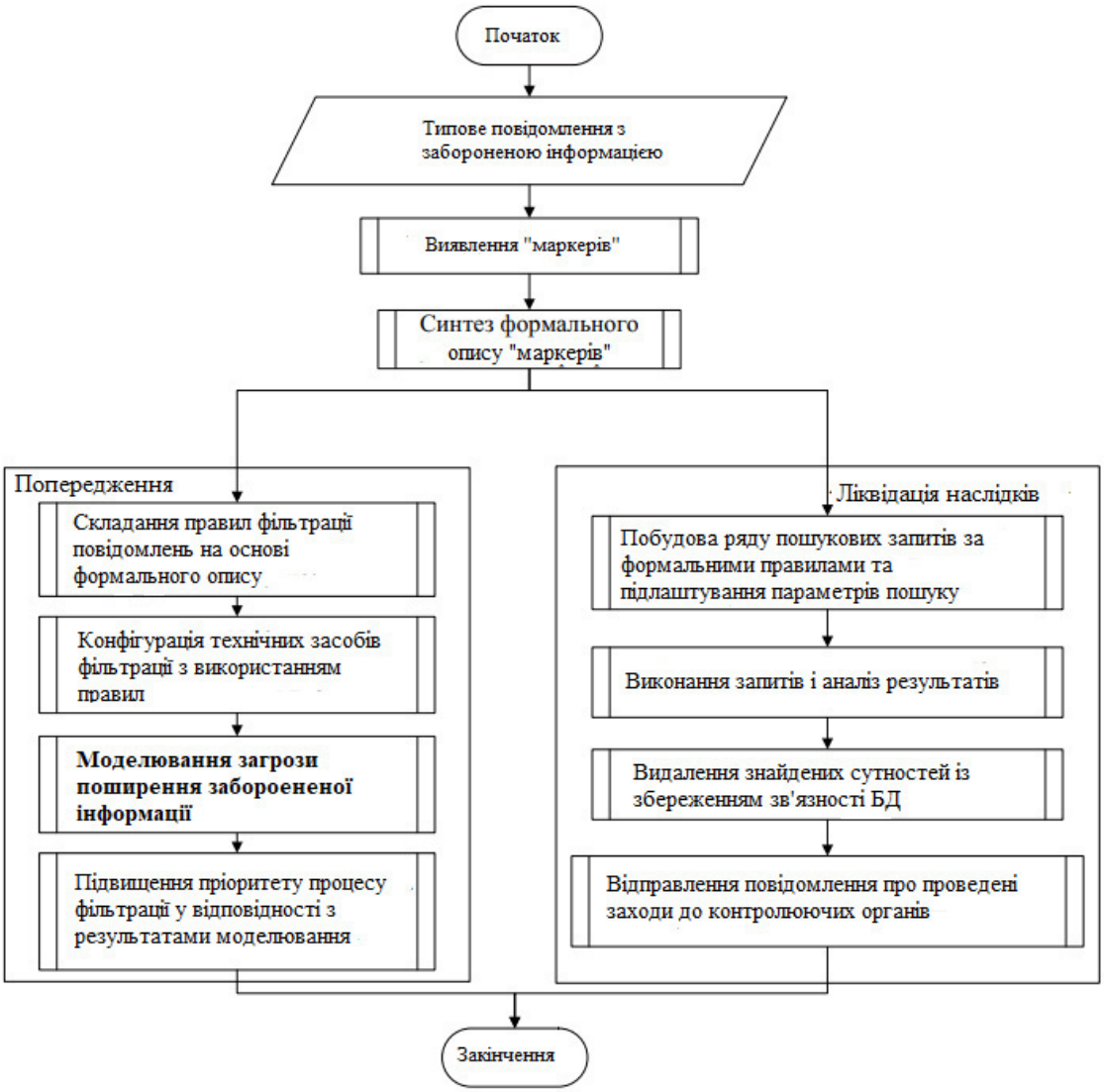


Рисунок 4.24 – Алгоритм протидії поширенню загрози забороненої інформації

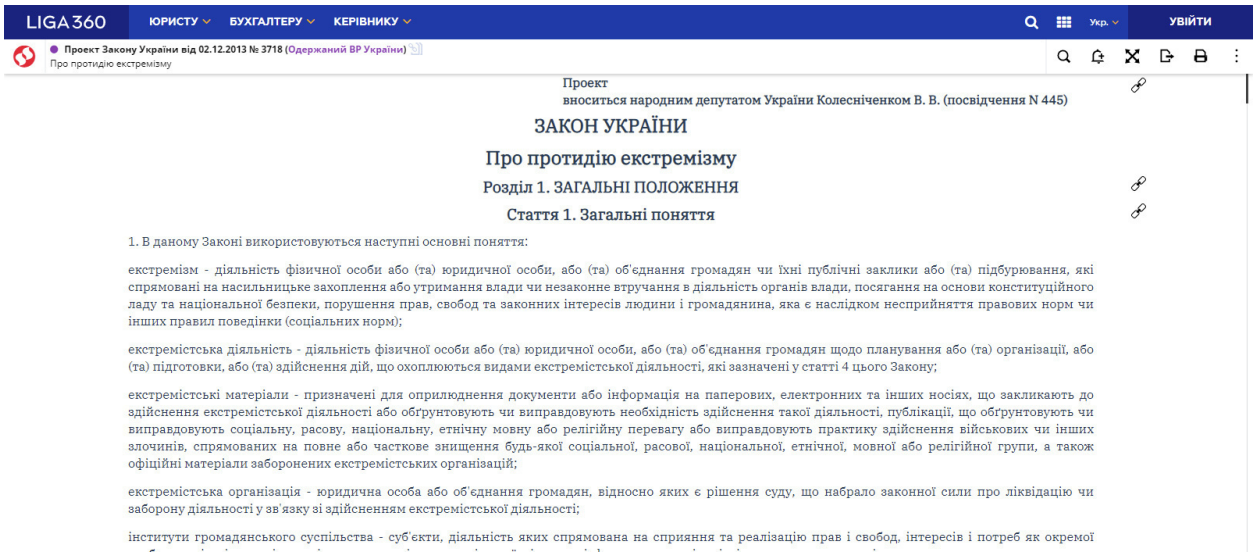


Рисунок 4.25 – Проєкт Закону України про протидію екстремізму

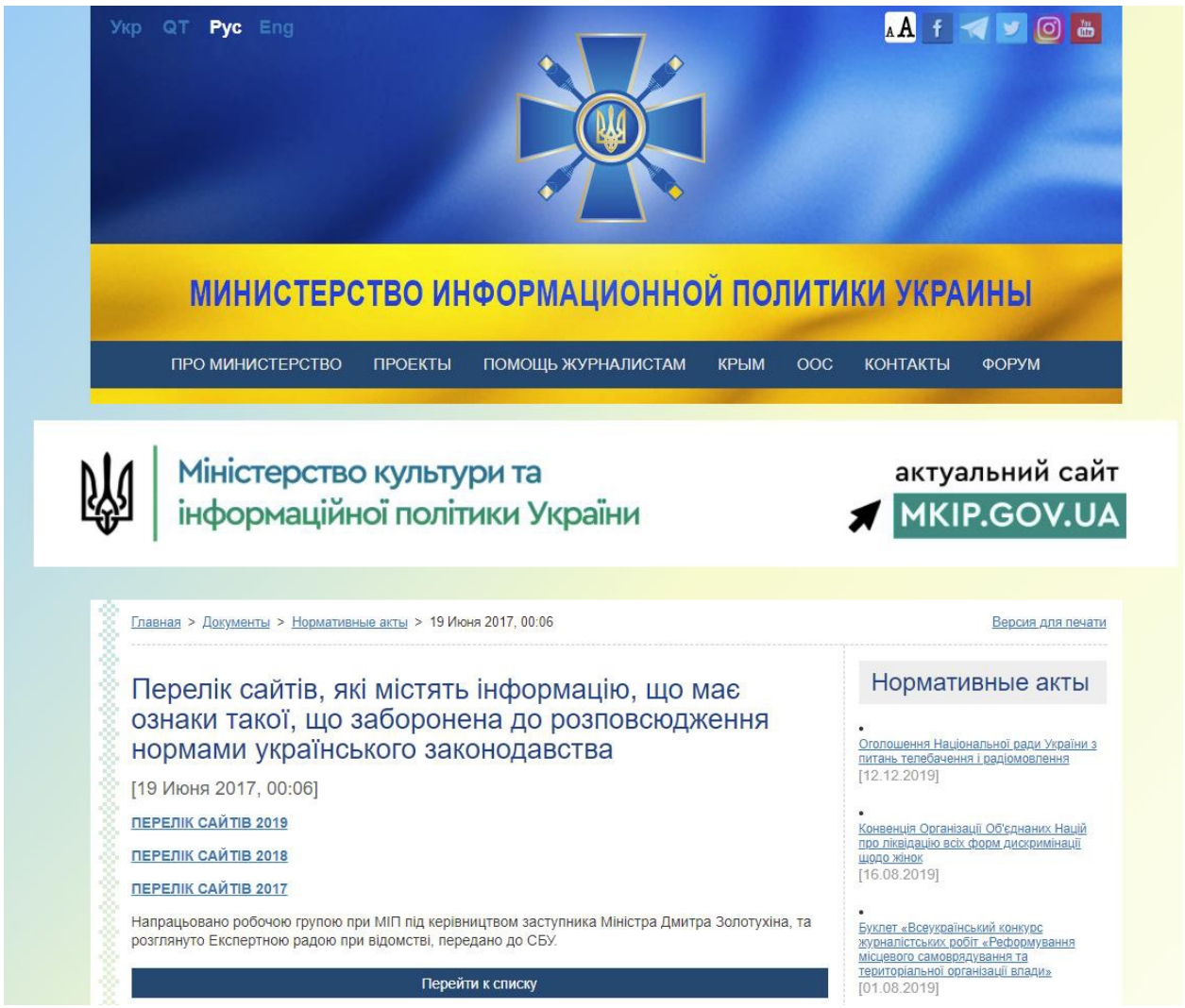


Рисунок 4.26 – Перелік сайтів, що містять заборонену інформацію

Попередження

Крок 4а. Складання правил фільтрації повідомлень на основі формального опису. Здійснюється шляхом компіляції регулярних виразів за допомогою засобів, що призначені для фільтрації (див. крок 5а).

Крок 5а. Конфігурація технічних засобів фільтрації з використанням правил. Як правило, це антиспам системи такі як Apache Spamassassin, Yandex Spamooborona, Kaspersky Antispam, FASTBL, dnsbl тощо. (рисунок 4.27).

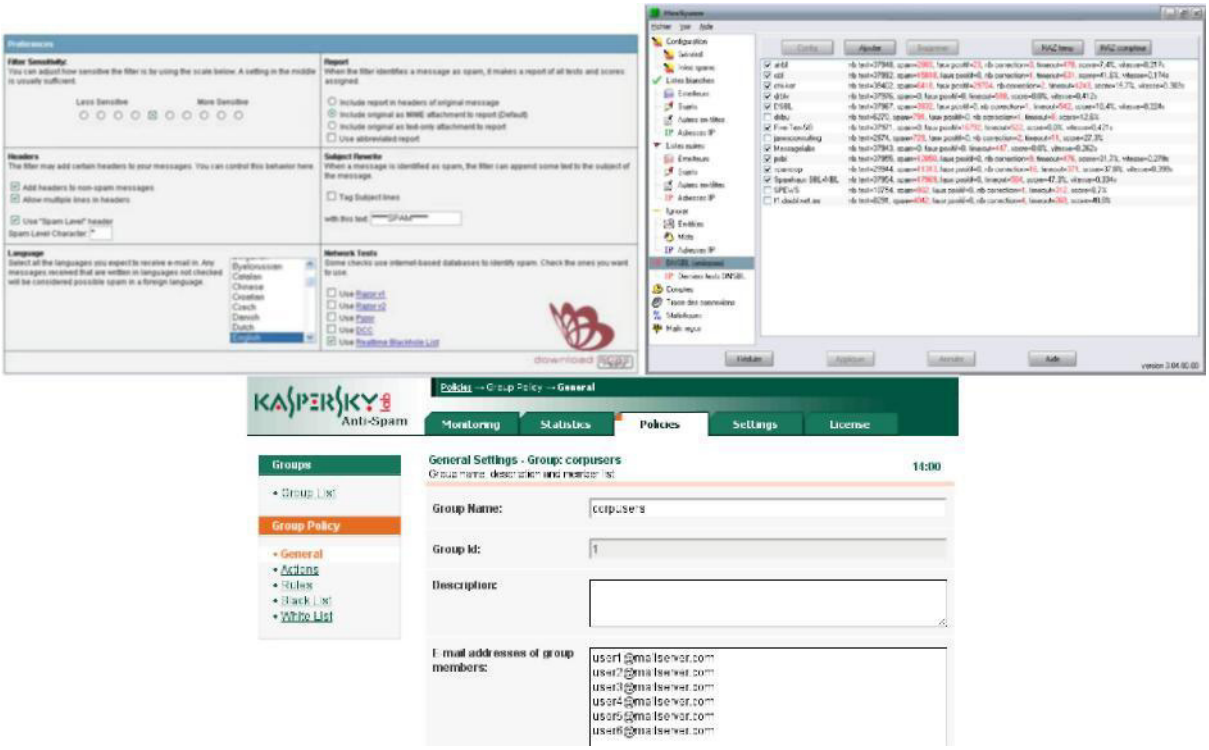


Рисунок 4.27 – Скріншоти програм

Крок 6а. Моделювання загрози поширення забороненої інформації.

Крок 7а. Підвищення пріоритету процесу фільтрації у відповідності з результатами моделювання загрози поширення забороненої інформації.

Ліквідація наслідків

Крок 4б. Побудова ряду пошукових запитів за формальними правилами, та підлаштування параметрів пошуку (пріоритет, глубина тлщо)

Крок 5б. Виконання запитів і аналіз результатів. На даному етапі можливе уточнення результатів.

Крок 6б. Видалення знайдених сутностей із збереженням зв’язності БД.

Крок 7б. Відправлення повідомлень про проведені заходи до контролюючих органів.

4.4 Особливості практичного застосування аналітичної моделі загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Використовуючи розроблену аналітичну модель, можна отримати прогноз по динаміці ЗПЗІ в ІТКМ за прийнятний час. Алгоритм отримання прогнозу складається з послідовності наступних кроків.

Крок 1. Визначити коефіцієнт топологічної уразливості розглянутої ІТКМ. Необхідно постійно проводити моніторинг значення даного параметра для наймасштабніших і популярних мереж для використання його актуального значення.

Крок 2. При появі перших повідомлень із забороненою інформацією зібрати статистику таких повідомлень. Даний крок необхідно виконати на ранніх стадіях виникнення загрози. З одного боку, чим більше даних вдасться зібрати, тим точніше буде прогноз, з іншого боку, при затримці виконання даного кроку, актуальність прогнозу може бути втрачена.

Крок 3. Апроксимувати зібрані дані за допомогою системи диференціальних рівнянь, що описують модель, підібравши потрібні значення β і γ (ймовірності атаки і захисту).

