МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютернихінформаційнихтехнологій

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

Савченко А.С.

«___»_____2020 р.

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"МАГІСТРА"

ЗА СПЕЦІАЛІЗАЦІЄЮ "ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ (ЗА ГАЛУЗЯМИ)"

Тема: «Захист інформаційно-телекомунікаційних мереж від шкідливої інформації »

Виконавець: Ігнатенко Вадим Анатолійович

Керівник: д.т.н., проф.Зіатдінов Юрій Кашафович

Нормоконтролер): Райчев І.Е.

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕСИТЕТ

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра комп’ютерних інформаційних технологій

Галузь знань 12 «Інформаційні технології»

Спеціальність 122 «Комп’ютерні науки»

Спеціалізація «Інформаційні управляючі системи та технології (за галузями)»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Савченко А.С.

“ ” _____2019р.

З А В Д А Н Н Я

на виконаннядипломноїроботи студента

Ігнатенко ВадимаАнатолійовича

(прізвище, ім’я, побатькові)

1. Тема роботи(проекту): «Захист інформаційно-телекомунікаційних мереж від шкідливої інформації» затверджена наказом ректора №2175/ст.від 25.09.2019р.
2. Термін виконанняроботи (проекту): з 14.10.2019р. по 03.02.2020р.
3. Вихідні данні дороботи (проекту):завдання на розробку проекту захисту комп’ютерних мереж від шкідливої інформації, література з питань захисту комп’ютерних мереж.
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):дослідити сучасні моделі розповсюдження шкідливої інформації в мережах, дослідити множину функцій захисту від забороненої інформації, провести огляд сучасних епідеміологічним моделей, дослідити питання топологічної уразливості ІТКМ, сформувати основні принципи протидії та прогнозування ЗРЗІ.
5. Перелік обов’язкового графічного матеріалу: результати моделювання з параметрами, результати експерименту.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Завдання	Термін виконання	Підпис керівника
1.	Аналіз літератури та джерел за темоюдипломної роботи.	14.10.19р.– 20.10.19	
2.	Розроблення та затвердження плану дипломної роботи.	21.10.19– 22.10.19	
3.	Проведенняконсультації з науковимкерівникомщодостворенняпершогорозділу.	23.10.19 – 27.10.19	
4.	Розробкарозділу 1: Безпека в інформаційно-телекомукаційних мережах.	30.10.19 – 22.11.19	
5.	Розробкарозділу 2: Дослідження моделей загроз розповсюдження шкідливої інформації в ІТКМ.	23.11.19 – 08.12.19	
6.	Розробкарозділу 3: Моделювання загрози розповсюдження шкідливої інформації в ІТКМ.	09.12.19 – 22.12.19	
7.	Висновки та оформленняпояснювальної записки дипломної роботи.	25.12.19 – 29.12.19	
8.	Підписання необхіднихдокументів у встановленомупорядку.	15.01.20-19.01.20	
9.	Підготовкадо захисту та попередній захист дипломноїроботи на випусковій кафедрі.	22.01.20 – 31.01.20	

7. Дата видачі завдання: 14.10.2019р.

Керівник дипломної роботи _____ Зіатдінов Ю.К.

(підпис керівника) (П.І.Б.)

Завдання прийняв довиконання _____ Ігнатенко В.А.

(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Захист інформаційно-телекомунікаційних мереж від шкідливої інформації» викладена на 113 с., 5 таблиць, 17 рис., 31 літературних джерела, 4 додатки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ФУНКЦІЇ ЗАХИСТУ, ЕПІДЕМІОЛОГІЧНІ МОДЕЛІ, ШКІДЛИВА ІНФОРМАЦІЯ, ІНТЕРНЕТ, ТОПОЛОГІЯ МЕРЕЖІ, МОДЕЛЬ ЗАХИСТУ, СИСТЕМА ПРОТИДІЇ, ПРОГНОЗУВАННЯ,

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

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

Мета роботи:є аналіз та дослідження моделі загрози розповсюдження забороненої інформації в ІТКМ.

Отримані результати:

- проведено інформаційний огляд сучасних моделей розповсюдження шкідливої інформації в мережах;
- досліджено множину функцій захисту від забороненої інформації;
- проведено огляд сучасних епідеміологічним моделей;
- проведено експериментальне дослідження обраного варіанту моделі;
- досліджено питання топологічної уразливості ІТКМ;
- сформовано основні принципи протидії та прогнозування ЗРЗІ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІТКМ – інформаційно-телекомунікаційна мережа;

КОМ – корпоративна обчислювальна мережа;

ЕОТ – електронна обчислювальна техніка;

КСЗІ – комплексна система захисту інформації;

ЗРЗІ – загроза розповсюдження забороненої інформації;

МЕ – міжмережевий екран;

СВВ – системи виявлення вірусів;

НСД – несанкціонований доступ;

ШПр – шкідлива програма;

Інтерфейс – функції для керування об’єктом;

ЗММП – засоби маршрутизації мережевих пакетів;

ЗТК – засоби телекомунікацій;

ЗОТ – засоби обчислювальної техніки;

ЗКП – засоби комутації пакетів;

Канал 1 – канал ЛОМ;

Канал 2 – канал Internet;

КСЗ – клієнт сервера застосувань;

РС 1 – локальна робоча станція;

РС 2 – віддалена робоча станція;

СЗ – сервер застосувань;

ССУБД – сервер СУБД;

ФС ЛОМ – файловий сервер ЛОМ;

ТМО – теорія масового обслуговування.

ВСТУП

Актуальність дослідження. Інформаційно-телекомунікаційні мережі (ІТКМ) забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. Внаслідок складності та розповсюдженості проблемою таких систем є їх низький рівень інформаційної безпеки. Для забезпечення захисту інформації в телекомунікаційних мережах, включаючи Інтернет, розроблено безліч методів і засобів. Але ефективного захисту абонентів від загроз поширення забороненої інформації, зокрема в умовах широкого використання індивідуально-орієнтованих сервісів і пов'язаних з ними протоколів і технологій, не існує.

Серед множини функцій захисту принципової відносно даних систем є функція попередження прояви забороненої інформації. Вона реалізується за рахунок механізмів прогнозування загрози розповсюдження і розсилки повідомлень з попередженнями про наслідки дій із забороненим контентом. Використання інших функцій (попередження, виявлення, локалізації та ліквідації загрози) припускає наявність повного контролю над системою, що в справжніх умовах неможливо.

Одним з підходів до прогнозування загрози розповсюдження забороненої інформації (ЗРЗІ) 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 рамках цих математичних моделей описується переважно гомогенним графом, що при моделюванні великомасштабних мереж (більше 10 млн. вузлів) може дати похибку прогнозування ЗРЗІ більше 30%. Крім того, дані підходи носять в основному теоретичний характер, практика їх використання не виходить за рамки експериментів. Таким чином, дослідження, спрямовані на створення моделей та алгоритмів ЗРЗІ, є актуальними і мають теоретичне і

практичне значення у вирішенні проблеми забезпечення інформаційної безпеки в системах і мережах телекомунікацій.

Мета роботи. Метою роботи є аналіз та дослідження моделі загрози розповсюдження забороненої інформації в ІТКМ.

Для досягнення мети роботи необхідно вирішити наступні наукові та практичні**завдання**:

1. Провести інформаційний огляд сучасних моделей розповсюдження шкідливої інформації в мережах.

2. Дослідити множину функцій захисту від забороненої інформації.

3. Провести огляд сучасних епідеміологічним моделей.

4. Провести експериментальне дослідження обраного варіанту моделі.

5. Дослідити питання топологічної уразливості ІТКМ.

6. Сформувати основні принципи протидії та прогнозування ЗРЗІ.

Методи дослідження. Під час проведення досліджень використовувалися наступні наукові методи:

- аналіз спеціальної літератури, нормативно-правової бази, загальноприйнятих стандартів в галузі захисту інформації;
- системний аналіз;
- метод аналогій;
- моделювання;
- порівняльний аналіз;
- узагальнення та ін.;
- елементів теорії ймовірностей та математичної статистики.

Наукова новизна одержаних результатів. Наукова новизна полягає у дослідженні епідеміологічної моделі для опису процесу розповсюдження шкідливої інформації в мережах.

Практичне значення одержаних результатів. Практичні результати роботи, що були отримані дозволили значно підвищити ефективність захисту від загроз розповсюдження забороненої інформації.

РОЗДІЛ 1. БЕЗПЕКА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

На сьогодні має місце величезне збільшення кількості користувачів Інтернету на теренах України (рис. 1.1). Згідно дослідження, яке проводилось в жовтні 2010 року, кількість активних Інтернет-користувачів країни досягла 12.9 мільйонів. Це означає, що майже 33% всього населення нашої держави користується Інтернетом кожного дня. На ці показники не вплинули економічні складові. При цьому експерти прогнозують подальший ріст активних користувачів [1].

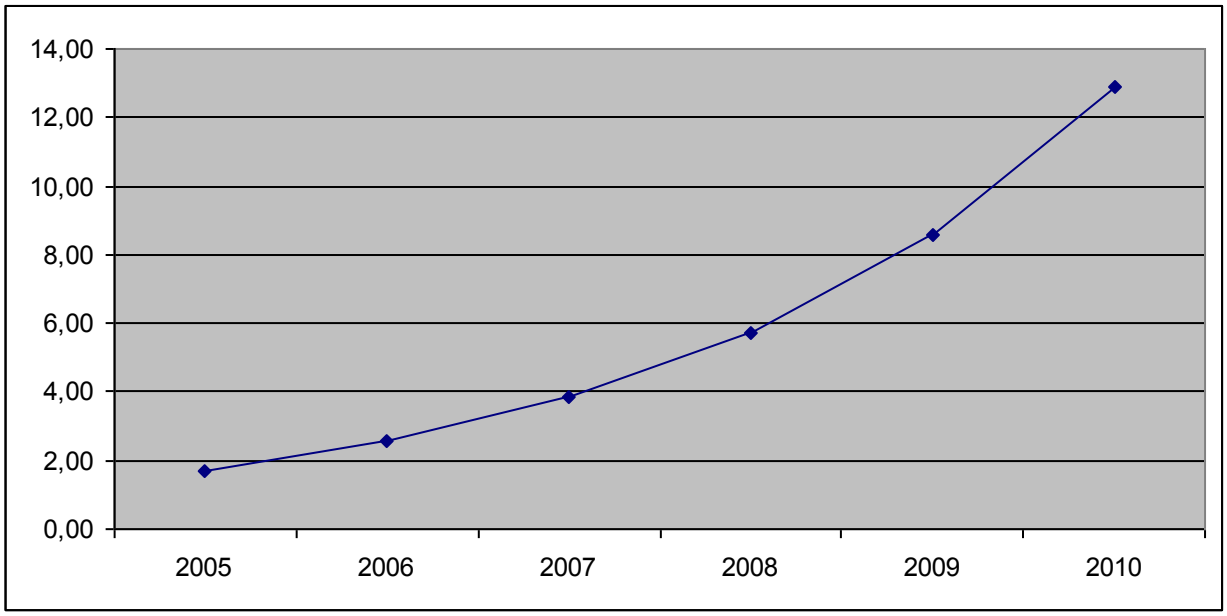


Рис. 1.1. Зростання кількості користувачів Інтернет

З кожним кроком людство наближається до інформаційної епохи. Вже сьогодні інформаційна економіка складає 40-60% у розвинених економічних країнах. До кінця століття планується зростання інформаційної економіки на 10-15%.

Визнаючи безсумнівність досягнень США та інших країн в області інформатизації, необхідно розуміти, що певна частка «інформаційності» цих країн створена за рахунок винесення низки матеріальних, нерідко екологічно шкідливих, виробництв в інші країни світу, за рахунок так званого «екологічного колоніалізму».

Враховуючи тенденції розвитку інвестицій в українські інформаційні підприємства можемо зробити висновок про доцільність подальшого розвитку вітчизняних інформаційних технологій. Найбільш розвинутою сферою інформаційних технологій слід вважати мережеві технології. Саме завдяки ним у світі здійснюється основна частина комунікаційної взаємодії.

1.1. Об’єкт дослідження

ІТКМ забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. ІТКМ надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярним з них є соціальні мережі.

У світі існує величезна кількість різних соціальних мереж, але практично в кожній країні або регіоні існують декілька найбільш популярних представників. У США це «Facebook», «MySpace», «Twitter» та «LinkedIn»; «Nexopia» – в Канаді, «Bebo» – у Великобританії, «Facebook», «dol2day» – у Німеччині. В Україні на сьогоднішній день найпопулярніший є «ВКонтакте».

На рис. 1.2 зображена динаміка зростання користувачів самої великомасштабної соціальної мережі «ВКонтакте» [2].

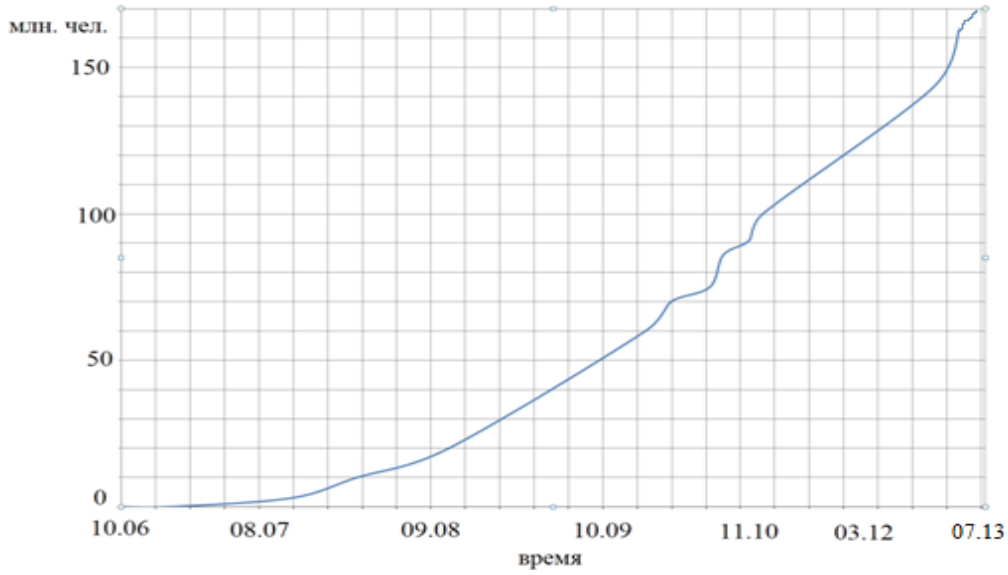


Рис. 1.2. Динаміка росту користувачів соціальної мережі «ВКонтакте»

З бурним ростом числа користувачів ІТКМ виникають і проблеми безпеки в них.

Для аналізу питань безпеки в ІТКМ слід провести аналіз щодо складу її основних елементів та їх функціонування.

У найбільш загальному випадку до складу типової ІТКМ входять наступні 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, що використовують мобільні пристрої (смартфони, планшети і т.д.), Для доступу до мережі також використовують програмне забезпечення (спеціальний додаток) і МЗ;

- сервери (С). У КОМ знаходяться інформаційні сервери різного функціонального призначення, які беруть участь у інформаційній взаємодії (наприклад, проксі-сервера).

КОМ включає в себе, крім абонентів і серверів, також засоби маршрутизації, комутації і адміністрування (МКА), систему безпеки (СБ), яка включає механізми захисту для всієї корпоративної мережі:

- засоби телекомунікації, що забезпечують взаємодію між собою абонентів;
- керуючий елемент, що технічно являє собою сукупність комутуючого та серверного обладнання і реалізує основні функції системи. Включає сервери, що містять у загальному випадку: балансувальник навантаження (БТ), елемент бізнес-логіки (БЛ), бази даних (БД), інфраструктурні системи (ІС) (системи статистики, конфігурації, моніторингу і т.д.).

Отже, як неважко побачити, структура ІТКМ складається із декількох підструктур (шарів), серед яких виділимо: презентаційний шар, шар бізнес-сервісів, персистентний шар, шар загальних інфраструктурних систем.

Опишемо цю багатошарову архітектуру більш детально.

1. Презентаційний шар.

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

2. Шар бізнес-сервісів.

Даний шар призначений для підбору і обробки даних.

3. Персистентний шар.

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

4. Шар загальних інфраструктурних систем.

На цьому шарі розміщуються системи протоколювання статистики, конфігурації додатків, моніторингу.

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

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

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

Крім того, для побудови моделі захисту інформації може розглядатися найбільш поширений і популярний варіант обчислювальної системи. Зокрема, це буде обчислювальна система, яка має наступну архітектуру (рис. 1.3) і включає такі об’єкти:

- канал передачі даних внутрішній (1);
- канал передачі даних зовнішній (2);
- файловий сервер;
- сервер СУБД;
- сервер застосувань;
- клієнт сервера застосувань;
- засоби комутації пакетів;
- засоби маршрутизації пакетів мережевих протоколів;
- персональна обчислювальна машина в локальній мережі (PC 1);

- віддалена персональна обчислювальна машина (PC 2).
-

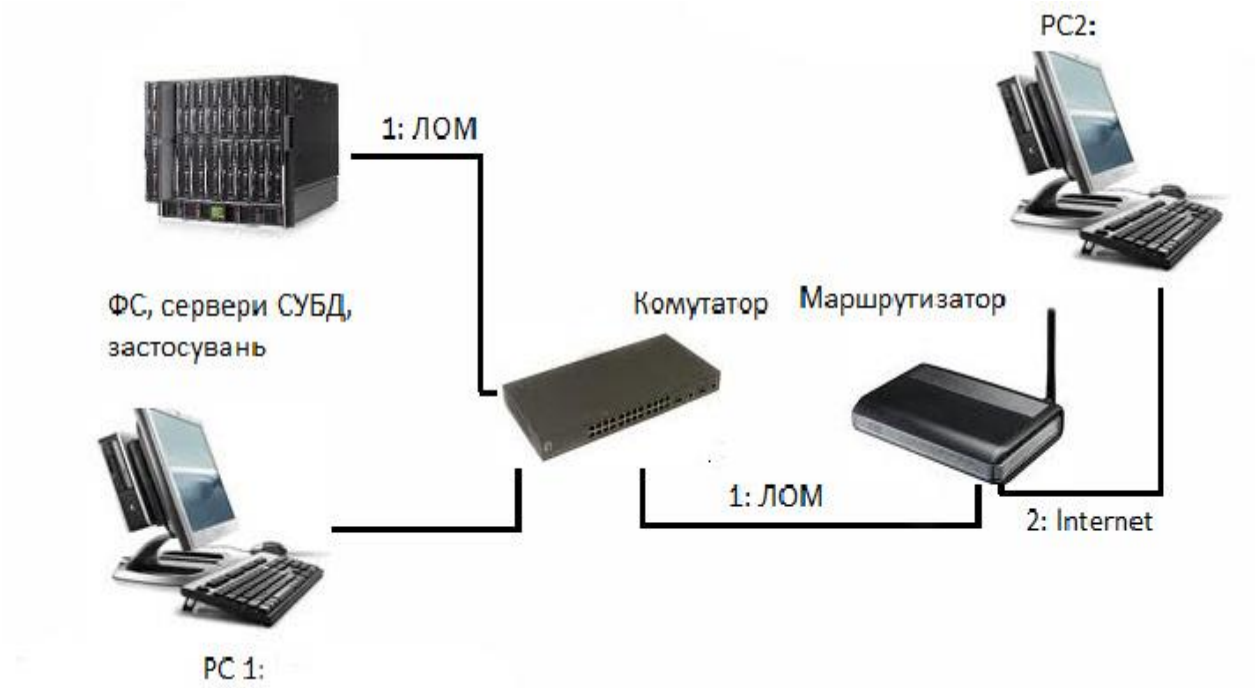


Рис. 1.3. Архітектура обчислювальної системи

Звичайно всі дані про об’єкти знаходяться на сервері. Сам же сервер зазвичай розташовується в будівлі. Таким чином, з точки зору класифікації обчислювальних систем, а також із вище описаних вимог виникає, що тут будемо розглядати ІТКМ класу 3.

1.2. Проблеми інформаційної безпеки в ІТКМ

Як згадувалося, сучасні ІТКМ мають багато проблем з інформаційної безпеки. Наведемо основні з них з визначенням можливих впливів на них, наслідків та можливостей протидії.

1. Використання глобальної мережі Інтернет як розподіленої інформаційно-телекомунікаційної системи.

Використання ІТКМ в такій якості призводить до того, що найбільш уразливими і тому часто атакованими компонентами системи є:

1) Сервери.

2) Робочі станції.

3) Середовище передачі інформації.

4) Вузли комутації.

Наведемо також типові найбільш розповсюджені інформаційні впливи зловмисників на дані компоненти:

1) **Прослуховування мережевого трафіку**. Для прослуховування трафіку (sniffing) мережевий адаптер зазвичай переводиться в «безладний» режим. У даному режимі адаптер перехоплює всі мережеві пакети, що проходять через нього, а не тільки призначені даною адресою, як у нормальному режимі функціонування. В останньому випадку використовуються технології – ARP Spoofing (ARP-poisoning), MAC Flooding і MAC Duplicating. Перехоплення здійснюється з використанням мережевих моніторів, серед яких найбільш функціональними є SnifferPro від компанії Sniffer Technologies [8], IRIS NetworkTrafficAnalyzer від компанії eEYE [5] і TCP Dump [8].

Наслідки. Сучасні мережні протоколи (TCP/IP, ARP, HTTP, FTP, SMTP, POP3 і т.д.) фактично не мають механізмів захисту (передаються у відкритому вигляді).

Зловмисник, що перехоплює трафік між сервером і будь-яким вузлом мережі, може заволодіти автентифікаційними даними користувача (зокрема, отримати пароль).

Протидія. На сьогодні відомо ряд методів визначення наявності запущеного сніффера в мережі, наприклад, метод пінгу, метод ARP, метод DNS і метод пастки [19].

2) **Сканування вразливостей**. Результатом роботи сканера є інформація про систему, яка включає список мережевого обладнання, комп'ютерів з запущеними на них службами, версіями мережевого ПЗ (а значить і вразливостей, властивих даному ПЗ), облікові записи користувачів. Сканування вразливостей зазвичай є етапом, що передує атаці. Адже саме

результати сканування дозволяють точно підібрати експлойти для здійснення безпосередньо НСД.

Виявлення. Саме 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 сліди сканування можна, вивчаючи журнали реєстрації МЕ. Однак такий підхід не дозволяє своєчасно реагувати на подібні інциденти, тобто може виникати певне запізнення з відповідними наслідками. Тому сучасні МЕ і СВВ мають модулі (plug-in) [3], що дозволяють виявити сканування в режимі реального часу. Деякі сканери вразливостей використовують оригінальні методи, що дозволяють виробляти сканування максимально приховано. Наприклад, в Nmap [4] існують можливості, що дозволяють значно утруднити виявлення сканування для СВВ.

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

3) **Мережеві атаки**. Мережеві атаки можна розділити на:

- атаки, засновані на переповненні буфера (overflowbasedattacks). Вони використовують вразливість системи, яка полягає в некоректній програмній обробці даних. При цьому з'являється можливість виконання шкідливого коду з підвищеними привілеями;
- атаки, спрямовані на відмову в обслуговуванні (DenialOfServiceattacks). Атаки не обов'язково використовують уразливості ПЗ системи, яка атакується. Порушення працездатності системи може відбуватися через те, що дані, які надсилаються до неї призводять до значних витрат ресурсів системи. Найпростішим прикладом атаки цього типу є атака «PingOfDeath», сутність якої полягає в наступному: на машину жертви надсилається сильно фрагментований ICMP-пакет великого розміру.

Зазвичай реакцією ОС Windows на отримання такого пакету є повне зависання системи.

4) **Атаки, засновані на використанні вразливостей в ПЗ мережевих застосувань** – експлойти (exploit) [14]. Даний клас атак заснований на експлуатації різних дефектів в ПЗ. Звичайно, експлойти являють собою шкідливі програми, що реалізують відому уразливість в ОС або прикладному ПЗ для отримання НСД до уразливого хосту або порушення його працездатності. Для експлойтів характерна наявність функцій придушення антивірусних програм і МЕ. Наслідки застосування експлойтів можуть бути самими критичними. У разі отримання зловмисником віддаленого доступу до системи, він має практично повний (системний) доступ до комп'ютера. Наступні дії і збиток від них можуть бути наступними: впровадження троянської програми, впровадження набору утиліт для приховування факту компрометації системи, несанкціоноване копіювання зловмисником даних з жорстких і знімних носіїв інформації системи, наведення на віддаленому комп'ютері нових облікових записів з будь-якими правами в системі для подальшого доступу як віддалено, так і локально, крадіжка файлу з хешамі паролів користувачів, знищення або модифікація інформації, здійснення дій від імені користувача системи і т.д.

Протидія. МЕ і СВВ, що встановлені на системі, яка піддається атаці, у ряді випадків не в змозі відобразити дію експлойтів. Для успішного відбиття атак експлойтів засоби захисту необхідно регулярно оновлювати, оскільки механізм виявлення вторгнень в основному заснований на розпізнаванні сигнатур вже відомих атак. Хоча існують розробки, здатні по завіреннях розробників відображати невідомі атаки, практика показує, що вони все ще не ефективні.

5) **Шкідливі програми** (ШПр). ШПр – це комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в мережі, або для прихованого нецільового використання ресурсів, або іншого впливу, що перешкоджає нормальному функціонуванню

мережі. До ШПр відносяться комп'ютерні віруси, троянські коні, мережеві хробаки та ін.

Протидія. Типовим методом протидії є використання 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, зокрема, сексуального, екстремізм і розпалювання расової ненависті.

В українському законодавстві існує поняття забороненої до поширення інформації. Визначається така інформація постановою уряду, яка фіксує єдиний реєстр доменних імен, покажчиків сторінок сайтів в мережі «Інтернет» і мережевих адрес, що дозволяють ідентифікувати сайти в мережі «Інтернет», містять інформацію, поширення якої в Україні заборонено.

Проблеми, що пов’язані із захистом від забороненої до поширення інформації, повинні ураховуватися при розробці концепції забезпечення комплексного захисту ІТКМ.

1.2.1. Канали поширення шкідливих програм

Важливо, щоб система захисту від вірусів і інших шкідливих об'єктів блокувала всі шляхи поширення небезпечного коду.

Перші комп'ютерні віруси поширювалися головним чином через файли і дискети. Потім, після появи пакета Microsoft Office та інших офісних додатків з макрокомандами віруси стали поширюватися через файли офісних документів, які строго кажучи, не є програмами.

Сьогодні найбільш небезпечними каналами поширення вірусів і інших шкідливих програм є Інтернет та електронна пошта. Саме по цих каналах поширюється переважна більшість сучасних шкідливих програм.

Слід зазначити, що комп'ютерні віруси поширюються в першу чергу завдяки недбалості користувачів і адміністраторів комп'ютерних систем. При використанні сучасних захисних засобів і дотриманні навіть елементарних технологій захисту можна різко знизити ризик ураження комп'ютерних систем вірусами і шкідливими програмами інших типів.

Для поширення шкідливих програм використовують такі об'єкти і канали:

- файли виконуваних програм;
- файли офісних документів;
- файли інтерпретованих програм;
- завантажувальні сектори дисків і дискет;
- повідомлення електронної пошти;
- пірінгові (файлообмінні) мережі;
- інтрамережа або Інтернет;
- драйвери ОС.

Не виключено, що з часом у міру вдосконалення інформаційних технологій і розробки нового комп'ютерного обладнання цей список буде розширено.

Файли програм складаються з двійкових команд, призначених для безпосереднього виконання центральним процесором. Змінюючи цей файл, можна змінювати дії, що виконуються програмою.

Файлові комп'ютерні віруси вставляють свій шкідливий код в тіло програмних файлів таким чином, що при запуску програми управління нею передається вірусу. Потім вірус виконує свої шкідливі дії і повертає керування програмі-жертві.

Як правило, програма, заражена комп'ютерним вірусом, зовні поводиться як завжди, тому користувач не підозрює, що на його комп'ютері «живе» вірус.

Деякі віруси впроваджуються в тіло програмного файлу таким чином, що розмір файлу-жертви залишається незмінним, що служить додатковим засобом маскування.

Програмні файли служать одним із широко використовуваних каналів поширення комп'ютерних вірусів і інших шкідливих об'єктів.

Документи, що створюються пакетом Microsoft Office і аналогічними за призначенням пакетами, створеними іншими компаніями, будемо називати офісними документами.

Офісні документи можуть містити не тільки текст і графіку, а й програмний код у вигляді макрокоманд.

Комп'ютерні віруси вміють модифікувати існуючі макрокоманди, розташовані всередині документів, а також додавати в документи нові макроси.

Таким чином, комп'ютерні віруси можуть впроваджуватися в документи типів *.doc, *.xls, а також інші офісні документи, створювані пакетом Microsoft Office і містять макроси. Віруси, здатні на це, називаються макрокоманднимі.

Існує потенційна можливість поширення комп'ютерних вірусів і з файлами графічних зображень, якщо ці файли містять програмний код.

Поширення макрокомандних вірусів відбувається в процесі обміну зараженими офісними документами. При цьому файли документів можуть передаватися з використанням дискет, компакт-дисків, флеш-дисків або будь-яких інших аналогічних пристроїв зовнішньої пам'яті, через інтрамережу або Інтернет.

Зараження макрокомандним вірусом може відбутися після того, як користувач відкриє офісний документ, що містить макрокомандний вірус, для перегляду у відповідному офісному додатку.

Що ж стосується інтерпретованих програм, то вони являють собою текстові файли (або фрагменти тексту, вбудовані в офісні документи), які

виконуються, а точніше кажучи, інтерпретуються за допомогою спеціальної програми. Така програма називається інтерпретатором.

Інтерпретовані програми складаються на таких мовах програмування, як Basic, Java, JavaScript, VB Script, VisualBasicforApplication і ін. Крім того, пакетні файли, що містять команди ОС, також можна розглядати як програми, що інтерпретуються.

Якщо програма, що інтерпретується, записана у файлі, то цей файл може стати об'єктом атаки комп'ютерного вірусу або шкідливої програми іншого типу.

Вірус може записати свій код всередину такого файлу, в результаті чого він отримає управління при запуску програми, що інтерпретується.

Комп'ютерний вірус може поширюватися через файли інтерпретованих програм, в тому числі через командні файли ОС.