В результаті отримуємо прогноз на весь період поширення загрози забороненої інформації.

Аналітична модель була апробована на даних, отриманих компаніями «SMM3» і «YOUSCAN» в ході експрес-моніторингу негативних згадок бренду Nestle (дезінформація з приводу виявлення скла в дитячому харчуванні Banana, 1-7.08.2011). Результати поширення даної дезінформації в мережі «ВКонтакті» були апроксимовані за допомогою аналітичної моделі (рисунок 4.28). Похибка апроксимації склала приблизно 13%.

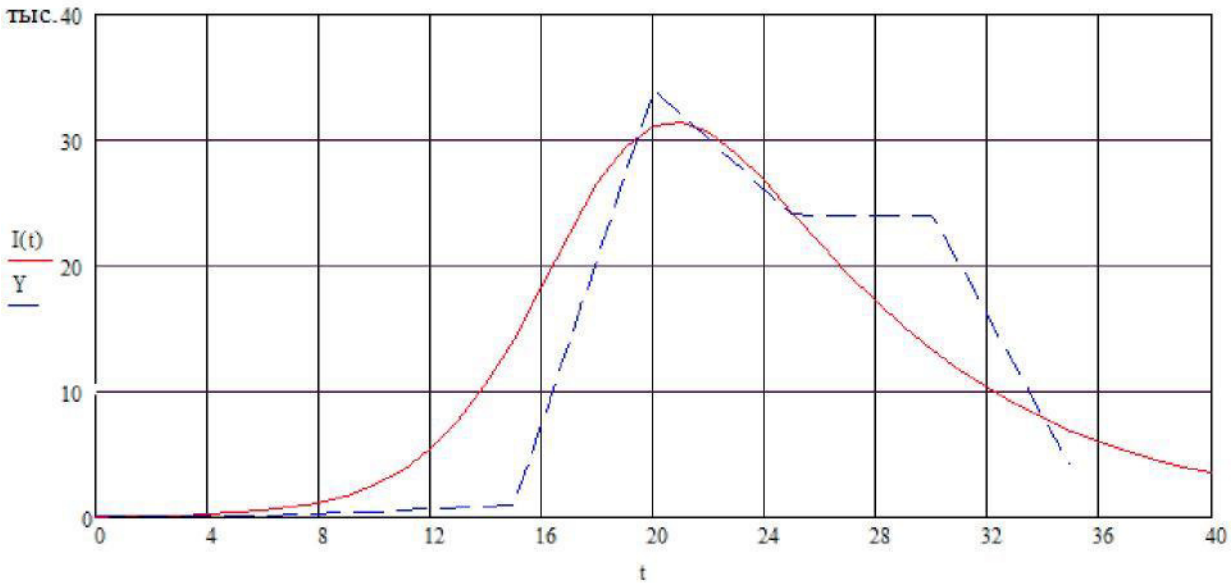


Рисунок 4.28 – Вихідні дані (*Y*) і результат аналитичної моделі (*I*), умовна одиниця часу рівна 5 годинам

4.5 Висновки

Розроблено програмне забезпечення, яке дозволяє за прийнятний час отримати результати моделювання ЗПЗІ в ІТКМ за рахунок використання розподілених обчислювальних ресурсів.

За допомогою розробленого ПЗ були проведені експериментальні дослідження, результати яких показали, що великомасштабні інформаційно-телекомунікаційні мережі не можна віднести ні до одного з існуючих класів складних мереж. Експерименти на топологиях реальних ІТКМ показали, що розподіл ступенів зв’язності вузлів мережі апроксимується гамма-розподілом, а не степеневим і не пуассоновским розподілом, як прийнято вважати. Також результати експериментів вказують, що коефіцієнт кластеризації ІТКМ значно нижче, ніж прийнято вважати (0,04 – 0,05 проти 0,16). Результати, отримані за значенням середньої довжини шляху (підтвердження теорії шести рукостискань), дозволяють нам при дослідженні великомасштабних ІТКМ використовувати фіксоване значення середньої довжини шляху.

В якості рекомендацій запропонований алгоритм роботи автоматизованої системи протидії поширенню загрози забороненої інформації.

Практична цінність роботи полягає в створеному програмному забезпеченні, завдання якого – автоматизація пошуку вузлів соціальної мережі, які є потенційними розповсюджувачами забороненої інформації. Результати впровадження показують, що розроблене програмне забезпечення підвищує ефективність за часом.

ВИСНОВКИ

В рамках дослідження за результатами магістерської роботи отримано рішення науково-технічної задачі розробки моделей і алгоритмів загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах. Основні результати роботи:

1. Розроблено алгоритм реалізації ЗПЗІ в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

2. Запропонована імітаційна модель ЗПЗІ в ІТКМ, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. За її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі.

3. Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

Приклади ефективного апробування механізмів прогнозування ЗПЗІ в ІТКМ дають підставу констатувати адекватність і функціональність основних теоретичних побудов і розроблених на їх основі алгоритмічних і інструментальних засобів.

Розроблено методику формування топології ІТКМ, яка враховує основні топологічні характеристики доступної частини мережі і працює в умові недостатньої репрезентативності вибірки вихідних даних. Запропонована методика складається з послідовності розроблених алгоритмів.

Створено алгоритм формування вихідних даних про топологію мережі (безлічі вершин і зв’язків між ними доступною частини мережі), який враховує обмеження зі збору даних і реалізований у вигляді розробленого програмного забезпечення.

Розроблено алгоритм формування повного графа мережі з урахуванням додавання недоступної частини на основі обчислених прогнозованих топологічних характеристик. Алгоритм реалізований у вигляді розробленого програмного забезпечення.

Введена оцінка топологічної уразливості мережі (вектор топологічної уразливості), що враховує такі параметри: середню довжину шляху мережі, коефіцієнт кластеризації мережі, середній ступінь зв'язності мережі і загальна кількість вузлів в мережі.

Розроблено програмне забезпечення, яке дозволяє за прийнятний час отримати результати моделювання ЗПЗІ в ІТКМ за рахунок використання розподілених обчислювальних ресурсів.

За допомогою розробленого ПЗ були проведені експериментальні дослідження, результати яких показали, що великомасштабні інформаційно-телекомунікаційні мережі не можна віднести ні до одного з існуючих класів складних мереж.

Експерименти на топологіях реальних ІТКМ показали, що розподіл ступенів зв'язності вузлів мережі апроксимується гамма-розподілом, а не степеневим і не пуассоновским розподілом, як прийнято вважати. Також результати експериментів вказують, що коефіцієнт кластеризації ІТКМ значно нижче, ніж прийнято вважати (0,04 – 0,05 проти 0,16). Результати, отримані за значенням середньої довжини шляху (підтвердження теорії шести рукостискань), дозволяють нам при дослідженні великомасштабних ІТКМ використовувати фіксоване значення середньої довжини шляху.

В якості рекомендацій запропонований алгоритм роботи автоматизованої системи протидії поширенню загрози забороненої інформації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Алешин Л.И. Защита информации и информационная безопасность [Текст]/ Л.И. Алешин. – М.: МГУК, 1999. – 176 с.

2. Аналіз та візуалізація дуже великих мереж. URL: http://mrvar.fdv.uni-lj.si/pajek/ (дата звернення: 02.09.2020).

3. Аналізатор Sniffer Pro LAN. URL: https://www.securitylab.ru/software/233623.php (дата звернення: 02.09.2020).

4. Атаманюк А.В. Дослідження проблем інформаційної безпеки в інформаційно-телекомунікаційних мережах/ А.В. Атаманюк, В.М. Джулій, Ю.П. Кльоц // «Інтелектуальний потенціал – 2020» – збірник наукових праць молодих науковців і студентів / Колектив авторів – Хмельницький: ПВНЗ УЕП, 2020. – Частина 2. – С. 5-9.

5. Атаманюк А.В. Проблеми інформаційної безпеки в інформаційно-комунікаційних мережах / С.В. Лєнков, В.М. Джулій, Ю.В. Хмельницький, А.В. Атаманюк// Тези доповідей XVI Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє" Том 1 [Текст] / за заг. редакцією Ігоря Толока. – К. : ВІКНУ, 2020. – С. 46-47.

6. Биячуев, Т.А. Безопасность корпоративных сетей: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. – СПб.: СПбГУ ИТМО, 2016.– 161 с.

7. Бібліотека графіків паралельного підсилення [Електронний ресурс]. Parallel Boost Graph Library [Electronic resource] URL: https://www.boost.org/doc/libs/1_74_0/libs/graph_parallel/doc/html/index.html. (дата звернення: 02.09.2020).

8. Брэгг Р. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг; – М : Эком, 2006. – 912 с.

9. Груздева, Л.М, Монахов, Ю.М., Монахов, М.Ю. Оценка сетевых характеристики компьютерных сетей в условиях информационного вредоносного воздействия [Текст]: учеб. пособие (с грифом УМО) /

Л.М. Груздева, Ю.М. Монахов, М.Ю. Монахов; Владим. Гос.ун-т. – Владимир: Изд-во Владим. Гос. унта, 2010. – 86 с.

10. Жаринов И.В. Конструирование графов с минимальной средней длиной пути [Текст] / И.В. Жаринов, В.В. Крылов; Вестник ИжГТУ, №4. – 2008. – С. 164-169. - ISSN 1813-7903.

11. Завдада А.А. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А.А. Завада, О.В. Самчишин, В.В. Охрімчук // Збірник наукових праць ЖВІ НАУ «Інформаційні системи'12», 2012. – Випуск 6. – С. 97–106.

12. Загальні рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=322B14F318F82FDEB1180D17FE0BFF97.app1?showHidden=1&art_id=320060&cat_id=317163 (дата звернення: 02.09.2020).

13. Касперски К. Компьютерные вирусы: изнутри и снаружи [Текст] / К. Касперски. – Спб: "Питер", 2005. – 528 с.

14. Качалин А.И. Моделирование процесса распространения сетевых червей для оптимизации защиты корпоративной сети [Текст] / А.И. Качалин; Искусственный интеллект, № 2. – 2006. – С. 84-88.

15. Концепція розвитку системи електронних послуг в Україні. Розпорядження Кабінету Міністрів України від 16.11.2016 р. № 918-р. URL: http://zakon3.rada.gov.ua/laws/show/918-2016-%D1%80 (дата звернення: 02.09.2020).

16. Кримінальний кодекс України від 05.04.2001 № 2341-III. Дата оновлення: 25.09.2020. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page (дата звернення: 02.09.2020).

17. Лукацький А.В. Предотвращение сетевых атак: технологии и решения / А.В. Лукацкий. – СПб. : Экспрес Электроника, 2006. – 268 с.

18. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. Дата оновлення: 01.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 02.09.2020).

19. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. Дата оновлення: 13.02.2020. URL*:* https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 02.09.2020).

20. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 02.09.2020).

21. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (дата звернення: 02.09.2020).

22. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 20.03.2020. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 02.09.2020).

23. Про інформацію : Закон України від 02.10.1992 №2657-XII. Дата оновлення: 16.07.2020. URL: http://zakon2.rada.gov.ua/laws/main/2657-12 (дата звернення: 02.09.2020).

24. Про науково-технічну інформацію : Закон України від 25.06.1993 № 3322-XII. Дата оновлення: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (дата звернення: 02.09.2020).

25. Собейкис В.Г. Азбука хакера 3. Компьютерная вирусология [Текст] / В.Г. Собейкис. – М.: Майор, 2006. – 512 с.

26. Столлингс В. Основы защиты сетей. Приложения и стандарты / В. Столлингс. – М.: Издательский дом "Вильямс", 2002. – 432 с.

27. Тропіна М. Дослідження соціальних мереж як нового феномену сучасного світу / М. Тропіна // Наукові записки Малої академії наук України. Серія «Педагогічні науки» : [зб. наук. праць ; редкол.: С.О. Довгий (голова), О.Є. Стрижак, О.В. Лісовий, І.М. Савченко та ін.]. — Київ : Національний центр «Мала академія наук України», 2019. — Вип. 16. – С. 57-63 (76 с.)

28. Чубин І. ARP-spoofing [Електронный ресурс] / І. Чубин; URL: http://xgu.ru/wiki/ARP-spoofing (дата звернення: 02.09.2020).

29. Amaral, LAN, Scala, A., Barthelemy, M., Stanley HE (2000) Classes of smallworld networks [Text] / Amaral LAN, A. Scala, M. Barthelemy, Stanley H.E; Proceedings of the National Academy of Sciences of the United States of America. – 97: 11149

30. Bace R., Mell P. Special Publication on Intrusion Detection Systems. [Text] / R. Bace, P. Mell; Tech. Report SP 800-31; National Institute of Standards and Technology. – 2001.

31. Blazek, R.B. A Novel Approach to Detection of «Denial-of-Service» Attacks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods [Text] / R.B. Blazek; Proc. IEEE Workshop Information Assurance and Security. - IEEE CS Press, 2001. – P. 220–226.

32. Bollobás, B. Random Graphs [Text] / B. Bollobás; Cambridge University Press. – 2001. – 520 p. - ISBN 0521809207.

33. Cohen, F. Simulating Cyber Attacks, Defenses, and Consequences [Text] /F. Cohen; IEEE Symposium on Security and Privacy. – Berkeley, 1999.

34. Dorogovtsev, S.N., Mendes, J.F.F. Evolution of Networks: From Biological Networks to the Internet and WWW [Text] / S.N. Dorogovtsev, J.F.F. Mendes; - Oxford, USA: Oxford University Press, 2003. — 280 p. - ISBN 978-0198515906.

35. Erdös, P., Rényi, A. On the evolution of random graphs [Text] / P. Erdös, A. Rényi; Publications of the Mathematical Institute of the Hungarian Academy ofSciences, 5. – 1960. – P. 17-61.

36. Ferrara, E., Fiumara, G., Topological features of Online Social Networks. Communications on Applied and Industrial Mathematics [Text] / E. Ferrara, G. Fiumara; – 2011.

37. Frauenthal, J.C. [Text] / J.C. Frauenthal; Mathematical Models in Epidemiology. – New York: Springer-Verlag, 1980. – 335 p.

38. Golbeck, J., Hendler, J. Inferring binary trust relationships in web-based social networks [Text] / J. Golbeck, J. Hendler; Transactions on Internet Technology - 2006. - Vol. 6, no. 4. - P. 497-529.

39. Heberlein, L.T., Dias, G.V., Levitt, K.N., Mukherjee, B., Wood, J., Wolber, D.A. Network security monitor [Text] / L.T. Heberlein [et al.]; Proc. of IEEE Symposium on Re-search in Security and Privacy. – Los Alamitos, CA, USA: IEEE Computer Society, 1990. – P. 296–304

40. Hofmeyr, S.A., Forrest, S., Somayaji, A. Intrusion detection using sequences of system calls [Text] / S.A. Hofmeyr, S. Forrest, A. Somayaji; Journal of Computer Security. - Amsterdam: IOS Press, 1998. – Vol. 6, no 3. – P. 151-180.