У завантажувальному секторі теж є програма завантаження, яка виконується на другому етапі. Ця програма призначена для завантаження ОС.

Програма завантаження з першого сектора диска або дискети завантажує і запускає завантажувач ОС, який включається в роботу на третьому етапі.

Модифікуючи вміст перших секторів дискет і дисків, завантажувальні і комбіновані файлово-завантажувальні віруси можуть перехопити управління на другому або третьому етапі завантаження ОС. Якщо це станеться, вірус отримає управління до моменту завантаження ОС і зможе контролювати як процес завантаження, так і операції, що виконуються системними модулями ОС.

Як відбувається поширення завантажувального вірусу?

Перш за все, цей вірус поширюється разом з дискетами.

Завантажувальні і файлово-завантажувальні віруси поширюються разом з дискетами, коли користувач намагається завантажити комп'ютер із зараженої дискети.

Якщо до користувача потрапила дискета, заражена завантажувальним вірусом, він може випадково або навмисно завантажити з неї ОС (наприклад, за допомогою комбінації клавіш Control + Alt + Delete, за допомогою кнопки скидання, або будь-яким іншим способом).

Це часто відбувається, якщо користувач забуває вийняти дискету з комп'ютера після завершення роботи. Включивши комп'ютер на другий день, він може, не бажаючи цього, виконати спробу завантаження з забутої дискети.

Канали електронної пошти також з успіхом можуть бути використані для поширення вірусів. Через ці канали поширюються звичайні віруси, черв'яки, троянські програми, програмиBackdoor, а також поштові віруси, створені спеціально для поширення через системи електронної пошти.

Сьогодні електронна пошта є основним каналом поширення шкідливих програм самих різних типів. Через ці канали не поширюється хіба лише завантажувальні віруси (але комбіновані файлово-завантажувальні поширюються).

Електронна пошта служить каналом поширення шкідливих програм практично будь-яких типів.

Шкідливі об'єкти можуть впроваджуватися в поштові повідомлення наступними способами:

- у вигляді приєднаних файлів (файлів вкладень);
- у вигляді посилань на шкідливі об'єкти ActiveX або аплетиJava, розташовані на троянських Web-сайтах або на Web-сайтах зловмисників;
- у вигляді конструкцій, що вбудовуються безпосередньо в тіло повідомлення електронної пошти, що має формат HTML.

Якщо вірус потрапив на комп'ютер користувача у вигляді приєднаного файлу, то для його активізації користувач повинен витягти і запустити такий файл на виконання.

Багато користувачів запускають приєднані файли, не замислюючись про наслідки. Якщо в якості приєднаного файлу виступає заражений

програмний (виконуваний або інтерпретований) файл, троянська програма або шкідлива програма іншого типу, такі дії зазвичай призводять до інфікування комп'ютера.

Відправники поштових вірусів часто маскують істинне призначення приєднаних файлів, вибираючи для них таке ім'я, яке потенційно може викликати у користувача інтерес. Такі поштові повідомлення називаються троянськими поштовими повідомленнями.

Існують віруси або інші шкідливі програми, спеціально призначені для мереж обміну файлами (званими також файлообмінними і пірінговими мережами) між комп'ютерами користувачів Інтернету, такими як Kazaa, Windows Messenger, ICQ і т.д.

Ці віруси створюють ситуацію, при якій користувач мережі копіює з зараженого вузла файл шкідливої програми. При цьому система пошуку файлів модифікується таким чином, щоб замість потрібних йому файлів користувач знаходив і завантажував файли з вірусом.

Шкідливі програми можуть поширюватися через Інтернет або інтрамережу компанії.

Такі програми можуть проникати на інфіковані вузли, долаючи захист від несанкціонованого доступу, а також використовуючи відкриті порти системи і ресурси, виділені на комп'ютері в спільне користування.

Шкідлива програма може підібрати пароль для отримання несанкціонованого доступу до вузла мережі, якщо адміністратор не блокував можливість підбору пароля системними засобами.

Шкідлива програма може підібрати пароль доступу до вузла мережі або перехопити пароль, який передається по мережі. Якщо пароль зашифрований, то на його розшифровку, можливо, доведеться витратити певний час.

Навіть якщо шкідливій програмі не відомий пароль доступу до ресурсів вузла мережі, вона може отримати до них доступ, якщо буде використовувати відомі помилки в прикладному і системному забезпеченні.

Одна з найбільш відомих помилок такого роду – помилка переповнення буфера в прикладній або системній програми.

Шкідлива програма може отримати доступ до ресурсів мережі, якщо на одному з вузлів мережі працює черв'як або троянська програма.

Шкідливі програми можуть поширюватися і через драйвери ОС, хоча цей канал поширення вірусів використовується досить рідко.

Вірус може потрапити в програмний файл драйвера операційної системи (наприклад, в драйвер диска) і виконувати системні операції під своїм контролем.

Слід зауважити, що в середовищі ОС Microsoft Windows NT/2000/XP/2003 для такого впровадження програмний код шкідливої програми повинен працювати з привілеями адміністратора.

Шкідлива програма може також функціонувати і як сервіс ОС Microsoft Windows NT/2000/XP/2003.

Вірус або інша шкідлива програма може потрапити в драйвер операційної системи LinuxFreeBSD та інших Unix-подібних операційних систем, якщо програмний код вірусу працює з привілеями адміністратора (користувача root).

Створюючи систему захисту від вірусів та шкідливих програм системний адміністратор повинен чітко уявляти собі, звідкіля може виникнути загроза безпеки.

1.2.2. Функції захисту

Для забезпечення захисту систем, зокрема ІТКМ, створюється КСЗІ. Розробка КСЗІ має починатись з аналізу об'єкта захисту і можливих загроз. Передусім мають бути визначені ресурси ІТКМ, що підлягають захисту. На підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту для всіх ресурсів, що підлягають захисту, мають бути оцінені ризики. На підставі виконаної роботи мають бути вироблені заходи захисту, перетворення яких в життя дозволило б знизити рівень

остаточного ризику до прийнятного рівня. Підсумком даного етапу робіт повинна стати сформульована або скоригована політика безпеки.

Далі розробляється план захисту, який включає в себе опис послідовності і змісту всіх стадій і етапів життєвого циклу КСЗІ, що мають відповідати стадіям і етапам життєвого циклу ІТКМ.

Існують і інші підходи щодо аналізу та забезпечення захисту інформації на об’єктах інформатизації. Аналогічно з концепцією забезпечення комплексного захисту об'єкта інформатизації можна сформувати повну множину функцій захисту від забороненої інформації.

Процес функціонування СЗІ ІТКМ можна моделювати шляхом визначення в ній ряду властивостей, завдяки яким вона певним чином реагує на події, які пов'язані із забезпеченням безпеки інформації в ІТС. Це, наприклад, такі події, як оцінювання реальної можливості (або заходи) прояву порушень безпеки інформації, виявлення фактів їх прояву, вживання заходів до запобігання їх дії на інформацію, що захищається, виявлення, локалізація і ліквідація наслідків дій на інформацію, що захищається, і ін. Кожному з них ставиться у відповідність певна властивість СЗІ ІТКМ, яку називаємо функцією захисту (ФЗ) інформації, і яка полягає в конкретних діях СЗІ відносно певної події. Методи реалізації цих функцій (організаційні, програмні, апаратні і ін.) для даного розгляду не мають значення і в подальшому не розглядаються.

Під **функцією захисту** розуміється сукупність однорідних у функціональному відношенні заходів, регулярно здійснюваних в автоматизованих системах різними засобами і методами з метою створення, підтримки і забезпечення умов, об'єктивно необхідних для надійного захисту інформації.

В рамках такого підходу основне завдання теорії і практики захисту інформації в будь-якій ІТКМ можна розуміти як формування і обґрунтування повної множини функцій захисту S [4], яка повинна характеризуватися очевидною властивістю: множина S повинна містити такі функції, щоби при

їх реалізації СЗІ ІТКМ могла протидіяти всім потенційно можливим порушенням безпеки інформації в процесі функціонування ІТКМ, а також при організації і забезпеченні захисту інформації.

У [4] встановлено, що множина S є об'єднанням з двох множин $S = S_a \bigcup S_c$: 1) множини функцій забезпечення захисту S_a, здійсненням яких створюються умови, які необхідні для надійного захисту інформації; 2) множини функцій S_c управління механізмами захисту, здійснюваних з метою ефективного використання механізмів захисту після реалізації функцій множини S_a. Надалі розглядатиметься тільки множина S_a.

Зокрема, в [4] розглянута одна з можливих схем формування множини функцій S_a. Нижче розглядаються питання обґрунтування, удосконалення і подальшої формалізації схеми подібного роду.

Спочатку розглянемо структуру множини S_a. Порушення інформаційної безпеки безпосередньо пов'язані з загрозами інформації. По суті порушення – це реалізація загроз інформації. Нагадаємо, що загрози інформації визначаються за результатом дії на основні властивості інформації, які визначають її цінність, тобто конфіденційність, цілісність, доступність і спостереженість. Таким чином, вводяться і розрізняються наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності (логічної або фізичної);
- порушення доступності або відмова в обслуговуванні;
- порушення спостереженості або керованості.

До цих загроз інформації необхідно додати ще загрозу несанкціонованого використання інформаційних ресурсів.

Проте визначені таким чином загрози є лише деякі абстрактні і досить загальні небажані дії на інформацію. Внаслідок цього зручним виявляється поняття дестабілізуючого фактора (ДФ), як конкретної причини виникнення

загрози інформації. ДФ – це такі явища або події, які можуть з'являтися на будь-якому етапі життєвого циклу (ЖЦ) ІТКМ і наслідком яких можуть бути загрози інформації і/або нанесення збитку компонентам ІТКМ. Таким чином, порушення інформаційної безпеки – це фактично виникнення і реалізація ДФ.

Тоді основним завданням функцій захисту інформації буде контроль над всіма можливими проявами ДФ. У будь-якій ІТКМ завжди можна визначити такі умови, при яких можуть (хоча б у принципі) виявитися які-небудь ДФ. Якщо їх не буде, то не буде необхідності в захисті, якщо ж потенційні можливості прояву ДФ все-таки матимуть місце, то треба уміти оцінювати реальну можливість (міру) їх прояву, виявляти факти їх прояву, приймати заходи щодо запобігання їх дії на інформацію, виявленню, локалізації і ліквідації наслідків дій на інформацію. Саме ці властивості повинні мати функції забезпечення захисту S_a.

З урахуванням аналізу і класифікації ДФ, проведеної раніше, а також основних завдань функцій захисту, їх множина S_a виглядатиме таким чином:

1. S_{a1} – створення і контроль умов, що обмежують можливості прояву ДФ. Можливість створення таких умов може бути реалізована ще на етапах проектування ІТС, за допомогою вибору відповідної архітектури ІТС, відповідних технологічних схем обробки інформації, моделі безпеки, політики безпеки, впровадження механізмів безпеки і т.д., тобто умов, що виключають навіть потенційну можливість прояву ДФ.

2. S_{a2} – попередження виникнення умов (негативних), що сприяють прояву ДФ. Ця функція реалізується подібно до попередньої і обидві вони відіграють випереджальну роль.

3. S_{a3} – попередження безпосереднього прояву ДФ в конкретних умовах функціонування ІТС. Ця функція також відіграє випереджальну роль, але стосовно конкретних умов і для ДФ, які вже потенційно можуть мати місце на різних етапах ЖЦ ІТС.

4. S_{a4} – виявлення ДФ, що проявилися, і контроль над ними. Тут передбачається здійснення таких заходів, в результаті яких ДФ (або реальна загроза їх прояву), що виявилися, будуть виявлені ще до того, як вони реалізують якусь дію на інформацію, яка захищається. Ця функція фактично – стеження за потенційними ДФ.

5. S_{a5} – попередження дій ДФ на інформацію. Її зміст – не допустити небажаної дії ДФ на інформацію навіть в тому випадку, якщо вони реально виявилися (тут це продовження попередньої функції). Проте здійснення попередньої функції може бути як успішним (прояв ДФ виявлено), так і неуспішним (прояв ДФ не буде виявлений), а дія все-таки можлива. Тому завданням цієї функції є – попередження дії на інформацію ДФ, що виявилися.

6. S_{a6} – попередження дії ДФ на інформацію з метою – не допустити небажаної дії ДФ на інформацію навіть в тому випадку, якщо вони реально виявилися (продовження попереднього пункту). Проте тут функція має завдання – попередження дії на інформацію тих ДФ, що проявилися, але не виявлених явно.

7. S_{a7} – виявлення і контроль дії ДФ на інформацію, що захищається. На відміну від функції S_{a3}, тут здійснюється стеження не тільки за потенційно можливими ДФ, але і за інформацією, що захищається.

8. S_{a8} – локалізація дії ДФ на інформацію, тобто недопущення розповсюдження дії на інформацію за межі максимального допустимих встановлених в ІТС розмірів. Тут основне завдання: локалізація дії ДФ, що проявилася і виявлені, на інформацію.

9. S_{a9} – локалізація дії ДФ на інформацію, тобто недопущення розповсюдження дії на інформацію за межі максимального допустимих встановлених в ІТС розмірів. Проте тут виділяється завдання: локалізація дій ДФ на інформацію, що проявився, але не виявлених.

10. S_{a10} – ліквідація наслідків дії ДФ на інформацію, що захищається. Під ліквідацією наслідків розуміється проведення таких заходів щодо локалізованої дії ДФ на інформацію, в результаті яких подальша обробка інформації може здійснюватися без урахування того, що мали місце дії. Тобто потрібно відновити той стан інформації, який мав місце ще до дії ДФ. Ясно, що для ліквідації наслідків дії у разі локалізації виявлених і невиявлених дій необхідні абсолютно різні механізми захисту. Це означає, що тут доцільно виділити завдання: ліквідація наслідків виявленої і локалізованої дії ДФ.

11. S_{a11} – ліквідація наслідків дії ДФ на інформацію, що захищається, але тут виділяється завдання: ліквідація наслідків локалізованої, але не виявленої дії ДФ на інформацію.

Як показує аналіз, для елементів множини S_a можна відзначити наступні характерні особливості:

- множина функцій S_a є вичерпною і повною в тому сенсі, що включає всі у принципі можливі дії щодо забезпечення захисту інформації в ІТКМ;
- жодну з функцій множини S_a не можна виключити з даної множини;
- множина функцій S_a повинна підтримуватися в будь-яких ІТКМ на всіх етапах їх ЖЦ і в будь-яких умовах їх функціонування.

Інакше кажучи, реалізація множини функцій забезпечення захисту інформації S_a в ІТКМ є необхідною умовою надійного захисту інформації. Це означає, що рівень захищеності ІТКМ повністю визначається набором конкретних заходів, необхідних для підтримки всіх функцій S_a. У свою чергу, кожний з таких заходів визначається своїми рівнем і повнотою реалізації.

Тепер розглянемо можливі підсумкові стани СЗІ, до яких може приводити виконання або невиконання кожної з перерахованих функцій. Незалежно від перерахованих можливостей функцій забезпечення захисту S_a для будь-якої СЗІ в будь-якій ІТКМ може виникати тільки наступна множина різних підсумкових станів (подій) A:

1. A_1 – СЗІ повністю виконує свої завдання, тобто навіть за умови прояву яких-небудь ДФ запобігає їх негативну дію на інформацію, що захищається, або повністю ліквідовуються наслідки такої дії.

2. A_2 – СЗІ не повністю виконує свої завдання, тобто не вдається повністю запобігти негативній дії ДФ на інформацію, проте ця дія локалізоване.

3. A_3 – СЗІ не виконує жодної з своїх завдань, тобто СЗІ порушена повністю, внаслідок чого негативна дія ДФ на інформацію не тільки не скасована, але навіть не локалізована.

Очевидно, що організація захисту інформації в ІТКМ полягає в досягненні першої події $A_1 \in A$ і/або хоч би частково – другої $A_2 \in A$.

Для подальшого аналізу перераховані функції захисту з множини S_a і підсумкові події (множина A) зручно представити у вигляді графа, в якому приведені всі можливі їх поєднання. У такому графі номерами функцій захисту відмічені його вершини, дуги описуються булевими змінними і фіксують факти виконання або невиконання функцій захисту, а результати визначаються як кінцеві вершини – деякі булеві функції.

Користуючись графом та відомими правилами, легко одержати явні вирази для булевих функцій:

$$F_1 = x_1,$$

$$F_2 = \bar{x}_1 \wedge x_2,$$

$$F_3 = \bar{x}_1 \wedge \bar{x}_2 \wedge x_3,$$

$$F_4 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 \wedge x_5,$$

$$F_5 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \bar{x}_6) \wedge x_7 \wedge x_8 \wedge x_{10},$$

$$F_6 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \bar{x}_6) \wedge \bar{x}_7 \wedge x_9 \wedge x_{11},$$

$$F_7 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge \bar{x}_4 \wedge x_6,$$

$$F_8 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \bar{x}_6) \wedge x_7 \wedge x_8 \wedge \bar{x}_{10},$$

$$F_9 = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \bar{x}_6) \wedge \bar{x}_7 \wedge x_9 \wedge \bar{x}_{11},$$

$$F_{10} = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \bar{x}_6) \wedge x_7 \wedge \bar{x}_8,$$

$$F_{11} = \bar{x}_1 \wedge \bar{x}_2 \wedge \bar{x}_3 \wedge (x_4 \wedge \bar{x}_5 \vee \bar{x}_4 \wedge \bar{x}_6) \wedge \bar{x}_7 \wedge \bar{x}_9.$$

Таким чином, кожній з функцій захисту $S_{ai} \in S_a$, i=1,...,11 поставлена у відповідність конкретна булева функція. Неважко також переконатися, що кожний з одинадцяти відмічених результатів є випадковою подією, причому ці події в основному незалежні і всі вони складають повну групу несумісних подій. Тому сума їх імовірностей повинна дорівнювати 1

$$\sum_{i=1}^{11} P_i = 1, \qquad (1)$$

де P_i – імовірність i-горезультату.

Насправді перераховані події не є повною мірою незалежними, проте в більшості випадків в першому наближенні припущення їх незалежності є цілком задовільним. Детальніший облік цієї обставини вимагає додаткового дослідження.

З 11 можливих результатів лише результати 1-7 приводять підсумковій події $A_1 \in A$; результати 8 і 9 – до підсумкової події $A_2 \in A$; результати 10 і 11 – до підсумкової події $A_3 \in A$. З точки зору захисту

інформаціїсприятливими якраз є результати 1-7 (і частково 8-9), тому сума їх ймовірностей буде не чим іншим як ймовірністю того, що захищеність інформації буде повністю (або частково, якщо враховувати результати 8-9) забезпечена. Отже, для випадку повного забезпечення захищеності це буде:

$$P_s = \sum_{i=1}^{7} P_i \ . \qquad (2)$$

Ймовірності сприятливих результатів можна виразити через імовірності успішної реалізації окремих функцій захисту, визначення яких є значно простішим завданням. Це можна зробити, застосовуючи до одержаних раніше булевих функцій логіко-ймовірнісний підхід, оскільки вони задовольняють всім необхідним для цього умовам. Тому, позначаючи ймовірність успішної реалізації функцій захисту $P_{fi}, i = 1,...,11$, для ймовірності сприятливих результатів одержимо наступні формули:

$$P_1 = P_{f1},$$

$$P_2 = (1 - P_{f1})P_{f2},$$

$$P_3 = (1 - P_{f1})(1 - P_{f2})P_{f3}$$

$$P_4 = (1 - P_{f1})(1 - P_{f2})(1 - P_{f3})P_{f4}P_{f5},$$

$$P_5 = (1 - P_{f1})(1 - P_{f2})(1 - P_{f3})(P_{f4}(1 - P_{f5}) + (1 - P_{f4})(1 - P_{f6}))P_{f7}P_{f8}P_{f10}$$

,

$$P_6 = (1 - P_{f1})(1 - P_{f2})(1 - P_{f3})(P_{f4}(1 - P_{f5}) + (1 - P_{f4})(1 - P_{f6}))(1 - P_{f7})P_{f9}P_{f11},$$

$$P_7 = (1 - P_{f1})(1 - P_{f2})(1 - P_{f3})(1 - P_{f4})P_{f6}.$$

Для випадку часткового забезпечення захищеності інформації слід врахувати результати 8 і 9, тобто отримаємо співвідношення

$$P_s = \sum_{i=1}^{9} P_i \ , \qquad (3)$$

у якому використані дві відповідні формули для імовірності:

$$P_8 = (1-P_{f1})(1-P_{f2})(1-P_{f3})(P_{f4}(1-P_{f5}) + (1-P_{f4})(1-P_{f6}))P_{f7}P_{f8}(1-P_{f10}),$$

$$P_9 = (1-P_{f1})(1-P_{f2})(1-P_{f3})(P_{f4}(1-P_{f5}) + (1-P_{f4})(1-P_{f6}))(1-P_{f7})P_{f9}(1-P_{f11}).$$

У обох випадках для сум ймовірностей підстановкою в них формул для ймовірності виходить загальна символічна залежність

$$P_s = F(P_{f1},...,P_{f11}), \qquad (4)$$

з якої видно, що захищеність інформації в ІТКМ повністю визначається ймовірностями реалізації перерахованих функцій захисту. У свою чергу, ці імовірності визначаються набором конкретних практичних заходів щодо реалізації функцій захисту і/або рівнем їх реалізації.

З цього виникає, що можна ставити задачу забезпечення певного рівня захищеності $\overline{P}_s$ шляхом вибору такої сукупності заходів для здійснення кожної з функцій захисту S_a, при яких

$$F(P_{f1},...,P_{f11}) \geq \overline{P}_s, \qquad (5)$$

тобто досягнути рівня захищеності не нижче заданого.

Більше того, стає можливим сформулювати наступну задачу оптимізації СЗІ. Дійсно, реалізація кожної з функцій захисту S_a завжди пов'язана з певними витратами на них і, природно, рівень реалізації кожної з них залежатиме від величини цих витрат. Тому, якщо кількість витрат (у деяких умовних одиницях) на реалізацію *i*-оїфункції позначити C_i, то, звичайно, $P_{fi} = f_i(C_i)$ і

$$P_s = F(f_1(C_1),..., f_{11}(C_{11})) = G(C_1,...,C_{11}). \qquad (6)$$

Тоді задача оптимізації формулюється таким чином: мінімізувати витрати на захист, забезпечивши її рівень не нижче заданого

$$\begin{cases} \min \sum_{i=1}^{11} \alpha_i C_i, \\ G(C_1,...,C_{11}) \geq \overline{P}_s. \end{cases}$$

Тут α_i – вагові коефіцієнти, за допомогою яких можна урахувати важливість тої чи іншої функції захисту. Їх значення встановлюються, наприклад, шляхом експертних оцінок.

Крім того, тепер легко також сформулювати задачу максимізації рівня захищеності при обмеженні на витрати зверху

$$\begin{cases} \max P_s \\ C_i \geq \overline{C}_i, i = 1,...11. \end{cases}$$

Очевидна практична важливість і цінність таких оптимізаційних задач, проте використання їх на практиці наштовхується на винятково складну проблему визначення функціональних залежностей (3). Ці труднощі виникають унаслідок того, що рівні успішної реалізації окремих функцій захисту множини S_a істотно залежать ряду від інших чинників, які дуже важко формалізуються (уразливості, атаки, загрози, наявність або відсутність засобів захисту, людський чинник і ін.).

Таким чином, описано повну множину функцій захисту інформації і множину можливих підсумкових подій в ІТКМ. За допомогою графа далі встановлено взаємозв'язок функцій захисту і підсумкових подій, що дозволило одержати вирази для імовірностей успішної реалізації окремих функцій захисту. У свою чергу, це дозволило сформулювати деякі важливі задачі оптимізації СЗІ.

1.2.3. Функції захисту від забороненої інформації

У випадку моделювання процесу розповсюдження забороненої інформації в ІТКМ перелік і взаємодія ФЗ суттєво спрощуються. Зокрема, як показує аналіз, для організації захисту від розповсюдження забороненої інформації список вивчених вище функцій захисту суттєво скорочується та модернізується [4]. Точніше, до списку таких функцій захисту повинні входити наступні:

- попередження умов виникнення забороненої інформації;

- попередження безпосередньої її прояви;
- виявлення її;
- попередження впливу її на абонентів;
- виявлення впливу її на абонентів;
- локалізація, обмеження впливу її на абонентів;
- ліквідація наслідків.

Наведений перелік повної множини функцій захисту від забороненої інформації в мережах розглянемо більш детально.

1) **Попередження умов виникнення забороненої інформації.**

Функція реалізується за допомогою нормативно-правових актів. Вона не може повністю виключити загрозу розповсюдження 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 розповсюдження забороненої інформації в соціальній мережі. Більш докладно дана функція буде розглянута нижче.

3) **Виявлення забороненої інформації, яка проявилася.**

Функція пов'язана з моніторингом ІТКМ на предмет забороненої інформації на сторінках абонентів. Як правило, для реалізації даної функції захисту використовується різні СОРМ. 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 автоматичної розсилки повідомлень з попередженням про відповідальність за поширення забороненої інформації, аж до блокування абонента. Блокування може здійснюватися легітимними засобами за наявності доступу до управління системи і нелегітимними – за його відсутності (злом акаунта). Така ФЗ

ділиться на дві функції (ФЗ4а і ФЗ4б). 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 ФЗ3.

6) **Локалізація, обмеження впливу забороненої інформації на абонентів.**

Функція реалізується через блокування абонентів, що поширюють заборонену інформацію (ФЗ6а), або абонентів – потенційних розповсюджувачів (ФЗ6б). 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 рис. 1.4 наведено всі комбінації подій [3], які потенційно можливі при здійсненні всіх ФЗ.

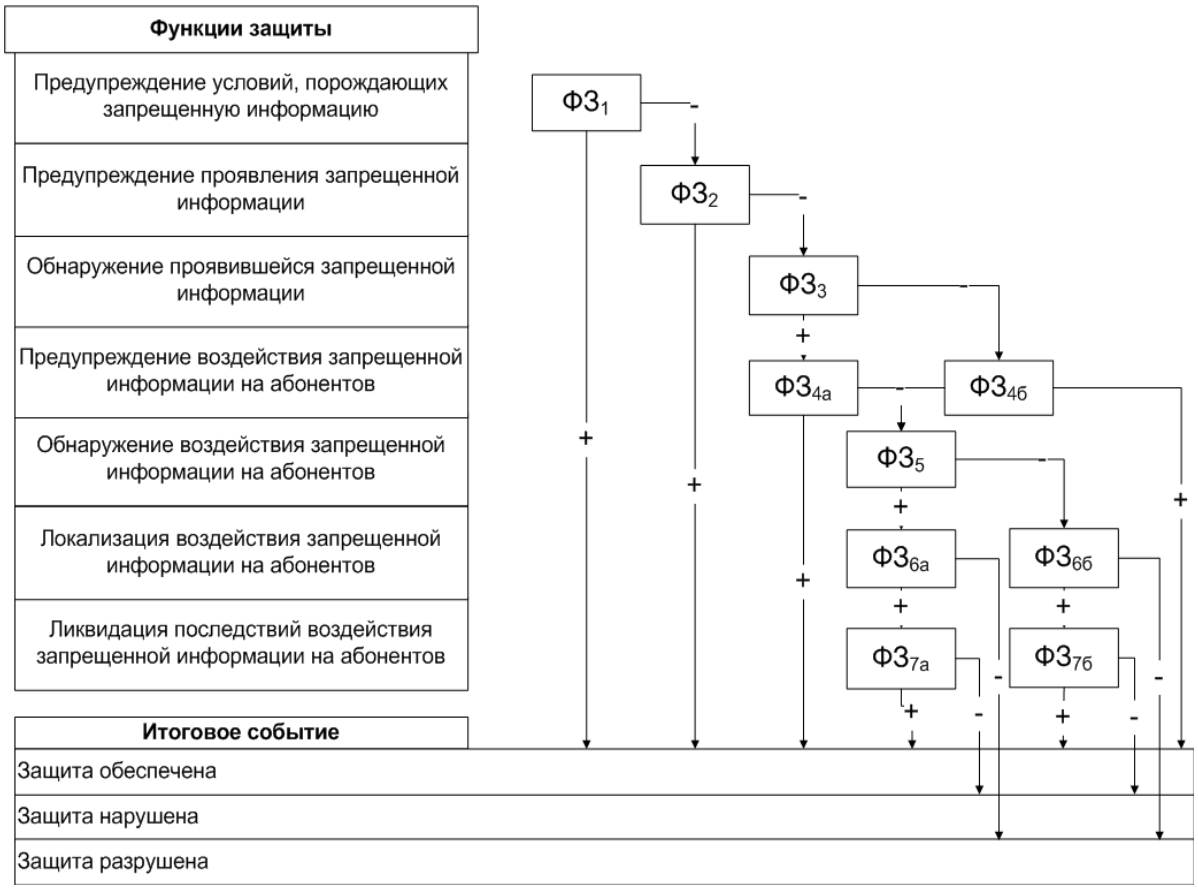


Рис. 1.4. Функції захисту від забороненої інформації в ІТКМ

З аналізу функцій захисту видно, що найбільш ефективні функції – це перші функції, так як вони забезпечують захист на ранніх етапах. Всі функції мають свої недоліки.

Найбільш перспективною ФЗ інженерно-технічного напряму є ФЗ2. Саме їй присвячена дана робота. На даному етапі, маючи інформацію про топологію ІТКМ і потенційних розповсюджувачів забороненої інформації, можливе прогнозування процесу її поширення.

Як показує аналіз відкритих джерел, основними характерними рисами мереж з позиції поширення в них вірусів є:

1) завжди апріорна обмеженість інформації про склад програмного і технічного забезпечення вузлів мереж;

2) фіксована структура мереж, корелює з ієрархічною структурою організаційно-технічної системи і включає від десятків до тисяч вузлів;

3) середньостатистичні часові характеристики функціонування конкретних вірусів в вузлах мереж відповідні вектору цілей і можливостям цих вірусів;

4) середньостатистичні часові характеристики функціонування підсистем захисту інформації мережевих вузлів, отримані з «інсайдерських» та відкритих джерел.

Очевидно, що оцінка захищеності ІТКМ від впливу вірусів із застосуванням натурних методів моделювання в переважній більшості випадків є вкрай дорогою.