41. Jung, J., Krishnamurthy, B., Rabinovich, M. Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites / J. Jung, B. Krishnamurthy, M. Rabinovich; WWW2002 (May 7-11, 2002) – Honolulu, Hawaii, USA, 2002.

42. Kolotov, A. Мониторинг сети с помощью tcpdump. URL: http://www.linuxshare.ru/docs/net/tcpdump.html (дата звернення: 02.09.2020).

43. Leveille, J. Epidemic Spreading in Technological Networks [Text] / J. Leveille; Information Infrastructure Laboratory HP Laboratories Bristol. – 2002. – P. 65-76.

44. Liben-Nowell D., Kleinberg J. The link-prediction problem for social networks [Text] / D. Liben-Nowell, J. Kleinberg; J. American Society for Information Science and Technology. – 2007. – Vol. 58, no. 7. – P. 1019-1031.

45. Newman, Mark, Barabasi, Albert-La*sz*lo, Duncan, Watts, J. The Structure and Dynamics of Networks: (Princeton Studies in Complexity) [Text] / Mark Newman, Albert-La*sz*lo Barabasi, Duncan, J. Watts; — Princeton, USA: Princeton University Press, 2006. — 624 p. — ISBN 978-0691113579.

46. Pastor-Satorras, R., Vespignani, A. Critical load, congestion instabilities in scalefree networks [Text] / R. Pastor-Satorras, A. Vespignani; Europhys. Lett. – 2002. – Vol. 62. – P. 292.

47. Pastor-Satorras, R., Vespignani, A. Epidemic Spreading in Scale-Free Networks [Text] / R. Pastor-Satorras, A. Vespignani; Phys. Rev. Lett., 86. – 2001.

48. Pastor-Satorras, R., Vespignani, A., Absence of epidemic threshold in scale-free networks with connectivity correlations [Text] / R. Pastor-Satorras, A. Vespignani; Phys. Rev. Lett. – Pub.: American Physical Society, 2002. – Vol. 90, Iss. 2. – P. 1-4.

49. Wang, H., Guo, Y. Consensus on scale-free network [Text] / H. Wang, Y. Guo; American Control Conference. – 2008. – P. 748 – 752

50. Watts, D., Strogatz, S. Collective dynamics of small-world networks [Text] / D. Watts, S. Strogatz; Nature. – 1998. - Vol. 393, No. 6684. - P. 440-442.

Додаток А

(обовязковий)

Код (лістинг) програмного забепечення

Фрагмент коду з файлу DistributedGraph_main.cpp

```
void SIR modelling(DistributedGraph& g,
     vector<Node::id type>
     preinf,
     vector<Node::id type>
     prerec, double
     inf prob, double
     rec prob, string
     outFile) {
          mpi::communicator world;

          if(main process(g))
              log mpi() << "Preparing preinfected and
          prerecovered nodes..." << endl; auto sir =
          get(&Node::sir, g); if(main process(g)) {
               BOOST FOREACH(Node::id type v, preinf) {
             put(sir, add vertex(v, g), Node::SIR::I);
               }
               BOOST FOREACH(Node::id type v, prerec) {
             put(sir, add_vertex(v, g), Node::SIR::R);
               }
          }
          synchroniZe(g.proce
          ss group());
          if(main process(g))
               log_mpi() << "Finished." << endl;

          SIRHistory sirHistory;
          SIRManager sirManager(g, inf prob, rec prob);
          for(unsigned iter = 0;; ++iter) {
               log mpi() << "Iteration: "
               << iter << endl; SIRVector
               condition(3);
       vector<DistributedGraph::vertex descriptor> infected;
               vector<DistributedGraph::vertex descriptor>
               potentially susceptible; BGL FORALL VERTICES(v,
               g, DistributedGraph) { if(g[v].sir ==
               Node::SIR::I) { infected.push back(v);
               BGL FORALL ADJ(v, av, g, DistributedGraph) {
        // Збираємо всіх сусідів зараженних вузлів, також і з
        // статусами відмінними від 'S', оскільки отримання інфо
про статус вузла
        // з іншого процесу займає більшу кількість часу
                                  if(av.owner != g.processor()
|| av.owner == g.processor() && g[av].sir ==
Node::SIR::S)
                                       potentially susceptible.
                            push back(av); }
                            condition[Node::SIR
                       ::I]++; } else
                       if(g[v].sir ==
                       Node::SIR::S) {
                            condition[Node::SIR
                       ::S]++; } else
                       if(g[v].sir ==
                       Node::SIR::R) {
```

```
                    condition[Node::SIR::
                R]++; } }

                sirHistory.push_back(condition);
                log_mpi() << "SIR condition: " << condition <<
                endl;

        // Приймає рішення про припинення моделювання на основі
відсутності зараження вузлів
                bool infected exists = !infected.empty();
bool cont;
if(main process(g)) {
     mpi::reduce(world, infected exists, cont, logical or<bool>(), 0); }
else {
     mpi::reduce(world, infected exists, logical_or<bool>(), 0); }
mpi::broadcast(world, cont, 0);
// Припиняємо моделювання
if(!cont) break;

// Намагаємось заразити
BOOST_FOREACH(auto v, potentially_susceptible) {
     sirManager.infect(v); }
// Намагаємось вилікувати
BOOST FOREACH(auto v, infected) {
     sirManager.recover(v); }

// End of BSP superstep
synchronize(g.process_group());
}
if(main process(g)) {
     SIRHistory res;
     mpi::reduce(world, sirHistory, res, SIRHistoryReducer(), 0);
     ofstream os(outFile);
     os << res; } else {
mpi::reduce(world, sirHistory, SIRHistoryReducer(), 0);

}

}
```

Фрагмент коду з файлу aux_types.h

```
struct
     SIRManage
     r {
     private:
          typedef Node::id_type id_type;

     public:
      SIRManager(DistributedGraph& g, double inf prob, double rec prob):
          g(g),
                process group(g.process group(),
graph::parallel::attach distributed object()),
                sir(get(&Node::sir, g)),
                inf gen(std::time(0)),
                rec gen(std::tim
          e(0)) {
                graph::parallel::simple trigger(process group,
infect_tag, this, &SIRManager::trigger);
                double inf probs[] = {1.0 - inf prob, inf prob};
                double rec_probs[] = {1.0 - rec_prob, rec_prob};
```

```
                inf = random::discrete distribution<>(inf_probs);
                rec =
            random::discrete distribution<>(rec probs);
            }

            void infect(const
                DistributedGraph::vertex descriptor& v){
                using namespace std;
                if(v.owner ==
                    g.processor()) {
                    infect_local(v);

            } else {
         graph::distributed::send(process group, v.owner, infect tag, v); }
        }

        void recover(const DistributedGraph::vertex descriptor& v) {
            // На поточний момент оздоровлюються тільки локальні вузли
            recover local(v);
        }

    private:
        void trigger(int source, int tag, const
        DistributedGraph::vertex descriptor& v,
            graph::parallel::trigger receive context
        context) {
            using namespace std;
            infect local(v);
        }

        void infect local(const DistributedGraph::vertex_descriptor& v){
            if(g[v].sir == Node::SIR::S &&
                inf(inf gen)) { put(sir, v,
                Node::SIR::I);
            } }

        void recover_local(const DistributedGraph::vertex_descriptor& v){
            if(g[v].sir == Node::SIR::I && rec(rec gen))
                { put(sir, v, Node::SIR::R);
            } }

        DistributedGraph& g;
        DistributedGraph::process group type
        process_group;

        property_map<DistributedGraph, Node::SIR Node::*>::type sir;

        random::mt19937 inf gen;
        random::mt19937 rec gen;
        random::discrete distribution<> inf;
        random::discrete_distribution<> rec;

        enum Tags {
    infect_tag }; };
```

Додаток Б

(обовязковий)

Перелік наукових праць

УДК 004.891

к.т.н., доц. **Джулій В.М.** (ХмНУ)
Атаманюк А. В. (ХмКК)

МОДЕЛЬ БЕЗПЕКИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

В статті запропоновано підхід до визначення моделі безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу. Інформаційно-телекомунікаційні мережі є великомасштабними мережами з постійно зростаючим числом абонентів. З бурхливим зростанням кількості користувачів ІТКМ виникають проблеми інформаційної безпеки і захисту інформації в них.

Проведений аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту.

Створення моделей і алгоритмів поширення загрози забороненої інформації – один з ключових підходів при вирішенні даної задачі. Проведений аналіз публікацій з даної тематики показує, що існуючі рішення малоефективні. Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Розроблено алгоритм реалізації ЗПЗІ (загрози поширення забороненої інформації) в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

Запропонована імітаційна модель ЗПЗІ в ІТКМ, яка враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі.

Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

Ключові слова: інформаційна безпека, аналітична модель, імітаційна модель, поширення загроз, інформаційна взаємодія, модель мережі.

Вступ. Інформаційно-телекомунікаційні мережі (ІТКМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. Сучасною проблемою таких систем є їх низький рівень інформаційної безпеки. Ефективного захисту абонентів від загрози поширення забороненої інформації, зокрема в умовах широкого використання індивідуально-орієнтованих сервісів і пов'язаних з ними протоколів і технологій (SOAP, CORBA, REST тощо), не існує. Серед безлічі функцій захисту принциповою в відношенні даних систем є функція попередження прояву забороненої інформації. Вона реалізується за рахунок механізмів прогнозування загрози поширення і розсилання повідомлень з попередженнями про наслідки дій зі забороненим контентом. Використання інших функцій (попередження, виявлення,

локалізації та ліквідації загрози) припускає наявність повного контролю над системою, що в реальних умовах неможливо.

Інформаційно-телекомунікаційна мережа надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярними з них є соціальні мережі. З бурхливим ростом кількості користувачів інформаційно-телекомунікаційних мереж виникають і проблеми безпеки в них. Узагальнена структурна схема інформаційно-телекомунікаційних мереж (ІТКМ) приведена на рис. 1. Її склад в загальному випадку утворюють такі функціональні елементи:

- абоненти (А). Під абонентом розуміється людино-машинна система, що складається з пристрою, через який здійснюється доступ до мережі, і безпосередньо користувача ІТКМ. Абоненти можуть бути окремими вузлами мережі (якщо користувач використовує свій домашній комп'ютер), або можуть бути об'єднані в корпоративну обчислювальну мережу (КОМ) (якщо абонент використовує робочий комп'ютер), включають в себе модулі (інформаційного) захисту (МЗ) і програмне забезпечення (браузер) для взаємодії з керуючим елементом;
- мобільні абоненти (МА). Користувачі, які використовують мобільні пристрої (смартфони, планшети тощо), для доступу до мережі. Також використовують програмне забезпечення (спеціальний додаток) і модулі захисту (МЗ);
- сервери (С). У КОМ знаходяться інформаційні сервери різного функціонального призначення, які беруть участь в інформаційній взаємодії (наприклад, проксі-сервера);
- КОМ містить крім абонентів і серверів, також засоби маршрутизації, комутації та адміністрування (МКА), систему безпеки (СБ), що включає механізми захисту для всієї корпоративної мережі;
- засоби телекомунікації, що забезпечують взаємодію абонентів між собою;
- керуючий елемент технічно є сукупністю комутуючого і серверного устаткування, що реалізує основні функції системи. Включає в себе сервери, які містять в загальному випадку: балансувальник навантаження (БН), елемент бізнес-логіки (БЛ), бази даних (БД), інфраструктурні системи (ІС) (системи статистики, конфігурації, моніторингу тощо).

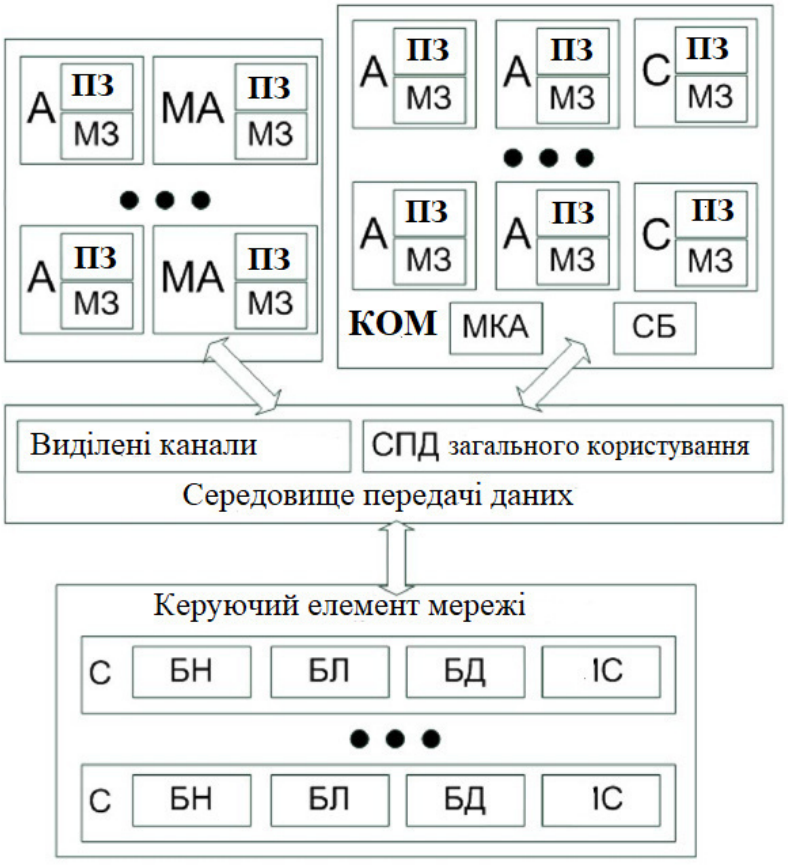


Рисунок 1 – Структурна схема ІТКМ

Розглянемо існуючі проблеми інформаційної безпеки в інформаційно-телекомунікаційних мережах, які актуальні для даного дослідження:

1. Використання глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи. Найбільш вразливими компонентами системи, що часто атакуються, є: сервери; робочі станції; середовище передачі інформації; вузли комутації. Типові інформаційні впливи зловмисників:

- Прослуховування мережевого трафіку. Щоб прослухати трафік (sniffing) мережевий адаптер переводиться в «безладний» режим. У цьому режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даною адресою, як в нормальному режимі функціонування-технології – ARP Spoofing (ARP-poisoning), MAC Flooding і MAC Duplicating. Перехоплення здійснюється з використанням мережевих моніторів, з яких найбільш функціональними є Sniffer Pro від компанії Sniffer Technologies, IRIS Network Traffic Analyzer від компанії EYE і TCP Dump.

Наслідки. Сучасні мережеві протоколи (TCP / IP, ARP, HTTP, FTP, SMTP, POP3 тощо) не мають механізмів захисту (дані передаються у відкритому вигляді). Зловмисник, що перехоплює трафік між сервером і будь-яким вузлом мережі, може заволодіти аутентифікаційними даними користувача (отримати пароль).

Протидія. Відомо ряд методів визначення наявності запущеного сніфера в мережі, наприклад метод пінга, метод ARP, метод DNS і метод пастки.

- Сканування вразливостей. Результатом роботи сканера є інформація про систему, що містить список мережевого обладнання, комп'ютерів з запущеними на них службами, версіями мережевого ПЗ (а отже і вразливостей, властивих даному ПЗ), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаку. Саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосереднього НСД.

Виявлення. Само по собі сканування не є незаконним. Однак, якщо сканування з боку зовнішньої, по відношенню до системи, мережі звичайне явище, то сканування комп'ютерів з внутрішньої мережі – безумовно, інцидент безпеки, що вимагає негайної реакції з боку мережевого адміністратора. Виявити кроки сканування можна, вивчаючи журнали реєстрації міжмережевих екранів (МЕ). Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти. Тому сучасні МЕ і системи виявлення вторгнень СВВ мають модулі (plug-in), що дозволяють виявити сканування в режимі реального часу. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють здійснювати сканування максимально приховано. Наприклад, в Nmap існують можливості, що дозволяють значно ускладнити виявлення сканування для СВВ.

Протидія. Використання мережевих СВВ, або періодичне вивчення журналів реєстрації МЕ.

- Мережеві атаки. Мережеві атаки можна розділити на: атаки, засновані на переповненні буфера (overflow based attacks). Вони використовують вразливість системи, яка полягає в некоректній програмної обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями; атаки, спрямовані на відмову в обслуговуванні (Denial Of Service attacks). Атаки не обов'язково використовують вразливості в ПЗ системи, що атакується. Порушення працездатності системи відбувається через те, що дані, що їй посилають, призводять до значної витрати ресурсів системи. Найпростішим прикладом атаки цього типу є атака «Ping Of Death». Суть її в наступному: на комп'ютер жертви надсилається сильно фрагментований ICMP-пакет великого розміру. Реакцією ОС Windows на отримання такого пакету є повне зависання.

- Атаки, засновані на використанні вразливостей в ПЗ мережевих додатків – експлойти (exploit). Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Експлойти є шкідливими програмами, що реалізують відому вразливість в ОС або прикладному ПЗ, для отримання НСД до вразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій подавлення антивірусних програм і МЕ. Наслідки застосування експлойтів можуть бути самими критичними. У випадку отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути такими: впровадження троянської програми, впровадження набору утиліт для приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких та зовнішніх носіїв інформації, створення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлів з хешами паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи.

Протидія. МЕ і СОВ, встановлені на системі, що атакується, в деяких випадків не в змозі відобразити дію експлойтів. Для успішного відображення атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень заснований на розпізнаванні сигнатур вже відомих атак. Хоча є розробки, здатні за завіреннями розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

- Шкідливі програми. Шкідливі програми – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів або якого іншого впливу, що перешкоджає нормальному функціонуванню мережі. До шкідливих програми відносяться комп'ютерні віруси, троянські коні, мережеві черв'яки тощо.

Протидія. Типовим методом протидії є застосування антивірусних засобів, що працюють в режимі реального часу (моніторів). Для виявлення троянських програм існує спеціалізоване програмне забезпечення.

2. Проблема забороненого контенту. Залежно від законодавства країни різні матеріали можуть вважатися нелегальними. У більшості країн заборонені: матеріали сексуального характеру за участю дітей і підлітків, порнографічний контент, описи насильства, в тому числі сексуального, екстремізм і розпалювання расової ненависті. В українському законодавстві кілька законів регулюють питання надання інформації про фізичних та юридичних осіб, а саме: Закон України «Про інформацію» від 02.10.92, що регулює відносини щодо одержання і поширення інформації; Закон України «Про захист персональних даних» від 01.06.2010, що визначає захист і обробку персональних даних; Закон України «Про доступ до публічної інформації» від 13.01.2011, який надає право на отримання інформації, що знаходиться у володінні розпорядників.

Аналогічно з концепцією забезпечення комплексного захисту об'єкта інформатизації, можна сформувати повну множину функцій захисту від забороненої інформації. Під функцією захисту (ФЗ) розуміється сукупність однорідних в функціональному відношенні заходів, що регулярно здійснюються в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

Перелік повної множини функцій захисту від забороненої інформації в соціальних мережах:

1. Попередження умов виникнення забороненої інформації. Функція реалізується за допомогою нормативно-правових актів. Вона не може повністю виключити загрозу поширення забороненої інформації в соціальних мережах, так як в цілому ситуація з дотриманням законів незадовільна, а в інтернет-просторі загострюється через технічні складнощі.

2. Попередження безпосередньої прояви забороненої інформації. Функція реалізується за рахунок механізмів прогнозування поширення забороненої інформації в соціальній мережі.

3. Виявлення забороненої інформації, яка проявилася. Функція пов'язана з моніторингом ІТКМ на предмет забороненої інформації на сторінках абонентів. Як правило, для реалізації даного захисту використовується різні СОРМ (система оперативно-розшукових заходів). Дана ФЗ пов'язана з проблемами контекстного пошуку, а також необхідністю контролю над всією системою.

4. Попередження впливу на абонентів забороненої інформації, яка проявилася. Функція може бути реалізована за допомогою автоматичного пересилання повідомлення з попередженням про відповідальність за розповсюдження забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до керування системи та нелегітимними – при його відсутності (зламання акаунта). ФЗ ділиться на дві функції. Перша пов'язана з попередженням абонентів, на сторінках яких була знайдена заборонена інформація, а друга – з розсилкою попереджень потенційним одержувачам забороненої інформації.

5. Виявлення впливу забороненої інформації на абонентів. Функція пов'язана безпосередньо з фіксацією процесу поширення забороненої інформації, може бути реалізована через контекстний аналіз повідомлень.

6. Локалізація, обмеження впливу забороненої інформації на абонентів. Функція реалізується через блокування абонентів, що поширюють заборонену інформацію, або абонентів – потенційних розповсюджувачів. Дана ФЗ опирається на попередні функції і для її ефективної реалізації необхідний контроль над системою.

7. Ліквідація наслідків виявленого впливу забороненої інформації на абонентів. Функція пов'язана з видаленням забороненої інформації з системи. Для реалізації даної функції також необхідний контроль над системою.

На основі проведеного аналізу функцій захисту видно, що найбільш ефективні функції – це перші функції, оскільки вони забезпечують захист на початкових етапах. Наведені функції захисту

мають свої недоліки. Найбільш перспективною ФЗ інженерно-технічного напряму є $ФЗ_2$. На даному етапі, маючи інформацію про топології ІТКМ і потенційних розповсюджувачів забороненої інформації, можливе прогнозування процесу її поширення.

Постановка задачі. Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗПЗІ) є моделювання, наприклад, з використанням моделей впливу, моделей просочування і зараження. Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня довжина шляху). Взаємодія між абонентами в межах цих математичних моделей описується переважно гомогенним графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування загрози поширення забороненої інформації більше 30%. Крім того, дані підходи мають в основному теоретичний характер, практика їх використання не виходить за межі експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів загрози поширення забороненої інформації, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Створення моделей та алгоритмів поширення загрози забороненої інформації – одна з ключових задач в даному напрямку. При її вирішенні виникають проблеми, пов'язані з властивостями розглянутої інформаційно-телекомунікаційної системи, а саме:

1. Відсутність перевірки достовірності даних про вузол системи. Дуже часто абоненти ІТКМ вказують недостовірну інформацію про себе.

2. Закритість системи. Структура та інформація про управління системою є конфіденційною інформацією.

3. Проблема збору інформації. Неможливо отримати повну інформацію про топологію ІТКМ. Існує можливість для звичайного абонента збору інформації про структуру мережі (функції API), але ця можливість має багато обмежень (налаштування приватності, часовий інтервал).

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу.

Прведений аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту, існуючі рішення малоефективні.

Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). А, якщо топологія враховується, то, як правило, використовується найпростіша SIS модель, а структура мережі відбивається SF мережею. При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Основна частина. За результатами проведеного дослідження предметної області вставлено необхідність розробки імітаційної і аналітичної моделей поширення загрози забороненої інформації в ІТКМ. Імітаційна модель необхідна для отримання експериментальних результатів для синтезування аналітичної моделі. Необхідність створення аналітичної моделі обґрунтовується тим, що для імітаційного моделювання на топології існуючих ІТКМ (десятки мільйонів вузлів) необхідні великі витрати часу. Не враховуючи час на збір інформації про топології мережі, який може становити близько тижня, безпосередньо моделювання загрози поширення забороненої інформації (ЗПЗІ) займає кілька годин навіть при використанні розподілених обчислювальних ресурсів. Аналітична модель може дати прогноз загрозі поширення забороненої інформації майже миттєво. З її допомогою можна отримати актуальні дані (до того моменту, коли кількість атакуючих абонентів буде максимальним) за динамікою ЗПЗІ.

Процес ЗПЗІ характеризується наступними особливостями. У мережі існують вузли трьох типів. Перший тип – атакуючі вузли, це вузли, які розповсюджують заборонену інформацію. Другий тип – захищені вузли, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися. Третій тип – потенційно вразливі. Вузли такого типу не беруть участі в процесі поширення загрози, але можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію.

Аналітична модель динаміки атаки $I(t)$ та модель ахисту вузлів $R(t)$ представлені наступним чином (1):

$$\begin{cases} I(t) = f(N, \beta, \gamma, \varphi, t) \\ R(t) = g(N, \beta, \gamma, \varphi, t) \end{cases} \quad (1)$$

де, N – кількість вузлів, яка дорівнює кількості абонентів мережі, β – параметр, що відображає силу загрози, ймовірність здійснення атаки, γ – параметр, що відображає ступінь протидії загрозі, ймовірність захисту абонента (β і γ в даному дослідженні визначено як константи, але можуть бути виражені як функції, що залежать від психосемантичних профілів абонентів ІТКМ), φ – коефіцієнт топологічної вразливості мережі, що відображає внутрішню властивість ІТКМ, засновану на характеристиках її топології, яке сприяє поширенню забороненої інформації , t – час процесу (в умовних одиницях часу).

Розробка аналітичної моделі включає в себе послідовність наступних дій:

- формування імітаційної моделі для дослідження характеру і параметрів процесу ЗПЗІ;
- синтез аналітичних залежностей параметрів процесу;
- проведення експериментів з метою перевірки точності (адекватності) моделі.

Наведемо алгоритм реалізації ЗПЗІ, грунтуючись на описі процесів, що відбуваються в реальних ІТКМ. Схема реалізації загрози зображена на рисунку 2.

Алгоритм 1 – Загрози поширення забороненої інформації в ІТКМ

1. Поширення забороненої інформації (ЗІ) (далі процес «атаки») ініціює будь-який абонент-зловмисник (на рис. 2 – вузол 1), поширюючи повідомлення з ЗІ (реалізує загрозу) за його списком контактів. Атаку може починати один зловмисник або група.

2. Абоненти-одержувачі (вузли 2, 3, 4), прийнявши повідомлення з ЗІ, читають його і включаються в процес атаки, поширюючи її далі по своєму списку контактів (вузол 3), або ігнорують або взагалі видаляють повідомлення (вузол 2) , тобто в атаці не беруть участь. Процес атаки зазвичай йде лавиноподібно. Атакуючі абоненти не закінчують атаку, одного разу передавши повідомлення із забороненою інформацією. Вікно атаки, як правило, триває протягом досить значного проміжку часу і залежить від типу подачі ЗІ в повідомленні, зацікавленості абонента тощо.

3. Абоненти можуть перестати сприймати і, відповідно, поширювати ЗІ (вузол 5) (далі процес «захисту»), внаслідок впливу механізмів захисту (наприклад, попередження про неї), тому повідомлення з ЗІ від атакуючих абонентів будуть постійно відхилятися.

4. Процес триває поки в мережі є абоненти-зловмисники, або є потенційно вразливі вузли, якщо відсутній процес захисту.

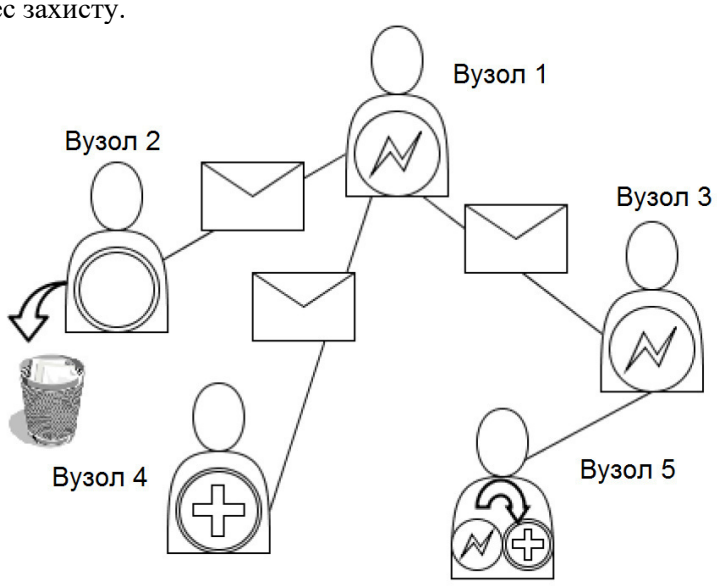


Рисунок 2 – Схема реалізації загрози поширення забороненої інформації в ІТКМ

Таким чином, ЗПЗІ в ІТКМ є складним динамічним процесом, що складається з двох протидіючих підпроцесів атаки і захисту вузлів мережі.

На основі описаного алгоритму побудована імітаційна модель ЗПЗІ в ІТКМ:

Вхідні дані: *N*, *k* – середній ступінь зв'язності вузлів, *a* – параметр, що відображає середню довжину шляху і рівень мережевої кластеризації, β, γ (в моделі вважається, що β та γ однакові для кожного абонента), I_0 - кількість абонентів-зловмисників - початкових джерел загроз, R_0 - кількість абонентів спочатку несприйнятливих до атакуючих дій.

Вихідні дані: $I(t), R(t), S(t)$ – чисельні масиви даних, що описують динамічний процес реалізації ЗПЗІ (кількості атакуючих, захищених і потенційно вразливих вузлів у кожну умовну одиницю часу відповідно).

1. Створення топології ІТКМ – графа $G_{SW} = \langle V, E \rangle$, де G_{SW} – граф small-world мережі (на основі моделі Watts-Strogatz), $V = \{v_i\}$ – множина вершин, $E = \{e_{ij}\}$ – множина ребер, $i = \overline{1, N}$, $j = \overline{1, N}$. Даний крок здійснюється з використанням програми Pajek, адаптованої під цю задачу, за рахунок заданих топологічних параметрів *N*, *k*, *a*.

2. Сформувати множину $V = \{V^I, V^S, V^R\}$, де $V^I = \{v_i^I\}$ – множина атакуючих вузлів $(|V^I| = I_0)$, $V^R = \{v_i^R\}$ – множина захищених вузлів $(|V^R| = R_0)$, $V^S = \{v_i^S\}$ – множина потенційно вразливих вузлів $(|V^S| = N - I_0 - R_0)$.

3. $\forall v_i^I$, якщо $\exists e_{ij}$ та $v_j \in V^S$, $j = \overline{1, N}$, то з ймовірністю β виконати: $V^S \setminus v_j$ та $V^I \bigcup v_j$; з ймовірністю γ виконати: $V^I \setminus v_i, V^R \bigcup v_i$.