Тому створення моделей і алгоритмів поширення загрози забороненої інформації – одне з ключових завдань у даному напрямку. Однак їх розробка вимагає наявності певної інформації, для отримання якої необхідно розв’язати низку проблем, що виникають при дослідженні властивостей розглянутої інформаційно-телекомунікаційної системи. Це, зокрема, такі проблеми:

1. Складнощі при перевірці достовірності даних про вузол системи. Досить часто абоненти ІТКМ вказують недостовірну інформацію про себе, а іншими способами її важко отримати.

2. Закритість системи. Структура і інформація про управління системою є конфіденційною інформацією – знову важко отримати інформацію.

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 (приватність, часовий інтервал і т.д.).

Сформульована в даній роботі мета дослідження вимагає вивчення найбільш цікавого аспекту ІТКМ – обміну повідомленнями між абонентами. Саме тому при її моделюванні найбільш зручним апаратом є апарат теорії графів. Тоді концептуальну математичну модель інформаційної взаємодії можна представити графом, вузлами якого є абоненти, а ребрами – зв'язки

між ними. Такий граф повинен мати низку специфічних особливостей, серед яких слід виділити наступні:

1. Велика розмірність. Сучасні системи можуть містити мільйони елементів.

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

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

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

5. Наявність груп вузлів, що мають велику кількість зв'язків усередині і невелику – між групами. Тобто граф, що представляє таку систему, володіє певною кластеризацией. Для таких систем характерним є те, що два вузли, які мають зв'язки до якого-небудь вузлу, часто також мають зв'язок між собою.

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

1.3. Моделювання ІТКМ

Поняття характеристики функціонування мережі включає вторинні властивості комп'ютерної мережі, які визначаються в процесі вирішення завдань аналізу, як функція параметрів. Параметри комп'ютерної мережі описують первинні властивості мережі і є вихідними даними при вирішенні задач аналізу.

Характеристики комп'ютерних мереж – це сукупність показників ефективності (якості) мережі. Характеристики комп'ютерних мереж можна розділити на якісні та кількісні [2].

Кількісні характеристики комп'ютерних мереж можна розділити на дві групи:

- глобальні, що визначають найбільш важливі властивості мережі як цілісного об'єкта;
- локальні, що визначають властивості окремих пристроїв або частин мережі і дозволяютьо тримати більш детальне уявлення про ефективність мережі.

До глобальних відносяться характеристики продуктивності, оперативності, надійності, вартісні, інші (енергоспоживання, масогабаритніі т.п.).

Продуктивність комп'ютерної мережі – міра потужності мережі, визначальна кількість роботи, виконуваної мережею в одиницю часу. Поняття продуктивності охоплює широку номенклатуру показників ефективності комп'ютерної мережі, що визначають якість функціонування як мережі в цілому, так і окремих її підсистем і елементів – технічних і програмних засобів.

Продуктивність мережі залежить, в першу чергу, від продуктивності окремих її елементів, званої швидкістю роботи або швидкодією пристроїв, наприклад, швидкість передачі даних по каналах зв'язку, вимірювана об'ємом даних, переданих за одиницю часу, швидкодія ЕОМ або, точніше, процесора, що вимірюється числом команд, виконуваних в одиницю часу, і т.п. Для оцінки продуктивності комп'ютерної мережі в цілому використовується наступна сукупність показників:

- продуктивність ЗТК (мережі передачі даних), яка вимірюється числом повідомлень (пакетів, кадрів, біт) переданих по мережі за одиницю часу;
- продуктивність ЗОТ (засобів обробки даних), що представляє собою сумарну продуктивність всіх засобів ОТ (ЕОМ і систем), що входять до складу мережі.

Продуктивність ЗТК (комунікаційна потужність) може бути задана наступними показниками:

- максимальна або гранична продуктивність, звана пропускною здатністю мережі передачі даних і вимірюється кількістю пакетів (кадрів), переданих в мережі за одиницю часу;
- реальна чи фактична продуктивність мережі передачі даних, яка може бути задана як середнє значення на деякому інтервалі часу або як миттєве значення в конкретний момент часу.

Продуктивність ЗОТ (обчислювальна потужність) в цілому складається з продуктивностей ЗОТ, що виконують обробку даних в мережі. Найбільш важливим показником продуктивності ЗОТ, як сукупності технічних і програмних засобів, є системна продуктивність λ_0, вимірювана числом завдань, виконуваних системою за одиницю часу:

Характеристики оперативності описують затримки, що виникають при передачі і обробці даних у мережі.

Для оцінки оперативності мережі в цілому використовуються наступні показники: **час доставки пакетів** (повідомлень), **час відгуку** (відповіді).

Час доставки (час затримки) пакетів характеризує ефективність організації передачі даних в обчислювальній мережі і являє собою інтервал часу, вимірюваний від моменту надходження пакету або повідомлення в мережу до моменту отримання пакету адресатом. У загальному випадку, час затримки – величина випадкова, що обумовлено випадковим характером процесів надходження і передачі даних в мережі.

У комп'ютерних мережах звичайно час доставки задається середнім значенням T, на яке може накласти обмеження $T<T^*$ в залежності від типу переданих даних.

При передачі мультимедійних даних крім середнього значення часу доставки пакетів важливою характеристикою є варіація або джиттер затримки, що представляє собою середньоквадратичне відхилення часу затримки різних пакетів.

Час відгуку (відповіді) – інтервал часу від моменту надходження запиту (повідомлення, транзакції) в мережу до моменту завершення його обслуговування, пов'язаного з виконанням деякої прикладної або обслуговуючою програми, зі зверненням до бази даних і т.п.

Час відповіді являє собою час перебування запиту в мережі і характеризує ефективність як телекомунікаційних, так і обчислювальних засобів комп'ютерної мережі.

Час відгуку, як і час затримки, – величина випадкова і може здаватися середнім значенням U або у вигляді ймовірності $P(t_u<U^*)$ неперевищення деякого заданого значення U^*.

У мережах реального часу замість терміна «час відповіді» часто використовують термін «час реакції».

В якості характеристик надійності зазвичай використовуються наступні показники:

- ймовірність безвідмовної роботи мережі $P(t)$ – імовірність того, що протягом часу t не станеться відмови;
- інтенсивність відмов λ_0 – середнє число відмов за одиницю часу;
- час напрацювання на відмову – проміжок часу між двома суміжними відмовами – величина випадкова, а її середнє значення T_0 називається середнім часом напрацюванням на відмову $T_0 = 1/\lambda_0$;
- час відновлення – інтервал часу від моменту настання відмови до моменту відновлення працездатності системи – величина випадкова і зазвичай задається середнім значенням $T_в$, званим середнім часом відновлення;
- коефіцієнт готовності $K_г$ – частка часу, протягом якого мережа працездатна: $K_г = T_0/(T_0 + T_в)$.

Величина $K_г$ може трактуватися як ймовірність того, що в будь-який момент часу мережа працездатна.

Аналогічно, значення $(1 – K_г)$ визначає ймовірність того, що мережа знаходиться в стані відновлення (непрацездатна).

В якості вартісних (економічних) характеристик комп'ютерної мережі можуть використовуватися такі показники:

- повна вартість володіння (Totalcostofownership, TCO) – витрати, що розраховуються на всіх етапах життєвого циклу мережі і включають вартість технічних, інформаційних і програмних засобів (прямі витрати) та витрати на експлуатацію мережі (непрямі витрати);
- вартість (ціна) передачі даних і обробки даних у мережі, яка обумовлена обсягом і вартістю використовуваних ресурсів мережі відповідно при передачі і обробці даних.

В якості локальних характеристик комп'ютерних мереж можуть використовуватися в залежності від цілей дослідження найрізноманітніші показники ефективності.

Локальні характеристики описують ефективність функціонування:

- вузлів і каналів зв'язку;
- окремих сегментів мережі;
- вузлів обробки даних: обчислювальної системи та її підсистем.

Локальні характеристики можуть бути розбиті на дві групи: часові; безрозмірні.

До часових характеристик відносяться:

- час доставки (затримки) пакетів при передачі між сусідніми вузлами мережі;
- час очікування передачі даних у вузлах мережі або звільнення ресурсів (сервера);
- час перебування даних у різних вузлах, пристроях або підсистемах.

До безрозмірних характеристик відносяться:

- число пакетів, що знаходяться в буферній пам'яті вузлів (маршрутизаторів, комутаторів);
- коефіцієнти завантажень вузлів, каналів зв'язку і пристроїв ЗОТ і т.д.

Коефіцієнт завантаження або просто завантаження ρ пристрою це – частка часу, протягом якого пристрій працює:

$$\rho = \lim_{T \to \infty} \frac{t}{T},$$

де t – час, протягом якого пристрій працював; T – час спостереження.

Завантаження ρ характеризує ступінь використання пристрою і часто називається коефіцієнтом використання пристрою. Оскільки $0 \leq \rho \leq 1$, то завантаження може трактуватися як ймовірність того, що в будь-який момент часу пристрій працює. Величина $\eta = 1 - \rho$ називається коефіцієнтом простою пристрою і характеризує частку часу, протягом якого пристрій не працює (простоює).

1.3.1. Постановка задачі аналізу характеристик ІТКМ

Бурхливе зростання складності комплектуючих комп'ютерних мереж вимагає підвищення ефективності їх застосування та вдосконалення методів управління і планування мереж.

Теорія масового обслуговування (ТМО) забезпечує можливість розрахунку кількісних характеристик функціонування мереж, включаючи оцінку ймовірносно-часових характеристик вузлів комутації, але не дозволяє розрахувати надійність мережі. Спрощений підхід ТМО вимагає подальшого уточнення характеристик мережі за допомогою більш реальних моделей, що призводить до ітераційної процедурі проектування комп'ютерних мереж [3].

В даний час технічні та програмні засоби комп'ютерної мережі та умови їх роботи стають все більш складними. Кількість елементів в окремих видах пристроїв комп'ютерної мережі обчислюється сотнями тисяч. Імовірність виникнення хоча б однієї відмови сучасного складного пристрою стає досить великою, отже, необхідні спеціальні заходи, що забезпечують доступність ресурсів і послуг. Доступність – такий стан комп'ютерної мережі, при якому мережа відповідає всім вимогам, що пред'являються до її функціонування, тобто це властивість зберігати працездатний стан протягом

деякого напрацювання. Для оцінки доступності застосовується кількісний показник: коефіцієнт оперативної готовності R_s.

Методи теорії надійності використовуються для забезпечення заданих вимог до функціонування комп'ютерної мережі та підвищення доступності на етапах проектування, виготовлення, випробування та експлуатації мережі. Методи теорії ймовірностей, як математичного апарату теорії надійності, використовуються для розрахунку показника ймовірності безвідмовної роботи комп'ютерної мережі.

При проектуванні мережі при зміні її структури з метою поліпшення характеристик або поновлення з'являється небезпека зниження готовності, тому необхідно розраховувати коефіцієнт готовності проекту мережі на кожному кроці ітерації проектування.

Використання пропонованої методики аналізу проекту КС призводить до цілеспрямованої зміни структури мережі і обчисленню, в тому числі і надійносних характеристик функціонування.

Характеристики функціонування мережі в цьому випадку пропонується представити як функцію структурно-функціональної організації і коефіцієнта оперативної готовності, не нижче заданого. У загальному випадку це виглядатиме наступним чином

$$H(t) = f(SF, R_s \geq R_z, C), \qquad (7)$$

де SF – структурно-функціональні параметри комп'ютерної мережі;

R_s, R_z – коефіцієнти оперативної готовності;

умова $R_s \geq R_z$ обмежує ймовірність безвідмовної роботи мережі,

C – вкладення (вартість) в комп'ютерну мережу.

Один з основних способів вивчення ІТКМ – моделювання, яке прийнято розглядати у двох аспектах. Перший стосується моделювання топології (структури інформаційних зв'язків між вузлами мережі) ІТКМ, а другий зачіпає проблему вивчення процесів, що проходять в ній. У даному випадку це загроза розповсюдження забороненої інформації (ЗРЗІ).

1.3.2. Моделювання топології ІТКМ

З погляду топології ІТКМ відносять до складних мереж. Складні мережі (комплексні мережі, complexnetworks) – це існуючі в природі мережі, що володіють нетривіальними топологічними властивостями.

Як і в загальній теорії систем в мережевих технологіях також існує проблема класифікації, тобто на сьогодні є різні підходи щодо класифікації ІТКМ. Це цілком зрозуміло, оскільки в природі просто не існує однакових ІТКМ – має місце величезна різноманітність за багатьма чинниками навіть з топологічної точки зору.

Для даного розгляду, як здається, досить прийнятною може бути наступна класифікація топологічних моделей мереж [8] (рис. 1.5). У 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.

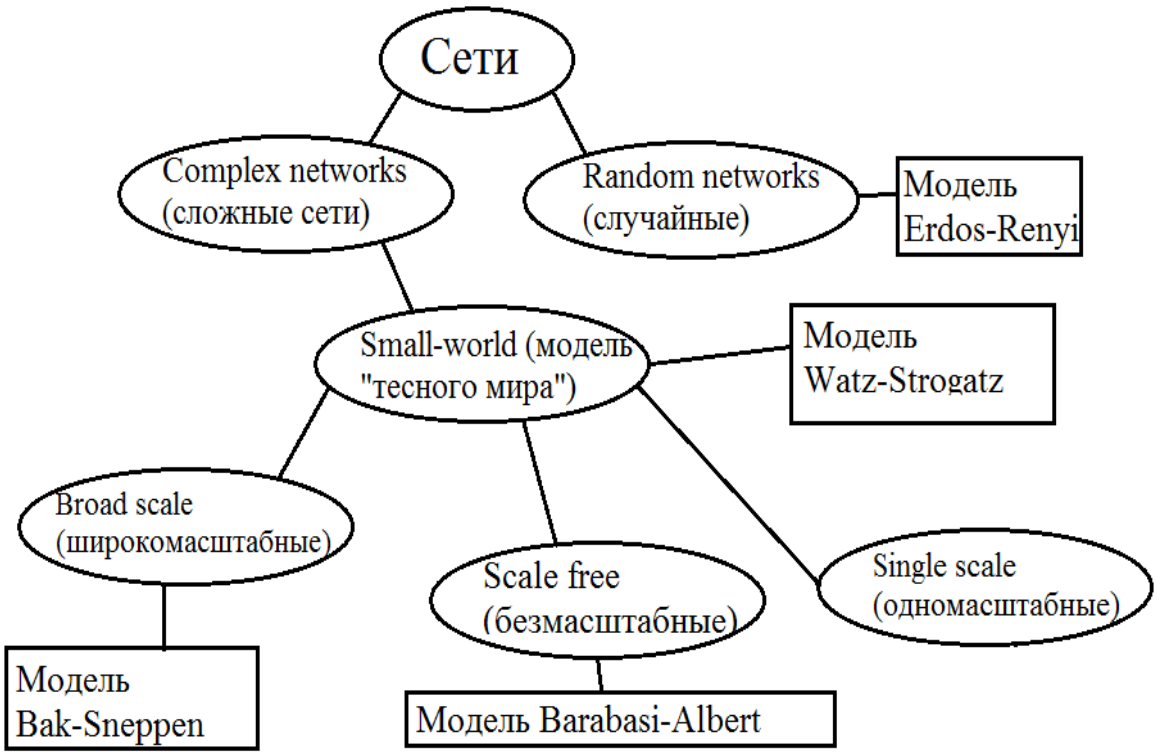


Рис. 1.5. Класифікація мереж

На сьогодні проводиться дослідження топології найбільш популярних ІТКМ і здійснюється пошук найбільш адекватної топологічної моделі. З

даної тематики є багато робіт, в яких розглянуті основні топологічні аспекти ІТКМ. Зокрема, виділено головні сучасні тенденції в галузі аналізу топології ІТКМ:

1. вивчення топологічних характеристик ІТКМ [9];

2. дослідження еволюції ІТКМ [5];

3. вивчення і розробка методів для обчислення характеристик великомасштабних ІТКМ, вирішення проблеми отримання репрезентативної вибірки з ІТКМ [21].