4. Якщо $V^I = \varnothing$ або $\gamma = 0$ та $V^S = \varnothing$, то кінець алгоритму, інакше перейти до п. 3.

Аналізуючи процес інформаційної взаємодії абонентів при поширенні забороненої інформації в ІТКМ, можна зробити наступні висновки. Маємо справу з трьома типами абонентів: атакуючі абоненти, які поширюють заборонену інформацію, захищені абоненти, які характеризуються тим, що не беруть участі в поширенні забороненої інформації і ніколи не будуть цим займатися, і потенційно вразливі абоненти, які можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію. При цьому ми спостерігаємо два протиборчих підпроцеси атаки і захисту абонентів мережі. Для моделювання таких явищ часто застосовують епідеміологічні моделі , зокрема нашому опису відповідає SIR-модель Кермак-Маккендріка. Характер графіків, отриманих у результаті імітаційного моделювання (рис. 3), подібний з результатами, що дає дана модель. Виходячи з вищесказаного, приходимо до висновку, що дана модель є найбільш релевантною для цього дослідження

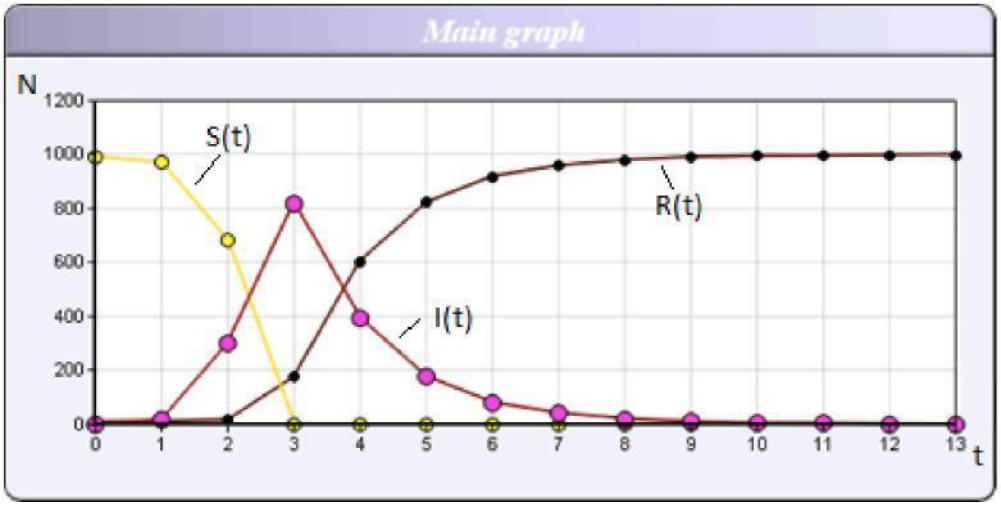


Рисунок 3 – Імітаційне моделювання
($N = 1000$, $\varphi = 20$, $I_0 = 1$, $\beta = 0.5$, $\gamma = 0.5$, $R_0 = 10$), $S(t)$ – кількість схильних до атаки вузлів

SIR–епідеміологічна модель, що спрощено описує поширення захворювання, які передаються від одного індивіда до іншого, яка розглядає суб'єктів з точки зору трьох можливих станів: сприйнятливий, інфікований, імунізований.

Система диференціальних рівнянь, що описують SIR-модель, має вигляд:

$$\begin{cases} \dfrac{\partial I}{\partial t} = \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -\beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (2)$$

де, $I(t)$ – кількість заражених (інфікованих) особин, $S(t)$ – кількість сприятливих особин, $R(t)$ – кількість «виключених з імунізацією» особин, $N = I(t) + S(t) + R(t)$ – кількість особин у популяції, γ – коефіцієнт відновлення / смерті, β – коефіцієнт зараження (інфікування), t – час.

При використанні системи (2) для аналізу ЗПЗІ в ІТКМ отримуємо результати, які хоча і адекватно описують характер процесу, але не дають потрібної точності прогнозу.

На основі проведенго аналізу даних, отриманих за результатами імітаційного моделювання та аналітичного рішення системи (2), і простеживши фізичний зміст рівнянь в даній системі, можна прийти до наступного висновку: процес атаки залежить від структури зв'язків між абонентами в мережі. Параметр топологічної вразливості φ може впливати на $I(t)$ через коефіцієнт β. У загальному вигляді адаптовану систему (2) можна представити в наступному вигляді

$$\begin{cases} \dfrac{\partial I}{\partial t} = 2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (3)$$

Система диференціальних рівнянь (3) дозволяє отримати прогноз ЗПЗІ у великомасштабної ІТКМ ($N = 10^5..10^8$) з похибкою до 18%.

Висновки. Інформаційно-телекомунікаційні мережі є великомасштабними мережами з постійно зростаючим числом абонентів. З бурхливим зростанням кількості користувачів ІТКМ виникають проблеми інформаційної безпеки і захисту інформації в них.

Аналіз проблем інформаційної безпеки виявив, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту.

Створення моделей і алгоритмів поширення загрози забороненої інформації – один з ключових підходів при вирішенні даної задачі. Проведений аналіз публікацій з даної тематики показує, що існуючі рішення малоефективні. Зазвичай при моделюванні поширення загрози забороненої інформації не враховується топологія ІТКМ (модель мережі – повнозв'язний граф). А, якщо топологія враховується, то, як правило, використовується найпростіша SIS модель, а структура мережі відбивається SF мережею. При моделюванні загрози поширення забороненої інформації важливо мати топологію, яка відображатиме структуру зв'язків реальної мережі, а також використовувати адекватну модель інформаційної взаємодії вузлів. Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Розроблено алгоритм реалізації ЗПЗІ в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

Запропонована імітаційна модель ЗПЗІ в ІТКМ, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі.

Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології

реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

ЛІТЕРАТУРА:

1. Кримінальний кодекс України від 05.04.2001 № 2341-III. Дата оновлення: 25.09.2020. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page (дата звернення: 02.09.2020).
2. Про інформацію : Закон України від 02.10.1992 №2657-XII. Дата оновлення: 16.07.2020. URL: http://zakon2.rada.gov.ua/laws/main/2657-12 (дата звернення: 02.09.2020).
3. Про науково-технічну інформацію : Закон України від 25.06.1993 № 3322-XII. Дата оновлення: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (дата звернення: 02.09.2020).
4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (дата звернення: 02.09.2020).
5. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. Дата оновлення: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 02.09.2020).
6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. Дата оновлення: 20.03.2020. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 02.09.2020).
7. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. Дата оновлення: 01.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 02.09.2020).
8. Концепція розвитку системи електронних послуг в Україні. Розпорядження Кабінету Міністрів України від 16.11.2016 р. № 918-р. URL: http://zakon3.rada.gov.ua/laws/show/918-2016-%D1%80 (дата звернення: 02.09.2020).
9. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 02.09.2020).
10. Аналізатор Sniffer Pro LAN. URL: https://www.securitylab.ru/software/233623.php (дата звернення: 02.09.2020).
11. Аналіз та візуалізація дуже великих мереж. URL: http://mrvar.fdv.uni-lj.si/pajek/ (дата звернення: 02.09.2020).
12. Биячуев, Т.А. Безопасность корпоративных сетей: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. – СПб.: СПбГУ ИТМО, 2016.– 161 с.
13.Брэгг, Р., Родс-Оусли, М., Страссберг, К. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг; – М : Эком, 2006. – 912 с.
14.Завдада А.А. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А.А. Завада, О.В. Самчишин, В.В. Охрімчук // Збірник наукових праць ЖВІ НАУ «Інформаційні системи'12», 2012. – Випуск 6. – с. 97 – 106.
15.Загальні рекомендації щодо підвищення рівня захищеності інформаційних ресурсів при віддаленій роботі співробітників установи. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=322B14F318F82FDEB1180D17FE0BFF97.app1?showHidden=1&art_id=320060&cat_id=317163 (дата звернення: 02.09.2020).
16.Kolotov, A. Мониторинг сети с помощью tcpdump. URL: http://www.linuxshare.ru/docs/net/tcpdump.html (дата звернення: 02.09.2020).
17. Лукацький, А.В. Предотвращение сетевых атак: технологии и решения / А.В. Лукацкий. – СПб. : Экспрес Электроника, 2006. – 268 с.
18.Столлингс, В. Основы защиты сетей. Приложения и стандарты / В. Столлингс. – М.: Издательский дом "Вильямс", 2002. – 432 с.
19.Тропіна М. Дослідження соціальних мереж як нового феномену сучасного світу / М. Тропіна // Наукові записки Малої академії наук України. Серія «Педагогічні науки» : [зб. наук. праць ; редкол.: С.О. Довгий (голова), О.Є. Стрижак, О.В. Лісовий, І.М. Савченко та ін.]. — Київ : Національний центр «Мала академія наук України», 2019. — Вип. 16. – С. 57-63 (76 с.)

REFERENCES:

1. Kryminal′nyy kodeks Ukrayiny vid [The Crimean Code of Ukraine from] 05.04.2001 № 2341-III. Data onovlennya: 25.09.2020. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/page (data zvernennya: 02.09.2020).
2. Pro informatsiyu : Zakon Ukrayiny vid [About information : Law of Ukraine from] 02.10.1992 №2657-XII. Data onovlennya: 16.07.2020. URL: http://zakon2.rada.gov.ua/laws/main/2657-12 (data zvernennya: 02.09.2020).
3. Pro naukovo-tekhnichnu informatsiyu : Zakon Ukrayiny vid [About scientific and technical information : Law of Ukraine from] 25.06.1993 № 3322-XII. Data onovlennya: 19.04.2014. URL: http://zakon5.rada.gov.ua/laws/main/3322-12 (data zvernennya: 02.09.2020).
4. Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh : Zakon Ukrayiny vid [On information protection in information and telecommunication systems : Law of Ukraine from] 05.07.1994 № 80/94-VR. Data onovlennya: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (data zvernennya: 02.09.2020).
5. Pro elektronni dovirchi posluhy : Zakon Ukrayiny vid [About electronic trust services : Law of Ukraine from] 05.10.2017 № 2155-VIII. Data onovlennya: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (data zvernennya: 02.09.2020).
6. Pro zakhyst personal′nykh danykh : Zakon Ukrayiny vid [On personal data protection : Law of Ukraine from] 01.06.2010 № 2297-VI. Data onovlennya: 20.03.2020. URL: http://zakon.rada.gov.ua/laws/show/2297-17 (data zvernennya: 02.09.2020).
7. Pro dostup do publichnoyi informatsiyi : Zakon Ukrayiny vid [On access to public information : Law of Ukraine from 13.01.2011] 13.01.2011 № 2939-VI. Data onovlennya: 01.10.2020. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (data zvernennya: 02.09.2020).
8. Kontseptsiya rozvytku systemy elektronnykh posluh v Ukrayini. Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid [The concept of development of the electronic services system in Ukraine. Order of the Cabinet of Ministers of Ukraine from] 16.11.2016 p. № 918-p. URL: http://zakon3.rada.gov.ua/laws/show/918-2016-%D1%80 (data zvernennya: 02.09.2020).
9. Pro zatverdzhennya Zahal′nykh vymoh do kiberzakhystu ob″yektiv krytychnoyi infrastruktury. Postanova Kabinetu Ministriv Ukrayiny vid [On approval of the General requirements for cyber protection of critical infrastructure. Resolution of the Cabinet of Ministers of Ukraine of June 19, 2019] 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (data zvernennya: 02.09.2020).
10. Analizator Sniffer Pro LAN. URL: https://www.securitylab.ru/software/233623.php (data zvernennya: ата звернення: 02.09.2020).
11. Analysis and visualization of very large networks. URL: http://mrvar.fdv.uni-lj.si/pajek/ (data zvernennya: ата звернення: 02.09.2020).
12. Biyachuyev, T.A. (2016), “Bezopasnost' korporativnykh setey” [Security of corporate networks] : ucheb. posobiye / T.A. Biyachuyev; pod red. Osovetskogo L.G. – SPb.: SPbGU ITMO, 161 p.
13. Bregg, R., Rods-Ousli, M., Strassberg, K. (2006) “Bezopasnost' setey. Polnoye rukovodstvo” [Network Security. Complete Guide] / R. Bregg, M. Rods-Ousli, K. Strassberg; – M : Ekom, 912 p.
14. Zavdada A.A. “Analiz suchasnykh system vyyavlennya atak i zapobihannya vtorhnennyam” [Analysis of of modern detection of attacks and prevention of invasions of systems] / A.A. Zavada, O.V. Samchyshyn, V.V. Okhrimchuk // Zbirnyk naukovykh prats′ ZHVI NAU «Informatsiyni systemy″12», 2012. – Vypusk 6, pp. 97 – 106.
15. Zahal′ni rekomendatsiyi shchodo pidvyshchennya rivnya zakhyshchenosti informatsiynykh resursiv pry viddaleniy roboti spivrobitnykiv ustanovy [General recommendations for improving the level of security of information resources in the remote work of employees of the institution] URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=322B14F318F82FDEB1180D17FE0BFF97.app1?showHidden=1&art_id=320060&cat_id=317163 (date of application: 02.09.2020).
16. Kolotov, A. Network monitoring with tcpdump. URL: http://www.linuxshare.ru/docs/net/tcpdump.html (date of application: 02.09.2020).
17. Lukats'kiy, A.V. (2006), “Predotvrashcheniye setevykh atak: tekhnologii i resheniya” [Prevention of network attacks: technologies and solutions] / A.V. Lukatskiy. – SPb. : Ekspres Elektronika, p. 268.
18. Stollings, V. (2002), “Osnovy zashchity setey. Prilozheniya i standarty” [Fundamentals of Network Security. Applications and standards] / V. Stollings. – M.: Izdatel'skiy dom "Vil'yams", p.432.
19. Tropina M. Doslidzhennya sotsial′nykh merezh yak novoho fenomenu suchasnoho svitu [Research of social networks as a new phenomenon of the modern world] / M. Tropina // Naukovi zapysky Maloyi

akademiyi nauk Ukrayiny. Seriya «Pedahohichni nauky» : [zb. nauk. prats′ ; redkol. : S.O. Dovhyy (holova), O.YE. Stryzhak, O.V. Lisovyy, I.M. Savchenko ta in.]. — Kyyiv : Natsional′nyy tsentr «Mala akademiya nauk Ukrayiny», 2019. — Vyp. 16. – pp. 57-63 (p. 76)

к.т.н. , доц. Джулий, Атаманюк А. В.

МОДЕЛЬ БЕЗОПАСНОСТИ РАСПРОСТРАНЕНИЕ ЗАПРЕЩЕННОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Ph.D. Dzhulij V.M., Atamaniuk A.V.

SECURITY MODEL DISSEMINATION OF FORBIDDEN INFORMATION IN INFORMATION AND TELECOMMUNICATION NETWORKS

Джулій Володимир Миколайович, кандидат технічних наук, доцент кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету (Хмельницький, Україна)

Атаманюк Алла Василівна, магістр кафедри кібербезпеки та комп'ютерних систем і мереж Хмельницького національного університету (Хмельницький, Україна)

Джулий Владимир Николаевич, кандидат технических наук, доцент кафедры кибербезопасности та компьютерных систем и сетей Хмельницкого национального университета (Хмельницкий, Украина)

Атаманюк Алла Васильевна, магистр кафедры кибербезопасности та компьютерных систем и сетей Хмельницкого национального университета (Хмельницкий, Украина)

Dzhuliy V.M., candidate of technical Sciences, associate Professor of the Department of cybersecurity the computer systems and networks Khmelnitsky national University (Khmelnitsky, Ukraine)

Atamaniuk A.V., master of the Department of cybersecurity the computer systems and networks Khmelnitsky national University (Khmelnitsky, Ukraine)

д.т.н., проф. Лєнков С.В. (ВІКНУ)
к.т.н., доц. Джулій В.М. (ХмНУ)
к.т.н., доц. Хмельницький Ю.В. (ХмНУ)
Атаманюк А.В. (ХмНУ)

Проблеми інформаційної безпеки в інформаційно-телекомунікаційних мережах

Створення моделей і алгоритмів поширення загрози забороненої інформації - одна з ключових завдань в даному напрямку. При її вирішенні виникають проблеми, пов'язані з властивостями даної інформаційно-телекомунікаційної системи, а саме:

1. Відсутність перевірки достовірності даних про вузол системи. Дуже часто абоненти інформаційно-телекомунікаційних мереж (ІТКМ) вказують недостовірну інформацію про себе.

2. Закритість системи. Структура і інформація про управління системою є конфіденційною інформацією.

3. Проблема збору інформації. Неможливо отримати повну інформацію про топології ІТКМ. Існує можливість для звичайного абонента збору інформації про структуру мережі (функції API), але ця можливість має багато обмежень (налаштування приватності, часовий інтервал).

Нас цікавить тільки обмін повідомленнями між абонентами, тому концептуальна математична модель інформаційної взаємодії представляється графом, вузлами якого є абоненти, а ребрами - зв'язки між ними. Перерахуємо властивості графа, принципові для дослідження:

1. Велика розмірність. Система містить мільйони елементів.

2. Гетерогенність. У графі, який відображає взаємозв'язок елементів в системі, вершини мають різну кількість прилеглих ребер.

3. Динаміка зв'язків. В системі протягом часу відбуваються зміни зв'язків.

4. Динаміка вузлів. Протягом часу змінюється кількість вузлів (елементів) системи.

5. Наявність груп вузлів, що мають велику кількість зв'язків всередині і невелику - між групами.

Граф, який представляє систему, володіє певною кластеризацією. Для таких систем характерно, що два вузли, які мають зв'язки до якого-небудь вузла, часто також мають зв'язок між собою.

Найбільш ефективне прогнозування поширення загрози забороненої інформації здійснюється за допомогою моделювання даного процесу. Таким чином, ми приходимо до задачі моделювання ІТКМ за допомогою їх математичної моделі (графів).

Список використаних джерел:

1. Биячуев, Т.А. Безопасность корпоративных сетей [Текст]: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. - СПб.: СПбГУ ИТМО, 2016. - 161 с.

Дослідження проблем інформаційної безпеки в інформаційнотелекомунікаційних мережах

Атаманюк А.В., Джулій В.М., Кльоц Ю.П.
Хмельницький національний університет

Інформаційно-телекомунікаційна мережа надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярними з них є соціальні мережі. З бурхливим ростом кількості користувачів інформаційно-телекомунікаційних мереж виникають і проблеми безпеки в них.

Розглянемо існуючі проблеми інформаційної безпеки в інформаційнотелекомунікаційних мережах, які актуальні для даного дослідження:

1. Використання глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи. Найбільш вразливими компонентами системи, що часто атакуються, є: сервери; робочі станції; середовище передачі інформації; вузли комутації. Типові інформаційні впливи зловмисників:

- Прослуховування мережевого трафіку. Щоб прослухати трафік (sniffing) мережевий адаптер переводиться в «безладний» режим. У цьому режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даною адресою, як в нормальному режимі функціонування-технології – ARP Spoofing (ARP-poisoning), MAC Flooding і MAC Duplicating. Перехоплення здійснюється з використанням мережевих моніторів, з яких найбільш функціональними є Sniffer Pro від компанії Sniffer Technologies, IRIS Network Traffic Analyzer від компанії EYE і TCP Dump.

Наслідки. Сучасні мережеві протоколи (TCP / IP, ARP, HTTP, FTP, SMTP, POP3 тощо) не мають механізмів захисту (дані передаються у відкритому вигляді). Зловмисник, що перехоплює трафік між сервером і будьяким вузлом мережі, може заволодіти аутентифікаційними даними користувача (отримати пароль).

Протидія. Відомо ряд методів визначення наявності запущеного сніфера в мережі, наприклад метод пінга, метод ARP, метод DNS і метод пастки.

- Сканування вразливостей. Результатом роботи сканера є інформація про систему, що містить список мережевого обладнання, комп'ютерів з запущеними на них службами, версіями мережевого ПЗ (а отже і вразливостей, властивих даному ПЗ), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаку. Саме результати сканування дозволяють точно підібрати експлойти для здійснення безпосереднього НСД.

Виявлення. Само по собі сканування не є незаконним. Однак, якщо сканування з боку зовнішньої, по відношенню до системи, мережі звичайне явище, то сканування комп'ютерів з внутрішньої мережі – безумовно, інцидент безпеки, що вимагає негайної реакції з боку мережевого адміністратора. Виявити кроки сканування можна, вивчаючи журнали реєстрації міжмережевих екранів (МЕ). Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти. Тому сучасні МЕ і системи виявлення вторгнень СВВ мають модулі (plug-in), що дозволяють виявити сканування в режимі реального часу. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють здійснювати сканування максимально приховано. Наприклад, в Nmap існують можливості, що дозволяють значно ускладнити виявлення сканування для СВВ.

Протидія. Використання мережевих СВВ, або періодичне вивчення журналів реєстрації МЕ.

- Мережеві атаки. Мережеві атаки можна розділити на: атаки, засновані на переповненні буфера (overflow based attacks). Вони використовують вразливість системи, яка полягає в некоректній програмної обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями; атаки, спрямовані на відмову в обслуговуванні (Denial Of Service attacks). Атаки не обов'язково використовують вразливості в ПЗ системи, що атакується.

Порушення працездатності системи відбувається через те, що дані, що їй посилають, призводять до значної витрати ресурсів системи. Найпростішим прикладом атаки цього типу є атака «Ping Of Death». Суть її в наступному: на комп'ютер жертви надсилається сильно фрагментований ICMP-пакет великого розміру. Реакцією ОС Windows на отримання такого пакету є повне зависання.

- Атаки, засновані на використанні вразливостей в ПЗ мережевих додатків – експлойти (exploit). Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Експлойти є шкідливими програмами, що реалізують відому вразливість в ОС або прикладному ПЗ, для отримання НСД до вразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій подавлення антивірусних програм і МЕ. Наслідки застосування експлойтів можуть бути самими критичними. У випадку отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути такими: впровадження троянської програми, впровадження набору утиліт для приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких та зовнішніх носіїв інформації, створення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлів з хешами паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи.

Протидія. МЕ і СОВ, встановлені на системі, що атакується, в деяких випадків не в змозі відобразити дію експлойтів. Для успішного відображення атак експлойтів засоби захисту необхідно оновлювати, оскільки механізм виявлення вторгнень заснований на розпізнаванні сигнатур вже відомих атак. Хоча є розробки, здатні за завіреннями розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

- Шкідливі програми. Шкідливі програми – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів або якого іншого впливу, що перешкоджає нормальному функціонуванню мережі. До шкідливих програми відносяться комп'ютерні віруси, троянські коні, мережеві черв'яки тощо.

Протидія. Типовим методом протидії є застосування антивірусних засобів, що працюють в режимі реального часу (моніторів). Для виявлення троянських програм існує спеціалізоване програмне забезпечення.

2. Проблема забороненого контенту. Залежно від законодавства країни різні матеріали можуть вважатися нелегальними. У більшості країн заборонені: матеріали сексуального характеру за участю дітей і підлітків, порнографічний контент, описи насильства, в тому числі сексуального, екстремізм і розпалювання расової ненависті. В українському законодавстві кілька законів регулюють питання надання інформації про фізичних та юридичних осіб, а саме: Закон України «Про інформацію» від 02.10.92, що регулює відносини щодо одержання і поширення інформації; Закон України «Про захист персональних даних» від 01.06.2010, що визначає захист і обробку персональних даних; Закон України «Про доступ до публічної інформації» від 13.01.2011, який надає право на отримання інформації, що знаходиться у володінні розпорядників.

Аналогічно з концепцією забезпечення комплексного захисту об'єкта інформатизації, можна сформувати повну множину функцій захисту від забороненої інформації. Під функцією захисту (ФЗ) розуміється сукупність однорідних в функціональному відношенні заходів, що регулярно здійснюються в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

Перелік повної множини функцій захисту від забороненої інформації в соціальних мережах:

1. Попередження умов виникнення забороненої інформації. Функція реалізується за допомогою нормативно-правових актів. Вона не може повністю виключити загрозу поширення забороненої інформації в соціальних мережах, так як в цілому ситуація з дотриманням законів незадовільна, а в інтернет-просторі загострюється через технічні складнощі.

2. Попередження безпосередньої прояви забороненої інформації. Функція реалізується за рахунок механізмів прогнозування поширення забороненої інформації в соціальній мережі.

3. Виявлення забороненої інформації, яка проявилася. Функція пов'язана з моніторингом ІТКМ на предмет забороненої інформації на сторінках абонентів. Як правило, для реалізації даного захисту використовується різні СОРМ (система оперативно-розшукових заходів). Дана ФЗ пов'язана з проблемами контекстного пошуку, а також необхідністю контролю над всією системою.

4. Попередження впливу на абонентів забороненої інформації, яка проявилася. Функція може бути реалізована за допомогою автоматичного пересилання повідомлення з попередженням

про відповідальність за розповсюдження забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до керування системи та нелегітимними – при його відсутності (зламання акаунта). ФЗ ділиться на дві функції. Перша пов'язана з попередженням абонентів, на сторінках яких була знайдена заборонена інформація, а друга – з розсилкою попереджень потенційним одержувачам забороненої інформації.

5. Виявлення впливу забороненої інформації на абонентів. Функція пов'язана безпосередньо з фіксацією процесу поширення забороненої інформації, може бути реалізована через контекстний аналіз повідомлень.

6. Локалізація, обмеження впливу забороненої інформації на абонентів. Функція реалізується через блокування абонентів, що поширюють заборонену інформацію, або абонентів – потенційних розповсюджувачів. Дана ФЗ опирається на попередні функції і для її ефективної реалізації необхідний контроль над системою.

7. Ліквідація наслідків виявленого впливу забороненої інформації на абонентів. Функція пов'язана з видаленням забороненої інформації з системи. Для реалізації даної функції також необхідний контроль над системою.

На основі проведеного аналізу функцій захисту видно, що найбільш ефективні функції – це перші функції, оскільки вони забезпечують захист на початкових етапах. Наведені функції захисту мають свої недоліки. Найбільш перспективною ФЗ інженерно-технічного напряму є ФЗ2. На даному етапі, маючи інформацію про топології ІТКМ і потенційних розповсюджувачів забороненої інформації, можливе прогнозування процесу її поширення.

Одним з підходів до прогнозування загрози поширення забороненої інформації (ЗПЗІ) є моделювання, наприклад, з використанням моделей впливу, моделей просочування і зараження. Дані моделі, як правило, не враховують топологічні особливості мережі (розподіл ступенів зв'язності, кластерний коефіцієнт, середня довжина шляху). Взаємодія між абонентами в межах цих математичних моделей описується переважно гомогенним
графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування загрози поширення забороненої інформації більше 30%. Крім того, дані підходи мають в основному теоретичний характер, практика їх використання не виходить за межі експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів загрози поширення забороненої інформації, актуальні і мають теоретичне і практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Проведене дослідження проблем інформаційної безпеки виявило, що крім проблем, пов'язаних з використанням глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи, які досить добре відомі і можна вирішити, існує маловивчена проблема забороненого контенту, існуючі рішення малоефективні.

Ще однією важливою проблемою є великомасштабність ІТКМ, яка заважає отримати дані з імітаційної моделі за прийнятний час. Розв'язання цієї задачі полягає у створенні аналітичної моделі загрози поширення забороненої інформації в ІТКМ.

Перелік посилань

1. Биячуев, Т.А. Безопасность корпоративных сетей: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. – СПб.: СПбГУ ИТМО, 2016.– 161 с.

2. Лукацький, А.В. Предотвращение сетевых атак: технологии и решения / А.В. Лукацкий. – СПб. : Экспрес Электроника, 2014. – 268 с.

3. Тропіна М. Дослідження соціальних мереж як нового феномену сучасного світу / М. Тропіна // Наукові записки Малої академії наук України. Серія «Педагогічні науки» : [зб. наук. праць ; редкол. : С.О. Довгий (голова), О.Є. Стрижак, О.В. Лісовий, І.М. Савченко та ін.]. — Київ : Національний центр «Мала академія наук України», 2019. — Вип. 16. – С. 57-63

Контактні дані авторів:

Атаманюк Алла Василівна: - credema2008@gmail.com

Джулій Володимир Миколайович: - dg2303@ukr.net

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії,
облікових та фінансових
дисциплін Хмельницького
кооперативного коледжу
Хмельницького кооперативного
торгово-економічного
інституту

_____ К.В. Трофименко
«___» _____ 2020 р.

АКТ

Про впровадження результатів магістерського дослідження Атаманюк А.В. на тему «Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах»

Науково-технічна комісія склала цей акт про те, що результати магістерського дослідження, а саме модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах та методика формування топології великомасштабної інформаційно-телекомунікаційної мережі, впроваджено для використання.

Очікується, що застосування цієї методики забезпечить проведення збору даних про топологію з будь-якого вузла-абонента; унеможливить загрозу поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Голова комісії _____ Трофименко К.В.
(підпис) (прізвище та ініціали)

ЗАТВЕРДЖУЮ

ТОВ "РЕКСДІДЖИТАЛ"

«02» 12 2020 р.

АКТ

Про впровадження результатів дипломної роботи магістра Атаманюк А.В. на тему «Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах»

Науково-технічна комісія під головуванням Кожак Є.В

склала цей акт про те, що результати магістерського дослідження, а саме:

- модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах;
- методику формування топології великомасштабної інформаційно-телекомунікаційної мережі, що включає: алгоритм формування графа доступної частини мережі, що дозволяє провести збір даних про топологію з будь-якого вузла-абонента; алгоритм формування повного графа мережі, що дозволяє в умовах неповноти вихідних даних спрогнозувати топологію частини мережі, якої бракує;

впроваджено для використання у роботі відділу інформаційно-технічного забезпечення ТОВ "РЕКС Діджитал".

Дана програмно-апаратна система буде використовуватися для проведення збору даних про топологію з будь-якого вузла-абонента.