Якщо оглянути окремі аспекти з аналізу топології ІТКМ, то слід відзначити наступні погляди та точки зору на моделі ІТКМ:

- ІТКМ з погляду маркетингових стратегій на їх основі розглянуті в [7,9];
- ІТКМ часто відносять до scale-free (SF) мережам [14,15,20]. Перші роботи належать Barabasi і Albert і присвячені однойменної моделі. Вони порівнюють існуючі моделі і свою модель, докладно її описують і приводять її сильні і слабкі сторони;
- В [23] Dorogovtsev і Mendes узагальнюють Barabasi-Albert модель і знаходять її рішення. Вони знаходять розподіл зв'язності вузлів і деякі інші пов'язані з ним параметри мережі. Також показано, що виникає масштабованість дійсна не тільки для даної моделі, але й для широкого класу зростаючих мереж. Вони призводять отримані універсальні відносини масштабування, що описують властивості розвиваються scale-free мереж і вказують межі їх дії. Дано доказ того, що основні властивості мереж *SF*, які розвиваються, можуть бути описані в рамках аналітичної моделі;
- розглядаються властивості перколяційного кластера, який часто зустрічається в ІТКМ;
- Romualdo Pastor-Satorras andAlessandroVespignani розглядали не тільки топологію ІТКМ як *SF* мережу, але аналізували процес поширення епідемії на таких мережах [26]. Отримали дані по комп'ютерним вірусам і виявляли такі їх параметри, як середня «тривалість життя» вірусу і стійкість

до знищення. 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 M.J. Newman, D.J. Watts, S.H. Strogatz і ряду інших вчених. Вони вважають, що ІТКМ топологічно являє собою клас small-world мереж. В [26] розглядається Watts-Strogatz модель, яка відноситься до класу small-world мереж. Ця модель імітує структуру ІТКМ;
- Розглянуто проблему 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 [25], але і як основа для епідеміологічних моделей. Більш докладно ця тема розкрита в пункті «Епідеміологічні моделі»;
- BroadScale мережі розглядаються в [29], де аналізується Bak-Sneppen модель. Даний вид складних мереж найменш привабливий при моделюванні топології ІТКМ.

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

1.3.3. Моделювання процесів інформаційної взаємодії в ІТКМ

При розгляді питань, що стосуються моделювання процесів, які протікають в ІТКМ, основним підходом є застосування моделей впливу, інформаційного управління і протиборства [25]. Найбільш розповсюдженими є моделі впливу, оскільки вони найбільш адаптивні до вирішуваних завдань. Коротко охарактеризуємо найбільш популярні 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 [28].

Моделі незалежних каскадів (Independent Cascade Model) належить категорії моделей так званих «систем взаємодіючих частинок» (Interacting Particle Systems). Вузол мережі (агент) визначається аналогічно вищеописаній моделі. Коли агент *i* стає активним в деякий момент часу, він отримує шанс активувати на наступному (і тільки на наступному) кроці кожного зі своїх сусідів *j* з імовірністю p_{ji} (причому *j* можуть намагатися незалежно активувати і інші агенти) [26].

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

Модель Ізінга – математична модель, що описує виникнення намагнічування матеріалу. В [29] передбачається, що конформність чи 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 управління. Більш складні моделі, що описують ІТКМ на термодинамічних аналогіях, розглядалися в [20].

Для опису процесів розповсюдження 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. Для моделювання та аналізу таких складних систем іноді використовуються клітинні автомати. Клітинний автомат складається з набору об'єктів (у даному випадку агентів), які 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 незмінних локальних імовірносних правил, які можуть

залежати від станів найближчих сусідніх агентів в околиці даного агента, а також, можливо, від стану самого агента.

Досить поширеним є підхід вивчення моделей за допомогою ланцюгів Маркова, в якій вивчається вплив в команді (групі агентів). Пропонована модель є динамічною Байесовою мережею (Dynamic Bayesian Network – DBN) з дворівневою структурою: рівнем індивідів (моделюються дії кожного агента) і рівнем групи (моделюються дії групи в цілому).

Цікавими є моделі взаємної інформованості. Є агент, що входить в деяку соціальну мережу. Агент інформований про поточну ситуаційну обстановку (про дії і уявлення інших агентів, параметри середовища – так званому стані природи (state of nature) і т.п.). Ситуаційна обстановка впливає на наявний у агента набір цінностей, установок і уявлень, пов'язаних таким чином: цінності впливають на установки, а ті, у свою чергу, призводять до схильності до уявлень того чи іншого рівня. Зі схильностями уявлень про світ узгоджена ієрархічна система, яка знаходиться «в пам'яті» агента.

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.

В моделі узгоджених колективних дій ключове значення 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 і т.п.). 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 й

формують його (неповні) уявлення, на основі яких агент приймає свої рішення. І, нарешті, в межах соціальних зв'язків агенти можуть прикладати спільні зусилля по створенню локального суспільного блага і спільно користуватися ним. Тому структура ІТКМ робить сильний вплив на рішення агентів про прийняття участі в колективній дії.

ІТКМ також може розглядатися як комунікаційна система, за допомогою якої агенти повідомляють один одному про свою готовність взяти участь у колективній дії. Кожен агент інформований про готовність тільки своїх найближчих сусідів і на основі цього локального знання приймає рішення про участь, використовуючи правило прийняття рішень «я візьму участь, якщо приймеш участь ти» (механізм координації). Тобто 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: «ведучі» (initial adopters), «послідовники» (followers) і т.д. до «пізніх послідовників» (late adopters). Такі мережі сприяють координації наступним чином:

1) інформуючи кожну ступінь про більш ранні щаблі;

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) – ситуація, в якій не існує агента, для якого будь-яка комбінація зміни його дії та зміни його зв'язків приведе до кращого результату. Тільки рівноваги з повною участю або повною неучастю є рівновагами стабільної мережі.

1.3.4. Епідеміологічні моделі

Далі розглядаються відомі моделі розповсюдження інфекційних захворювань серед населення, проводиться їх математичний аналіз і

застосування до конкретних захворювань. Розглядається класична епідеміологічна SIR модель Кермак-Маккендрік, MSEIR і SEIR ендемічні моделі.

Є епідеміологічні моделі розповсюдження вірусів і боротьби з ними. Така модель може бути використана для прогнозування процесу поширення шкідливих програм та оцінки ефективності протидії їм. Зокрема, вона може застосовуватися для аналізу динаміки системи, інфекційних спалахів та інших процесів, пов'язаних з поширенням вірусів.

В деяких моделях проводиться аналогія між біологічними і комп'ютерними вірусами і розглядається адаптація методів математичної епідеміології до вивчення комп'ютерних вірусів. В таких моделях використовуються орієнтовані графи для вивчення поширення вірусів, а також для вивчення критичного порогу епідемії.

Деякі дослідники представляють аналіз динаміки розвитку епідемії в складних гетерогенних мережах. Розглядають вплив початкових умов і актуальність статистичних результатів дослідження. Вважається, що представлені теоретичні відомості становлять великий інтерес і можуть дати корисну інформацію для розробки стратегій стримування епідемії.

Цікавим є вірусний маркетинг в ІТКМ. Вірусний маркетинг – загальна назва різних методів розповсюдження реклами, що характеризуються поширенням в прогресії близької 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.

Для даного дослідження найбільш підходять оптимізаційні та імітаційні моделі. З них розглядаються моделі просочування і зараження (клас епідеміологічних моделей), так як дані моделі найбільш точно відображають специфіку розглянутих тут проблем. Даний клас моделей є дуже поширеним при дослідженнях процесів взаємодії в ІТКМ.

ВИСНОВОК ДО РОЗДІЛУ1

ІТКМ забезпечують практично повний спектр можливостей для обміну інформацією між користувачами – мережевими абонентами. ІТКМ надає різні сервіси для організації соціальних взаємовідносин між користувачами (абонентами). На сьогоднішній день найбільш популярним з них є соціальні мережі.Сучасні ІТКМ мають багато проблем з інформаційної безпеки.

У першому розділі були розглянуті питання інформаційної безпеки ІТКМ та функції захисту інформації.

Проведений аналіз моделювання топології ІТКМ, а також моделювання процесів інформаційної взаємодії в ІТКМ. Розглянуті епідеміологічні модели.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ МОДЕЛЕЙ ЗАГРОЗ РОЗПОВСЮДЖЕННЯ ШКІДЛИВОЇ ІНФОРМАЦІЇ В ІТКМ

За результатами огляду предметної області цікаво розглянути питання створення імітаційної та 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 часові витрати. Не враховуючи час на збір інформації про топологію мережі, який може складати близько тижня, безпосередньо моделювання ЗЗІ займає кілька годин навіть при використанні розподілених обчислювальних ресурсів. Аналітична модель може дати прогноз ЗРЗІ майже миттєво. З її допомогою можна отримати актуальні дані (до того моменту, коли кількість атакуючих абонентів буде максимальним) по динаміці ЗРЗІ.

Процес ЗРЗІ характеризується наступними особливостями [12,13,14,15]. Вважається, що у мережі існують вузли трьох типів:

- перший тип – атакуючі вузли, це вузли, які розповсюджують заборонену інформацію;
- другий тип – захищені вузли, що характеризуються тим, що не беруть участь у поширенні забороненої інформації і ніколи не будуть цим займатися;
- третій тип – потенційно вразливі вузли, які не беруть участь у 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, що дорівнює числу абонентів мережі, I_0– кількість абонентів-зловмисників – першопочатковихджерелзагрози, R_0 – кількість абонентівспочаткунесприйнятливихдо атакуючихдій,β – параметр, що відображає силузагрози, імовірність здійсненняатаки,γ – параметрвідображає ступіньпротидії загрозі, ймовірністьзахистуабонента(βіγв даному дослідженнівизначені якконстанти, але можуть бути виражені якфункції, залежні від психосемантичнихпрофілівабонентівІТКМ[30-32]), φ – коефіцієнттопологічноїуразливостімережі, що відображає внутрішню властивістьІТКМ, засновану на характеристикахїїтопології,якасприяє поширеннюзабороненої інформації, t – часпроцесу (звичайно, в умовних одиницях часу).

Потрібно розробитианалітичнумодель динамікиатаки$I(t)$ і захистувузлів$R(t)$

$I(t)= f(N,\beta,\gamma,\varphi,t)$

$R(t)= g(N,\beta,\gamma,\varphi,t)$.

Методикарозробкианалітичної моделівключає в себепослідовністьнаступнихдій:

1) формування імітаційної моделідля дослідженняхарактеруі параметрів процесу ЗРЗІ;

2) синтезаналітичних залежностейпараметрів процесу;

3) проведення експериментів з метоюперевірки точності(адекватності) моделі.

2.1. Імітаційне моделювання

Наведемо узагальнений алгоритмреалізації ЗРЗІ [3],ґрунтуючись наописіпроцесів, що протікаютьв реальнихІТКМ. Схема реалізаціїзагрозипредставленана рис. 2.1. Фактично цей алгоритм

представляє собою звичайну послідовність (або схему) дій, які можуть здійснюватися в кожній мережі.

Алгоритм ЗРЗІвІТКМ

Крок 1.Поширення ЗРЗІ (даліпроцес «атаки») ініціює якийсьабонент-зловмисник (на рис. 2.1. – вузол1), поширюючи повідомленнязІ(реалізує загрозу) за його спискомконтактів.Атакуможепочинатиодинзловмисникабо група.

Крок 2.Абоненти-одержувачі (вузли2,3,4), прийнявши повідомленнязІ, читають йогоівключаються в процесатаки, поширюючи її даліза своїм списком контактів (вузол3) або ігнорують або взагалі видаляють повідомлення (вузол2), тобтов атаціне беруть участь.Процесатаки зазвичаййделавиноподібно. Атакуючіабоненти незакінчуютьатаку, одного разу передавшиповідомленняіз забороненою інформацією. Вікноатаки,як правило,триває протягомдоситьзначного проміжку часуі залежить від типуподачіЗІ вповідомленні, зацікавленості абонентаі т.д.

Крок 3.Абоненти можутьперестати сприйматиі, відповідно, поширюватиЗІ (вузол5) (даліпроцес«захисту»), внаслідок вплив у механізмів захисту(наприклад, попередження про неї), тому повідомленнязІ відатакуючихабонентівбудуть постійновідхилятися.

Крок 4.Процес триває,покив мережіє абоненти-зловмисники, або єпотенційновразливівузли, якщо відсутній процесзахисту.

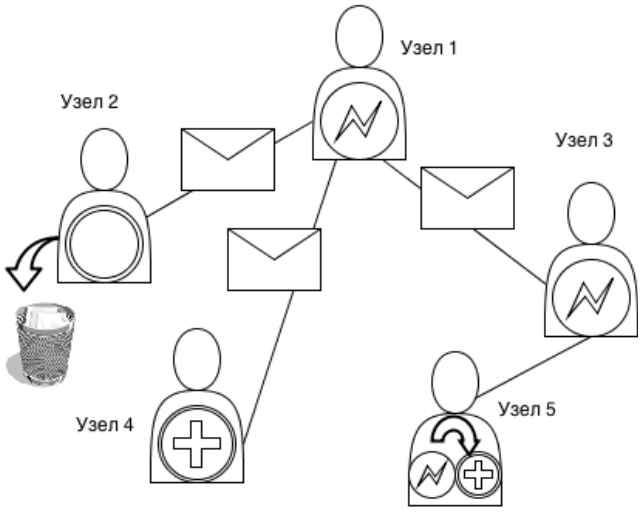


Рис. 2.1. Схема реалізації ЗРЗІ

Таким чином, ЗРЗІ вІТКМявляє собоюскладний динамічнийпроцес, що складаєтьсяз двохпротиборчихпід процесів – атакита захистувузлів мережі.

На основіописаногоалгоритму можна побудуватиімітаційнумодель ЗРЗІвІТКМ, якаскладається зрозробленої програмиModelGraphіданих, які можутьбути згенерованіза допомогою спеціального ПЗ. Дійсно, така модель була розроблена. Тут наведемо результати, що були отримані за допомогою даного підходу і які необхідні для подальшого дослідження. Спочатку опишемо імітаційну модель відповідно до [3].

Імітаційна модель ЗРЗІ

Вхідні дані:N,k – середній ступіньзв'язностівузлів,α – параметр, що відображає середню довжину шляхуірівень мережевоїкластеризації, β, γ(у моделівважається, щоβіγоднакові длякожного абонента), I_0, R_0.

Вихідні дані:$I(t)$, $R(t)$, $S(t)$ – чисельнімасиви даних, що описують динамічний процесреалізації ЗРЗІ(кількості атакуючих, захищених іпотенційно уразливихвузлівв кожнуумовну одиницючасувідповідно).