Очікується, що розроблене програмне забезпечення дозволить за прийнятний час отримати результати моделювання загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах за рахунок використання розподілених обчислювальних ресурсів.

Голова комісії Кожак Є.В. _____ _____
(підпис) (прізвище та ініціали)

Члени комісії _____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

_____ _____
(підпис) (прізвище та ініціали)

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«ДАТАРОБОТ УКРАЇНА»
Код ЄДРПОУ 39636281, 01030, Україна, м. Київ, вул. Богдана Хмельницького, буд.44
тел. 099 13 63 255

ЗАТВЕРДЖУЮ
ТОВ "Датаробот Україна"
_____
«02» 12 2020 р.

АКТ

Про впровадження результатів дипломної роботи магістра Атаманюк А.В. на тему «Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах»

Науково-технічна комісія під головуванням спеціаліста відділу інформаційно-технічного забезпечення Пихтіна Володимира Євгенійовича склала цей акт про те, що результати магістерського дослідження, а саме:

модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах;

- методику формування топології великомасштабної інформаційно-телекомунікаційної мережі, що включає: алгоритм формування графа доступної частини мережі, що дозволяє провести збір даних про топологію з будь-якого вузла-абонента; алгоритм формування повного графа мережі, що дозволяє в умовах неповноти вихідних даних спрогнозувати топологію частини мережі, якої бракує;

впроваджено для використання у роботі відділу інформаційно-технічного забезпечення ТОВ “Датаробот Україна”. Дана програмно-апаратна система буде використовуватися для проведення збору даних про топологію з будь-якого вузла-абонента.

Очікується, що розроблене програмне забезпечення дозволить за прийнятний час отримати результати моделювання загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах за рахунок використання розподілених обчислювальних ресурсів.

Голова комісії

_____ Пихтін В.Є.
(підпис) (прізвище та ініціали)

Члени комісії

_____ Турчин В.В.
(підпис) (прізвище та ініціали)

_____ Карпович А.В.
(підпис) (прізвище та ініціали)

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«ДАТАРОБОТ УКРАЇНА»
Код ЄДРПОУ 39636281, 01030, Україна, м. Київ, вул. Богдана Хмельницького, буд.44

тел. 099 13 63 255

15.10.2018 м. Київ

Повідомляємо Вас, що згідно з оновленою версією Статуту від 19.09.2018 року , Товариство з обмеженою відповідальністю «Датаробот Україна» працює без печатки.

Звертаємо Вашу увагу , що дані дії підприємства не суперечать нормам Наказу Міністерства фінансів України від 24.05.1995 року №88 «Про затвердження Положення про документальне забезпечення записів у бухгалтерському обліку».

З повагою,

Директор Піддубний А.В.

Додаток В

(обов’язковий)

Презентація

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

АТАМАНЮК Алла Василівна

МЕТОД ВИЯВЛЕННЯ ЗАГРОЗИ ПОШИРЕННЯ ЗАБОРОНЕНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Науковий керівник
к.т.н., доцент Джулій В.М.

кафедра кібербезпеки та комп'ютерних систем і мереж

Тема Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Мета магістерської роботи полягає в підвищенні точності прогнозування загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

Наукова задача – розробка методу виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Об'єкт дослідження: інформаційно-телекомунікаційні мережі, що знаходяться під впливом загрози поширення забороненої інформації.

Предмет дослідження: моделі загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Задачі досліджень у роботі формулюються наступним чином:

1. Виконати аналіз основних підходів до моделювання загрози поширення забороненої інформації.
2. Розробити імітаційну модель загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.
3. Синтезувати і показати адекватність аналітичної моделі загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.
4. Розробити методику формування топології інформаційно-телекомунікаційної мережі.
5. Змоделювати процес реалізації загрози поширення забороненої інформації на топології реальної великомасштабної інформаційно-телекомунікаційної мережі з використанням розробленого програмного забезпечення. Провести експериментальне дослідження за отриманими результатами.

Наукова новизна роботи визначає:

1. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах
2. Методику формування топології великомасштабної інформаційно-телекомунікаційної мережі, що включає:

- алгоритм формування графа доступної частини мережі, що дозволяє провести збір даних про топологію з будь-якого вузла-абонента;
- алгоритм формування повного графа мережі, що дозволяє в умовах неповноти вихідних даних спрогнозувати топологію частини мережі, якої бракує.

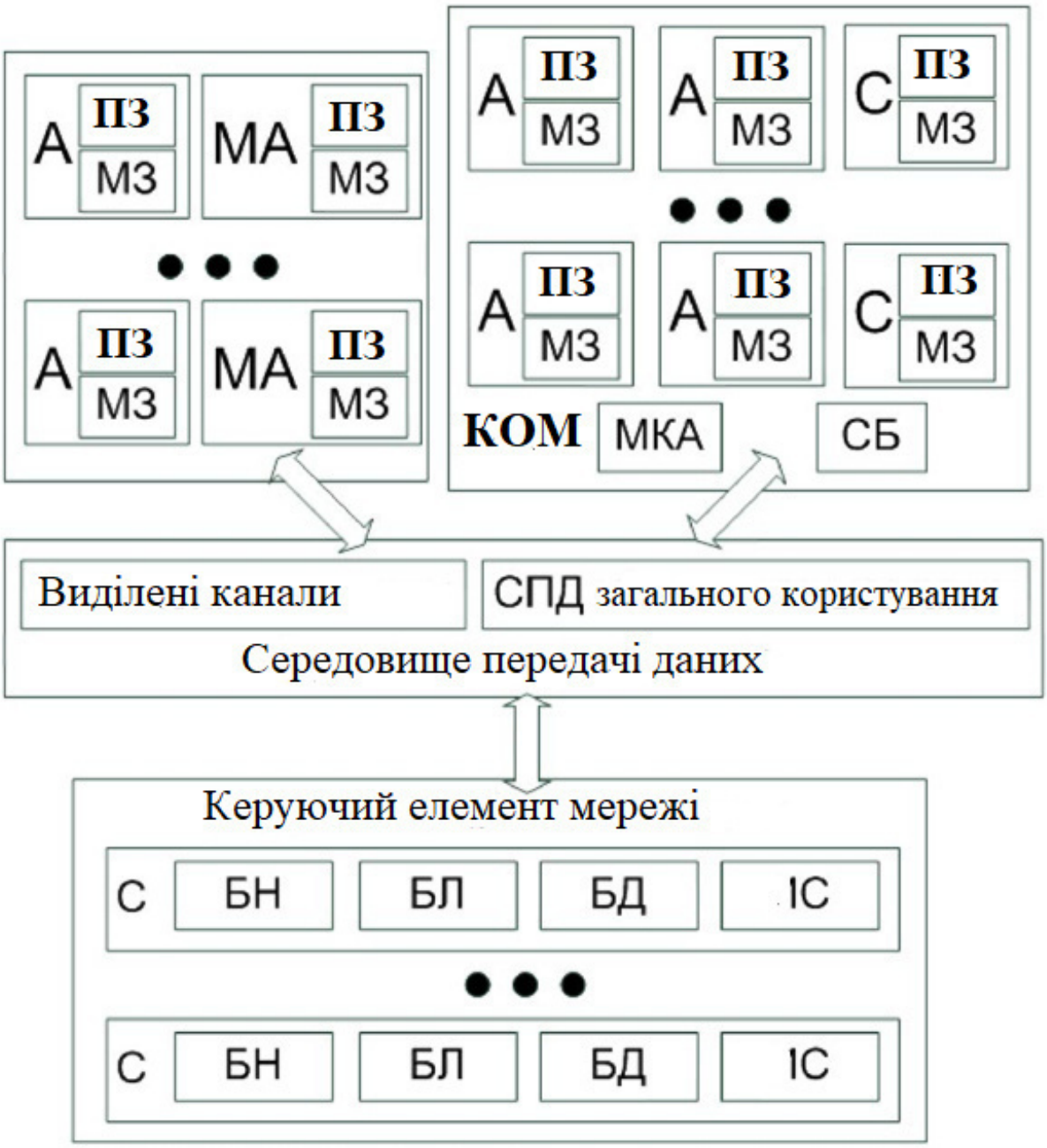
Методика проведення досліджень. При вирішенні задач, що поставлені в магістерській роботі, використовувались аналітичні і експериментальні дослідження. Аналітичні методи ґрунтуються на теорії диференціального числення, на теорії статистичних рішень і методах математичної статистики. При вирішенні поставлених завдань використовувалися методи теорії диференціального числення, теорії графів. Рішення сформульованої в магістерській роботі, проблеми розробки моделей і алгоритмів виявлення загроз поширення забороненої інформації в інформаційно-телекомунікаційних мережах, базується на методах системного аналізу, теорії ймовірності, випадкових процесів і математичної статистики, методів чисельного аналізу, імітаційного моделювання.

Практична цінність Практична цінність результатів магістерської роботи полягає в отриманих розрахункових виразах, моделях і алгоритмах, що реалізують виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах.

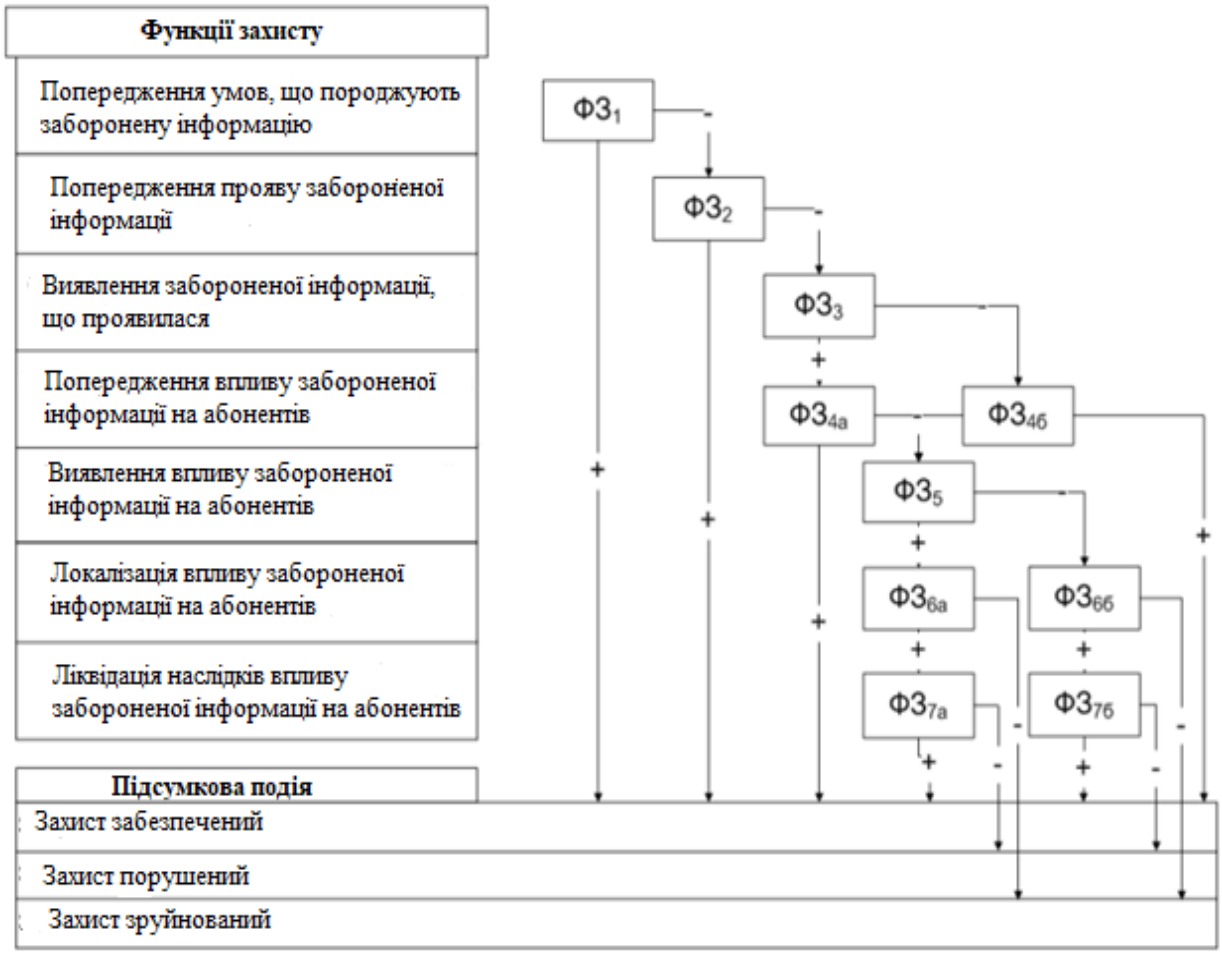
Апробація роботи. Наукові результати і основні положення магістерської роботи доповідались і обговорювались на всеукраїнських та міжнародних науково-технічних конференціях,

Публікації. По темі магістерської роботи опубліковано 2 статті (1 статтю у фаховому журналі, 1 статтю у нефаховому збірнику наукових праць), 1 – теза доповіді на всеукраїнській конференції.

Структурна схема ІТКМ



Функції захисту від забороненої інформації в ІТКМ



Аналітична модель динаміки атаки $I(t)$ та модель захисту вузлів $R(t)$

Аналітична модель динаміки атаки $I(t)$ та модель захисту вузлів $R(t)$ представлені наступним чином:

$$\begin{cases} I(t) = f(N, \beta, \gamma, \varphi, t) \\ R(t) = g(N, \beta, \gamma, \varphi, t) \end{cases}$$

де, N – кількість вузлів, яка дорівнює кількості абонентів мережі,

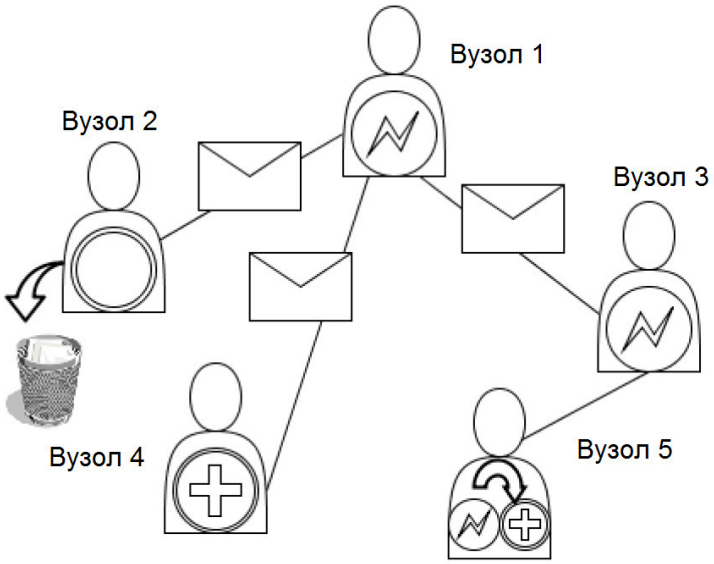
β – параметр, що відображає силу загрози, ймовірність здійснення атаки,

γ – параметр, що відображає ступінь протидії загрозі, ймовірність захисту абонента (β і γ в даному дослідженні визначено як константи, але можуть бути виражені як функції, що залежать від психосемантичних профілів абонентів ІТКМ),

φ – коефіцієнт топологічної вразливості мережі, що відображає внутрішню властивість ІТКМ, засновану на характеристиках її топології, яке сприяє поширенню забороненої інформації ,

t – час процесу (в умовних одиницях часу).

Схема реалізації загрози поширення забороненої інформації в ІТКМ



Імітаційна модель ЗПЗІ в ІТКМ

Вхідні дані: N, k – середній ступінь зв'язності вузлів, a – параметр, що відображає середню довжину шляху і рівень мережевої кластеризації, β, γ (в моделі вважається, що β та γ однакові для кожного абонента), I_0 - кількість абонентів-зловмисників - початкових джерел загроз, R_0 - кількість абонентів спочатку несприйнятливих до атакуючих дій.

Вихідні дані: $I(t), R(t), S(t)$ – чисельні масиви даних, що описують динамічний процес реалізації ЗПЗІ (кількості атакуючих, захищених і потенційно вразливих вузлів у кожну умовну одиницю часу відповідно).

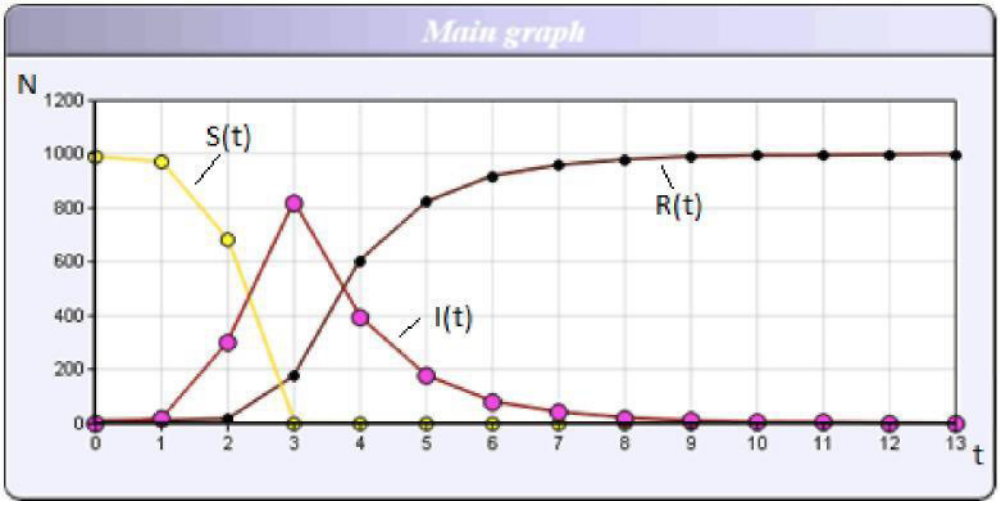
1. Створення топології ІТКМ – графа $G_{SW} = \langle V, E \rangle$, де G_{SW} – граф small-world мережі (на основі моделі Watts-Strogatz), $V = \{v_i\}$ – множина вершин, $E = \{e_{ij}\}$ – множина ребер, $i = \overline{1, N}$, $j = \overline{1, N}$. Даний крок здійснюється з використанням програми Pajek, адаптованої під цю задачу, за рахунок заданих топологічних параметрів N, k, a.

2. Сформувати множину $V = \{V^I, V^S, V^R\}$, де $V^I = \{v_i^I\}$ – множина атакуючих вузлів $\left(\left|V^I\right| = I_0\right)$, $V^R = \{v_i^R\}$ – множина захищених вузлів $\left(\left|V^R\right| = R_0\right)$, $V^S = \{v_i^S\}$ – множина потенційно вразливих вузлів $\left(\left|V^S\right| = N - I_0 - R_0\right)$.

3. $\forall v_i^I$, якщо $\exists e_{ij}$ та $v_j \in V^S, j = \overline{1, N}$, то з ймовірністю β виконати: $V^S \setminus v_j$ та $V^I \bigcup v_j$; з ймовірністю γ виконати: $V^I \setminus v_i, V^R \bigcup v_i$.

4. Якщо $V^I = \varnothing$ або $\gamma = 0$ та $V^S = \varnothing$, то кінець алгоритму, інакше перейти до п. 3.

Імітаційне моделювання (*N* = 1000, $\varphi = 20,\ \ I_0 = 1,\ \beta = 0.5,\ \gamma = 0.5,\ R_0 = 10$**),** $S(t)$ **– кількість схильних до атаки вузлів**



SIR–епідеміологічна модель

Система диференціальних рівнянь, що описують SIR-модель, має вигляд:

$$\begin{cases} \dfrac{\partial I}{\partial t} = \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -\beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (1)$$

де, $I(t)$ – кількість заражених (інфікованих) особин, $S(t)$ – кількість сприятливих особин, $R(t)$ – кількість «виключених з імунізацією» особин, $N = I(t) + S(t) + R(t)$ – кількість особин у популяції, γ – коефіцієнт відновлення / смерті, β – коефіцієнт зараження (інфікування), t – час.

У загальному вигляді адаптовану систему (1) можна представити в наступному вигляді

$$\begin{cases} \dfrac{\partial I}{\partial t} = 2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} - \gamma \cdot I(t) \\ \dfrac{\partial R}{\partial t} = \gamma \cdot I(t) \\ \dfrac{\partial S}{\partial t} = -2 \cdot \ln \varphi \cdot \beta \cdot \dfrac{S(t) \cdot I(t)}{N} \end{cases} \quad (2)$$

Розподілене моделювання загрози поширення забороненої інформації в ІТКМ

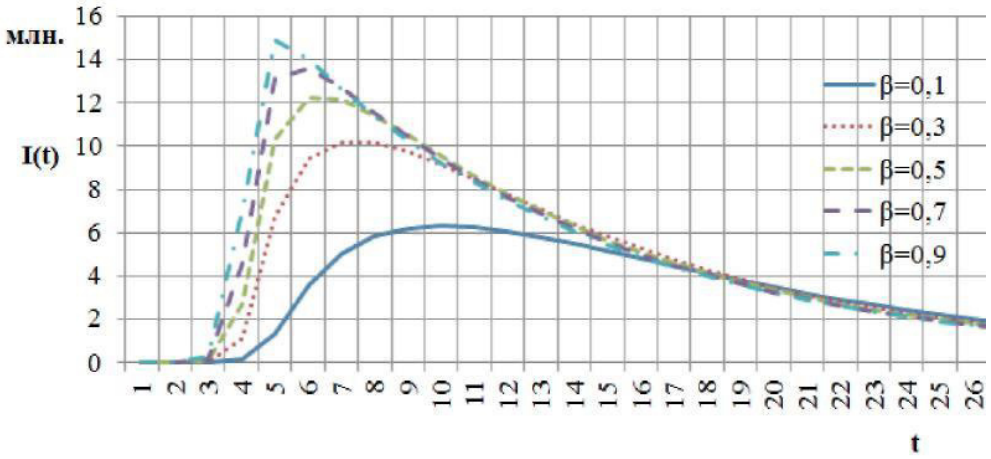


Рисунок 1 – Результати моделювання з параметрами $\gamma = 0{,}1$, $I_0 = 1$, $R_0 = 0$

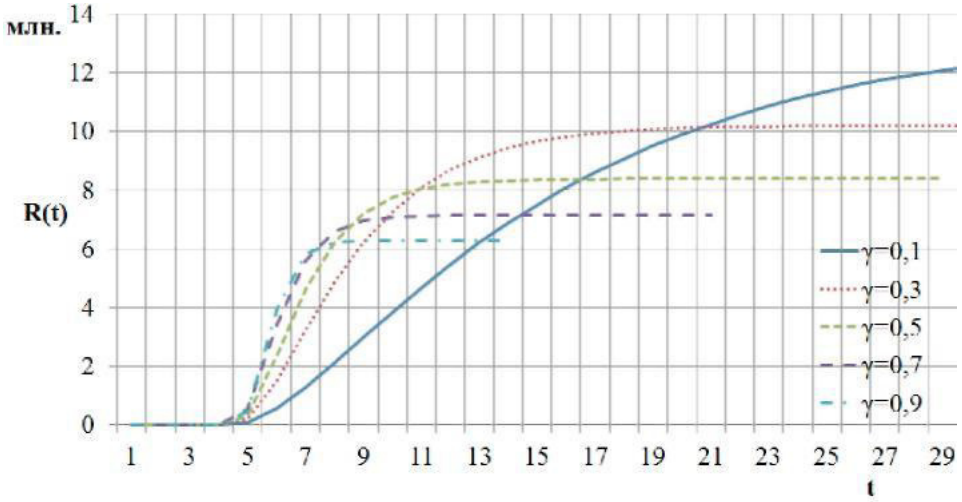


Рисунок 2 – Результати моделювання з параметрами $\beta = 0{,}2$, $I_0 = 1$, $R_0 = 0$

ВИСНОВКИ

В рамках дослідження за результатами магістерської роботи отримано рішення науково-технічної задачі розробки моделей і алгоритмів загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах. Основні результати роботи:

1. Розроблено алгоритм реалізації ЗПЗІ в ІТКМ, заснований на характерах процесів, що протікають в реальних умовах.

2. Запропонована імітаційна модель ЗПЗІ в ІТКМ, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем. З її допомогою проведені експерименти, результати яких показали залежність реалізації ЗПЗІ від топологічної уразливості мережі.

3. Розроблено аналітичну модель ЗПЗІ з урахуванням топологічної уразливості мережі. Релевантність результатів аналітичного рішення підтверджена серією експериментів на топології реальної мережі з використанням імітаційного моделювання. При цьому похибка для процесу захисту склала не більше 10%, для процесу атаки – не більше 15%.

4. Розроблено методику формування топології ІТКМ, яка враховує основні топологічні характеристики доступної частини мережі і працює в умові недостатньої репрезентативності вибірки вихідних даних. Запропонована методика складається з послідовності розроблених алгоритмів.

5. Створено алгоритм формування вихідних даних про топологію мережі (безлічі вершин і зв’язків між ними доступною частини мережі), який враховує обмеження зі збору даних і реалізований у вигляді розробленого програмного забезпечення.

6. Розроблено алгоритм формування повного графа мережі з урахуванням додавання недоступної частини на основі обчислених прогнозованих топологічних характеристик. Алгоритм реалізований у вигляді розробленого програмного забезпечення.

7. Введена оцінка топологічної уразливості мережі (вектор топологічної уразливості), що враховує такі параметри: середню довжину шляху мережі, коефіцієнт кластеризації мережі, середній ступінь зв’язності мережі і загальна кількість вузлів в мережі.

8. Розроблено програмне забезпечення, яке дозволяє за прийнятний час отримати результати моделювання ЗПЗІ в ІТКМ за рахунок використання розподілених обчислювальних ресурсів.

UNICHECK

User name:
Kafedra kiberbezpeky

Check ID:
1005347291

Check date:
03.12.2020 14:20:56 EET

Check type:
Doc vs Internet

Report date:
03.12.2020 14:22:37 EET

User ID:
100005590

File name: **Атаманюк**

Page count: **106** Word count: **17134** Character count: **122127** File size: **3.76 MB** File ID: **1005639678**

Text modifications detected (similarity score might be affected)

15.1% Matches

Highest match: **8.08%** with Internet source (**http://inmad.vntu.edu.ua/portal/static/0A0C3506-D8C4-4C2D-9795-87006660F6E5.doc**..

15.1% Internet sources | 671 ..... Page 108

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters | 25

Suspicious formatting | 19 Pages

Tue Dec 01 09:25:17 EET 2020, Муляра І.В, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 26.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 10%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 81780 Название: Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах Добавлено в БД: 2020-12-01 Авторы: А.В. Атаманюк Руководители: В.М. Джулій Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	93766	800	25557 (27%)	258 (32%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы
33097	Название: Метод виявлення загрози поширення забороненої до розповсюдження інформації в комп'ютерних мережах Добавлено в БД: 2017-01-04 Авторы: Юмашов В.С. Руководители: Бойчук В.О. Консультанты: Опоненты:	24528 (26.0%)	269 (34.0%)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРІ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Автор: Атаманюк Алла Василівна

Спеціальність: 123 Компютерна інженерія

Освітня програма:

Науковий керівник: Джулій Володимир Миколайович

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Виявлені запозичення є законними. Допускається до захисту

4.12.2025

Дата Підписи

Клюя Ю.М.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Атаманюк Алла Василівна

Тема Метод виявлення загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах

Спеціальність 123 Комп'ютерна інженерія

Спеціалізація Програмування та захист комп'ютерних систем і мереж

Обсяг дипломної роботи освітнього ступеня «магістр»:

кількість листів креслень 10 ; кількість сторінок записки 102

1. Короткий зміст роботи та прийнятих рішень У магістерській роботі проведено аналіз основних підходів до моделювання загрози поширення забороненої інформації. Розроблено імітаційну модель загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах. На її основі змодельовано процес реалізації загрози поширення забороненої інформації на топології реальної великомасштабної інформаційно-телекомунікаційної мережі з використанням розробленого програмного забезпечення. Проведено експериментальне дослідження за отриманими результатами

2. Висновок про відповідність роботи дипломному завданню Дипломна робота освітнього ступеня «магістр» у повній мірі відповідає поставленому завданню як у теоретичній, так і в практичній її частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи У вступі обґрунтовується актуальність теми роботи, дається аналіз досліджуваної проблеми та обґрунтовується застосовуваний підхід до її вирішення, формулюються цілі і завдання дослідження, описується наукова новизна та практична значимість отриманих результатів. У першому розділі якісно та в повній мірі проведено аналіз та дослідження поширення забороненої інформації в інформаційно-телекомунікаційних мережах. Наступні розділи присвячені розробці методики формування топології великомасштабної інформаційно-телекомунікаційної мережі, особливостям реалізації автоматизованої системи протидії загрозі поширення забороненої інформації.

4. Позитивні сторони роботи Дипломна робота містить низку інноваційних рішень, зокрема, у методиці формування топології великомасштабної інформаційно-телекомунікаційної мережі, що включає: алгоритм формування графа доступної частини мережі, що дозволяє провести збір даних про топологію з будь-якого вузла-абонента; алгоритм формування повного графа мережі, що дозволяє в умовах неповноти вихідних даних спрогнозувати топологію частини мережі, якої бракує.

5. Негативні сторони роботи Запропонована імітаційна модель загрози поширення забороненої інформації в інформаційно-телекомунікаційних мережах, що враховує топологічні характеристики мережі. Постає питання, чи можна було цю модель реалізувати аналітично?

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

7. Відгук про роботу в цілому В цілому дипломна робота заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи є послідовними та логічними, що дозволяє чітко розуміти викладений матеріал у рамках тематики дипломної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для вирішення поставленої задачі.

8.Інші зауваження

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

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)

Бедратюк Леонід Петрович, д.ф.-м.н. завідувач кафедри інженерії програмного забезпечення Хмельницького національного університету

« 04 » 12 2020р.

(підпис)