Нагадаємо, що параметр β – відображує силу загрози, це ймовірність здійснення атаки, коли β = 0– атака відсутня, γ – параметр, що відображує ступінь протидії загрозі, ймовірність захисту абонента, при γ = 0– захисту немає. Тут вони визначені як константи, але можуть бути виражені як функції, що залежать від психосемантичних профілів абонентів ІТКМ. I_0– кількість абонентів-зловмисників – першопочатковихджерелзагрози.

Згідно з [3] надамо послідовність дій до імітаційної моделі ЗРЗІ. Суть цих дій полягає створенні топологічної моделі ІТКМ, а потім у формуванні трьох множин вузлів: атакуючих, захищених, потенційно уразливих.

Крок1. СтвореннятопологіїІТКМ – графаG_{SW}=<V,E>, де G_{SW} – графsmall-worldмережі(на основі моделі Watts-Strogatz), V = {v_i} – множина вершин, E= {e_{ij}} – множина ребер,i= 1,…,N,j= 1,…,N. Даний крокздійснюється з використаннямвільнопоширюваноїпрограми Pajek, адаптованої під це завдання, за рахунок топологічнихпараметрів, які задаютьсяN,k, α.

Крок 2.Сформувати множину $V = \{V_I, V_S, V_R\}$, де $V_I = \{v^I_i\}$ – множина атакуючихвузлів ($|V_I| = I_0$), $V_R = \{v^R_i\}$ – множина захищених вузлів($|V_R| = R_0$), $V_S = \{v^S_i\}$ – множина потенційно уразливихвузлів ($|V_S| = N - I_0 - R_0$).

Крок 3. $\forall v^I_i$ якщо $\exists e_{ij}$ іv_j, $j = 1,\ldots,N$,то з імовірністюβвиконати: $V_S \backslash v_j$іV_I Uv_j, зймовірністю γвиконати: $V_I \backslash v_j$, V_R U v_j.

Крок 4.Якщо$V_I = \emptyset$або$\gamma = 0$і$V_S = \emptyset$, то кінець алгоритму, інакше перейти до кроку3.

ModelGraph – програма для імітаційного моделювання ЗРЗІ в ІТКМ, яка описана в [2]. Даний програмний продукт є однопоточним додатком. Програма складається з виконуваного файлу ModelGraph.exe і бібліотеки chartdir50.dll для побудови графіків. Після вибору типу мережі та введення її параметрів відбувається імітаційне моделювання за наведеним алгоритмом. Потім результати відправляються в функцію побудови графіків для виведення результатів у графічному вигляді. Програма написана в середовищі розробки Microsoft Visual Studio.NET 2008. Вихідними даними для гетерогенної мережі є файл формату .net, визначений в програмі Pajek.

ПЗPajekявляє собою програму, дляOCMS Windows, призначену для аналізуівізуалізаціївеликихмереж.Дана програмазнаходиться у вільному доступіі призначена длянекомерційного використання.

Тепер надамо результати ряду обчислювальних експериментів [8] з використанням даної імітаційної моделі(φкоефіцієнттопологічноїуразливостімережі) і які торкалися наступних питань:

- впливсилиатакина процес;
- впливзначеннясереднього ступенязв'язностівузлів умережіна процес;
- впливкількостіпочатковоатакуючихвузлівна процес.

Таблиця 2.1

Таблиця експерименту

Номер експерименту	N	φ	I_0	β
1	1000	20	1	0,1-0,9
2	1000	0,5-60	1	0,5
3	1000	20	1-40	0,5

Як відзначено в [3], що кожен з трьох типів експериментів проводився 100 разів, бралися усереднені значення.

За результатами даних експериментів зроблено наступні важливі висновки, які використовувалися в подальшому:

- процес атаки $I(t)$ має експоненційну залежність;
- при збільшенні значень φ, I_0, β зростає динаміка зараження вузлів (інтенсивність атаки);
- 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);
- коефіцієнт топологічної уразливості φ має найбільший вплив (порівняно з I_0, β) на тривалість процесу. Наприклад, при φ = 0,5 (низька вразливість) атака триває 24 умовні одиниці часу, а при φ = 60 всього лише 4;
- велика кількість початково 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.

Дали наведені експерименти, умови яких суттєво ускладнюються шляхом додавання підпроцесу захисту, який залежить від початкової кількості захищених вузлів R_0 і ймовірності захисту γ.

Таблиця 2.2

Таблиця експерименту

Номер експерименту	N	φ	I_0	β	γ	R_0
1	1000	20	1	0,5	0,1-0,9	0
2	1000	20	1	0,5	0,5	0-200

За результатами даних експериментів зроблено наступні висновки:

- введення підпроцесу захисту збільшує час всього процесу ЗРЗІ;
- при невеликих значеннях ймовірності захисту ($\gamma < 0,3$) загроза реалізується практично на всіх вузлах в мережі;
- при невеликих значеннях ймовірності захисту ($\gamma < 0,3$) час процесу складає більше 50 умовних одиниць часу;
- при великій імовірності захисту ($\approx 0,9$) процес триває ≈ 7 умовних одиниць часу і максимальну кількість атакуючих вузлів знижується залежно від імовірності проведення атаки;
- при випадковому виборі спочатку захищених вузлів картина процесу атаки практично не змінюється;
- при високій топологічної уразливості зростає тривалість процесу ЗРЗІ.

Представлені результати фактично підтверджують основні міркування щодо поведінки та взаємозв'язків використаних в моделі параметрів.

Наведені висновки використовуються в подальшому для дослідження розповсюдження забороненої інформації в конкретних ІТКМ. Спочатку розглядається відома епідеміологічна модель розповсюдження вірусів в мережах. Далі, на відміну від [3], запропонована певна модифікація моделі, яка експериментально досліджується.

2.2. Моделі динаміки розповсюдження хробаків

Серед різноманітних застосувань моделей в захисті інформації дуже цікавим є дослідження динаміки розповсюдження вірусів в мережах.

Дослідження особливостей розповсюдження мережевих хробаків останні роки стало дуже популярною темою. Математичний апарат для вивчення динаміки «звичайних» біологічних епідемій розроблений давно, проте цей напрямок набув став модним лише в 2001 році, коли стався спалах вірусів Code Red і Nimda. Основні і досить неприємні для перспектив безпеки результати можна отримати вже з аналізу класичних моделей епідемій, які

підходять для вивчення комп’ютерних інфекцій навіть дещо ліпше, ніж для їх біологічних аналогів [25].

На сьогоднішній день відомий досить широкий спектр результатів досліджень в області моделювання процесу поширення вірусів. З метою визначення можливості їх застосування для аналізу процесу поширення вірусів в ІТКМ обмежимося згадкою найбільш типових з них.

Роботи, присвячені аналізу процесу поширення вірусів, традиційно діляться на два основних напрямки [25]: аналітичний та імітаційний.

Моделі аналітичного напряму в свою чергу можна розділити на дві групи. Моделі першої групи (наприклад, [25]) не враховують структуру мереж, але надають можливість для аналізу важливих з точки зору вірусної загрози станів вузлів з урахуванням часу. Історично склалося, що такі моделі з'явилися піонерськими в даній області і були запозичені з математичних основ епідеміології. У цих моделях вся множина об'єктів в зоні ризику поділялася на кілька підмножин «інфікованих», «вразливих до зараження», «вилікуваних» і т.д., а динаміка чисельності цих підмножин описувалася диференціальними рівняннями.

Моделі другої групи враховують структуру мереж. Але вони або обмежені використанням завідомо недостатньої кількості станів вузлів через високу обчислювальну складність застосовуваних методів (наприклад, [15-17]), або не дають інформації про стан захищеності кожного конкретного вузла мережі в за даний момент часу (наприклад, [18]).

Одна з найбільш вдалих класифікацій моделей і систем імітаційного напрямку представлена в [19]. Імітаційні моделі отримали широке застосування в умовах появи високопродуктивних систем імітаційного моделювання, в тому числі об'єктно-орієнтованих (приклад такої системи показаний в [20]).

Вони забезпечують високу точність моделювання при великій кількості мережевих вузлів. Однак такі моделі вимагають детального знання

алгоритмів інформаційної взаємодії вузлів мережі, які часто є недоступними для дослідника.

Для найбільш ймовірних на практиці вихідних даних тільки про структуру ІТКМ і середньостатистичних часових характеристик функціонування вірусів і ПЗІ [21] їх вузлів пріоритет мають аналітичні моделі. Вони відрізняються високою швидкістю моделювання і можливістю отримання рішення «в загальному вигляді» [5]. Однак спроби застосування відомих аналітичних моделей до процесу поширення вірусів або їх комбінацій для потенційно доступного набору вихідних даних про ІТКМ виявилися безуспішними, оскільки переваги цих моделей з лишком перекривалися їх недоліками. В результаті виникла потреба в розробці нового підходу, що парирує недоліки відомих аналітичних моделей в даній області.

В даний час відомо кілька різновидів математичних моделей поширення комп'ютерних вірусів, розроблених на основі біологічних підходів, які відрізняються між собою областю обмеження і умовами застосування в реальних технічних системах. Серед них можна виділити наступні моделі:

- SI (Suspected-Infected), загальна кількість об’єктів $N = S(t) + I(t)$, де $S(t)$ – кількість вразливих об'єктів, $I(t)$ – кількість заражених об'єктів;
- SIR (Suspected-Infected-Recovered), загальна кількість об’єктів $N = S(t) + I(t) + R(t)$, де $S(t)$ – кількість вразливих об'єктів, $I(t)$ – кількість заражених об'єктів, $R(t)$ – кількість вилікуваних об'єктів, що володіють імунітетом;
- SEIQR (Suspected-Exposed-Infected-Quarantined-Recovered) загальна кількість об’єктів $N = S(t) + E(t) + I(t) + R(t) + Q(t)$, де $S(t)$ – кількість вразливих об'єктів, $E(t)$ – кількість об'єктів, заражених вірусом, але не розповсюджують інфікування (латентний період вірусу), $I(t)$ – кількість заражених об'єктів, $R(t)$ – кількість вилікуваних об'єктів, що володіють імунітетом, $Q(t)$ – кількість об'єктів в карантині;

- PSIDR (Progressive Suspected-Infected-Detected-Recovered) загальна кількість об’єктів $N = S(t) + I(t) + R(t) + D(t)$, де $S(t)$ – кількість вразливих об'єктів, $I(t)$ – кількість заражених об'єктів, $R(t)$ – кількість вилікуваних об'єктів, що володіють імунітетом, $D(t)$ – кількість знайдених заражених об'єктів.

Проведені дослідження показали, що існуючі моделі поширення комп'ютерних вірусів на даний момент мають ряд недоліків:

1) не враховують зв'язність комп'ютерної мережі;

2) не враховують часові затримки як всередині кожної комп'ютерної локальної мережі, так і на «мостах».

2.2.1. Проста епідемічна модель

Розглянемо більш детально просту епідемічну модель, в якій вважається, що будь-який вузол мережі, яка складається з постійної кількості комп’ютерів (всього їх N), може бути уразливим (S) або інфікованим (I), тобто $N = S + I$. Припустимо, що на кожному інфікованому вузлі може існувати лише одна копія хробака, яка випадковим чином обирає в доступному адресному просторі потенційну жертву зі середньою швидкістю β на одиницю часу (тобто на пошук і зараження одної жертви витрачається $1/\beta$ секунд). У найпростішому випадку в можна визначити швидкістю сканування мережі хробаком (V_s) і розміром її адресного простору (N_{ip})

$$\beta = V_s \frac{N}{N_{ip}}. \qquad (8)$$

Якщо ввести змінні $i = I/N$ (доля інфікованих вузлів) і $s = S/N$ (доля неінфікованих вузлів, $s = 1 – i$), неважко отримати рівняння динаміки частини інфікованих вузлів

$$\frac{di}{dt} = \beta(1-i)i. \qquad (9)$$

Це рівняння має аналітичний розв'язок, який, зважаючи на те, що в початковий момент часу $t_0 = 0$ доля інфікованих вузлів складає i_0, виглядає так

$$i(t) = \frac{i_0}{i_0 + (1 - i_0)\exp(-\beta t)}. \qquad (10)$$

З цієї формули випливає, що епідемія у прийнятій моделі цілком залежить від двох параметрів: швидкості розмноження хробака β і початкової зараженості мережі i_0. Як показує досвід, цілком справедливою є така оцінка – хробак починає атаку на мережу приблизно з одного комп'ютера.

Аналіз динаміки останньої функції дозволяє виділити три етапи:

1-й етап – повільне зростання зараженості до деякого порогового значення $i_{\text{пор}} \approx 0.05$;

2-й етап – вибухова фаза в діапазоні $0.05 < i < 0.95$;

3-й етап – насичення, $i > 0.95$, на цій ділянці при випадковому скануванні адресного простору заражені вузли переважно контактують між собою і неінфіковані вузли можуть залишатися «чистими» невизначено довгий час.

Для досягнення порогу насичення $i = 0.95$ необхідний час

$$t = \frac{1}{\beta}\ln(19\frac{1 - i_0}{i_0}), \qquad (11)$$

з чого виникає, що динаміка епідемії не залежить від масштабів мережі. Наприклад, мережа з мільйону комп'ютерів, в якій в початковий момент буде інфіковано лише один вузол, практично буде зараженою за той же час, що і аналогічна мережа зі ста мільйонів зі ста зараженими вузлами у початковий момент.

Викладене дає можливість зробити наступні висновки:

- однорідність мережі відносно певної уразливості представляє головну загрозу. Як показує практика, навіть хробаків, що обирають жертву

випадковим чином, отже, є найбільш повільними, можуть за лічені хвилини уразити ключові вузли Інтернету;

- експоненційне зростання кількості вірусів у будь-якій мережі свідчить про відсутність захисних механізмів або про їх повну неефективність;
- механізм випадкового вибору жертви обмежує знизу швидкість розповсюдження вірусів по мережі. Суттєво її збільшити можна досить простими засобами: попередньо підготувати список адрес для атаки, сканувати підмережі, виділити для кожної копії хробака окремого фрагмента мережевого адресного простору і ін.;
- інфекційна здатність β значною мірою залежить від швидкості проходження мережевих пакетів. Сучасні Web-додатки орієнтовані на передачу великих масивів даних, що автоматично підвищує швидкість розповсюдження хробаків;
- системи раннього сповіщення про розвиток епідемії виявляються ефективними лише на ділянці $i<<i_{\text{пор}}$ і при низьких значеннях β. Але аналіз звернень до неіснуючих адрес дозволяє визначити ознаки вірусної активності при зараженні 1-2% уразливих вузлів. Це означає, що попередження можна отримати через дуже короткий час, тобто епідемії можна лише зафіксувати, але не запобігти;
- ефективність мережевих епідемій можна значно підвищити шляхом попереднього зараження окремих уразливих вузлів;
- збільшення адресного простору знижує інфекційну здатність хробаків з випадковим вибором жертви, особливо коли адреси рівномірно «розмазані» по всьому просторі.

Аналіз епідемій вірусів CodeRed v2 і Slammer на основі даної моделі показав задовільне спів падіння з реальною динамікою епідемій.

2.2.2. Інші варіанти епідемічної моделі

Фактори, що забезпечують затухання мережевих епідемій, оцінюються на моделі, в якій мережеві вузли бувають трьох типів: уразливі (*S*), інфіковані (*I*), несприйнятливі (*R*), тобто $N = S + I + R$. Спочатку припустимо, що вузли виявляються невразливими лише після їх лікування. Якщо ввести постійну середню швидкість «імунізації» на одиницю часу γ, отримаємо систему рівнянь

$$\begin{cases} \dfrac{ds}{dt} = -\beta is, \\ \dfrac{di}{dt} = \beta is - \gamma i, \\ \dfrac{dr}{dt} = \gamma i. \end{cases} \qquad (12)$$

В цій моделі існує порогова умова для розвитку епідемії. На ділянці зростання $i(t)$ похідна di/dt повинна бути позитивною. Оскільки $s(t)$ постійно зменшується за рахунок інфікованих комп'ютерів, то отримаємо, що для початку епідемії необхідно

$s(0) > \gamma r/\beta$.

На жаль, така умова виконується досить легко, оскільки γ визначається людською реакцією, яка зазвичай запізнюється, та необхідністю завантаження громіздких «латок». Крім того, β постійно збільшується за рахунок технічних характеристик мережі та «доброї волі» зловмисника (він може, наприклад, зробити паузу в циклі розмноження і знизити швидкість інфікування).

В реальних умовах «імунітет» шляхом установки антивірусного ПЗ, міжмережевих екранів і інших «латок» набувають не лише інфіковані вузли, а і уразливі. Вважаючи, що середня швидкість імунізації приблизно однакова для вузлів обох типів і дорівнює γ, отримаємо систему рівнянь

$$\begin{cases} \dfrac{di}{dt} = \beta i(1-r-i) - \gamma i, \\ \dfrac{dr}{dt} = \gamma(1-r), \end{cases} \qquad (13)$$

причому умова розвитку епідемії зберігається.

З цієї системи отримаємо $r(t) = 1 - \exp(-\gamma t)$, звідкіля випливає, що за достатньо великий час епідемію, здається, можна подолати. Але цей час може виявитися неприйнятно великим. Цей час частково можна було б скоротити за рахунок автоматизації процесів усунення уразливостей. Проте на практиці імунізація незаражених вузлів здійснюється набагато повільніше, оскільки зазвичай люди діють за принципом «поки грім не гряне».

Динаміка системи зі змінним числом вузлів визначатиметься швидкістю приросту нових уразливих вузлів (S)

$$\begin{cases} \dfrac{ds}{dt} = -\beta is - (\gamma+\alpha)s + \alpha, \\ \dfrac{di}{dt} = \beta is - (\gamma+\alpha)i, \\ \dfrac{dr}{dt} = \gamma(1-r) - \alpha r. \end{cases} \qquad (14)$$

Тепер умова розвитку епідемії набуває вигляду

$s > (\gamma + \alpha)/\beta$.

За такої умови в система має постійний рівень, до якого прагне доля інфікованих комп'ютерів. Це означає, що в реальних умовах від конкретного вірусу в системі з приростом уразливих вузлів повністю позбавитись неможливо навіть при автоматичній «вакцинації».

Моделювання і порівняння його результатів з фрагментарними даними спостерігачів за розвитком реальних епідемій підштовхує до інтуїтивно зрозумілого висновку: масове розповсюдження ПЗ, однорідного відносно конкретної уразливості і вкрай низька швидкість усунення виявлених «дірок» призводять до того, що високі технології створюють більше проблем, ніж

вирішують. Поспішне впровадження неперевірених новацій створило патову ситуацію: з одного боку неможливо безболісно відмовитись від нововведень, що стрімко змінюють середовище проживання людини, а з іншого – небезпека цих нововведень зростає з кожним днем.

Оповіщення про нові «дірки» зараз налагоджено непогано, проте переважна маса користувачів ігнорує попередження, оскільки не має достатньої кваліфікації, щоб зрозуміти їх зміст. Крім того, зараз творці вірусів навчилися успішно блокувати та навіть знищувати антивірусні засоби.

2.3. Аналітична модель

Аналізуючи процес інформаційної взаємодії абонентів при поширенні забороненої інформації в ІТКМ, можна зробити наступні висновки. Як виявляється, в ІТКМ завжди приймають участь три типи абонентів:

- атакуючі абоненти, які поширюють заборонену інформацію;
- захищені абоненти, що характеризуються тим, що не беруть участь у поширенні забороненої інформації і ніколи не будуть цим займатися;
- потенційно вразливі абоненти, які можуть бути схильні до негативного впливу з боку атакуючих вузлів і можуть почати поширювати заборонену інформацію.

При цьому спостерігається два протиборчі підпроцеси – атаки та захисту абонентів мережі. Для моделювання таких явищ часто застосовують епідеміологічні моделі. Зокрема нашому опису точно відповідає SIR-модель Кермак-Маккендрік [27]. Характер графіків, отриманих в результаті імітаційного моделювання (рис. 2.2), схожий з результатами, які дає дана модель [4]. Виходячи з вищесказаного, приходимо до висновку, що дана модель є найбільш релевантною для цього дослідження.

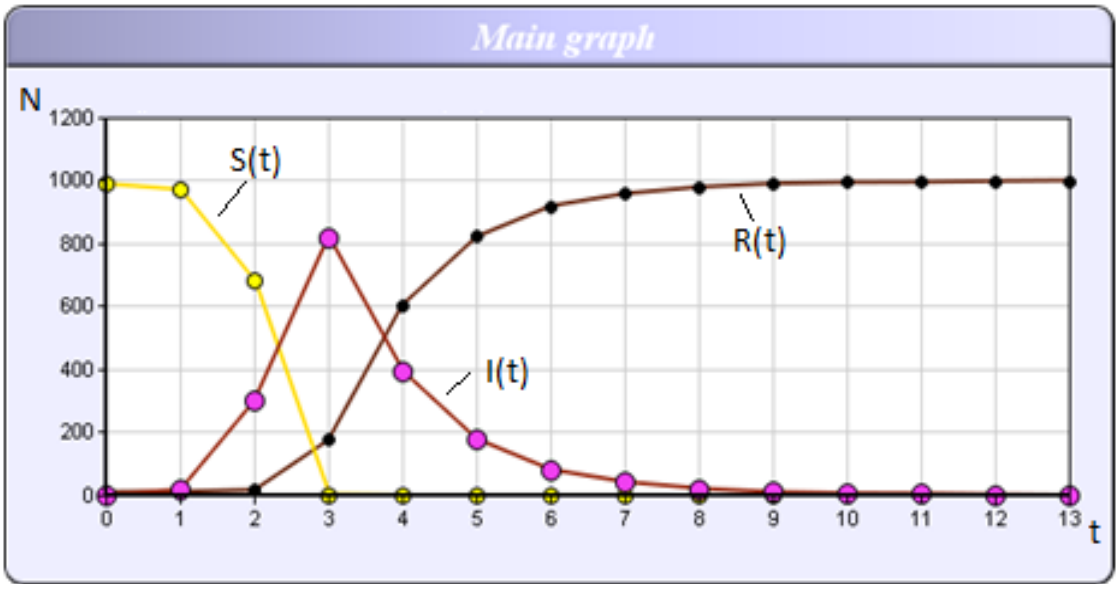


Рис.2.2. Імітаційне моделювання(N= 1000, φ = 20, I_0 = 1, β = 0,5, γ = 0,5, R_0 = 10), $S(t)$ – кількість схильних до атакивузлів

SIR(від англ.Susceptibles – Infectives – Removedwithimmunity) – епідеміологічнімодель, спрощено описуєпоширеннязахворювання, що передаєтьсявідодного індивіда до іншого, яка розглядаєсуб'єктівз поглядутрьох можливихстанів:сприйнятливий, інфікований, імунізований.

Системадиференціальнихрівнянь, що описуютьSIR-модель, має вигляд:

$$\begin{cases} \dfrac{dI}{dt} = \beta \dfrac{S(t)I(t)}{N} - \gamma I(t), \\ \dfrac{dR}{dt} = \gamma I(t), \\ \dfrac{dS}{dt} = -\beta \dfrac{S(t)I(t)}{N}, \end{cases} \qquad (15)$$

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

При використанні даної системи для аналізу ЗРЗІ в ІТКМ отримуємо результати у вигляді графіків (рис. 2.3), які хоч і правильно описують характер процесу, але не дають потрібної точності прогнозу [4].

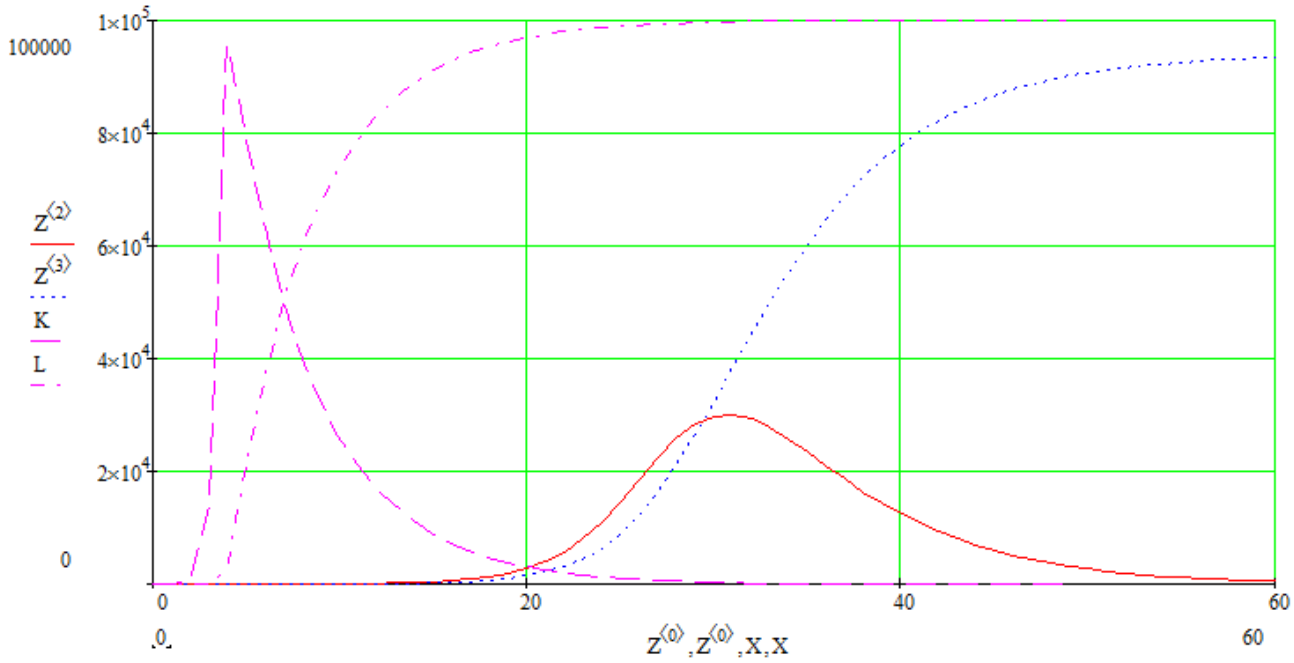


Рис. 2.3. Результати імітаційного моделювання (N = 100000, φ = 150, I_0 = 1, β = 0,3, γ = 0,2, R_0 = 0) і аналітичного рішення ($Z^{<2>}$, $Z^{<3>}$ – аналітичний розв’язок для процесів атаки та захисту відповідно, K, L – результати імітаційного моделювання для процесів атаки та захисту відповідно)

Суттєві відхилення запропонованої моделі підтверджують міркування про те, що запропонована модель не дає потрібної точності у зв'язку з тим, що в моделі, яку вона описує, не враховуються топологічні особливості мережі. У зв'язку з цим було поставлено завдання адаптування цієї системи під прогнозування ЗРЗІ в ІТКМ шляхом інтегрування до неї параметра топологічної уразливості мережі φ.

Проаналізувавшиграфіки, отримані за результатами імітаційного моделювання тааналітичного розв’язку даної системи, і

простежившифізичний змістрівняньв даній системі[27], можна прийтидо наступного висновку.

Процесзахисту незалежить відтопології мережі,тому «змінювати» $R(t)$ не має сенсу.А осьпроцесатаки може залежати від структуризв'язків міжабонентамив мережі. Реально параметртопологічноїуразливостіφможе впливати на$I(t)$ через коефіцієнтβ. Тоді у загальному виглядіадаптовануможна представити в наступномувигляді:

$$\begin{cases} \dfrac{dI}{dt} = C\beta \dfrac{S(t)I(t)}{N} - \gamma I(t), \\ \dfrac{dR}{dt} = \gamma I(t), \\ \dfrac{dS}{dt} = -C\beta \dfrac{S(t)I(t)}{N}, \end{cases} \qquad (16)$$

де C – коефіцієнт, що залежить від параметра φ.

Відзначимо, що в [2] вже пропонувався аналогічний підхід, при цьому зазначалося, що коефіцієнт C може бути виражений функцією або апроксимований константою.

Аналіз топологій великомасштабних ІТКМ показав, що типові значення параметра φ для них знаходяться в діапазоні від 100 до 600.

Як показано в [2], результати серії експериментів з імітаційного моделювання ЗРЗІ в ІТКМ дозволили одержати залежність параметра C від φ у вигляді $C = 2*\ln\varphi$. Апроксимація проводилась методом найменших квадратів з використанням пакету MathCAD.

Отже, в [2] підсумкова система мала вигляд:

$$\begin{cases} \dfrac{dI}{dt} = 2\ln\varphi\beta \dfrac{S(t)I(t)}{N} - \gamma I(t), \\ \dfrac{dR}{dt} = \gamma I(t), \\ \dfrac{dS}{dt} = -2\ln\varphi\beta \dfrac{S(t)I(t)}{N}. \end{cases} \qquad (17)$$

Система даних диференціальних рівнянь дозволила, згідно з [2], отримати прогноз ЗРЗІ у великомасштабній ІТКМ (N = 105...108) з похибкою до 20%.

Однак, як показує більш детальний розгляд, запропонована логарифмічна залежність виглядає досить штучною і призводить до певних обчислювальних ускладнень. Тому в даній роботі пропонується спрощена залежність, а саме, лінійна апроксимація даної величини $C = k*\varphi + b$. Розрахунки за допомогою MatLAB показують, що для зазначеного діапазону параметра φ апроксимація матиме вигляд лінійної залежності $C = 0{,}0072*\varphi + 8{,}48$.

Тоді система диференціальних рівнянь матиме остаточний вигляд:

$$\begin{cases} \dfrac{dI}{dt} = (0{,}0072\varphi + 8{,}48)\beta \dfrac{S(t)I(t)}{N} - \gamma I(t), \\ \dfrac{dR}{dt} = \gamma I(t), \\ \dfrac{dS}{dt} = -(0{,}0072\varphi + 8{,}48)\beta \dfrac{S(t)I(t)}{N}. \end{cases} \quad (18)$$

Саме ця система диференціальних рівнянь була досліджена в подальшому. Розрахунки проводилися за допомогою системи MathLAB. Чисельні результати з [4], що використовувалися для порівнянь та власні експериментальні дані наведені в додатку Б.

2.4. Дослідження аналітичної моделі

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

Було проведено три експерименти з наступними вхідними даними.

Таблиця 2.3

Таблиця експерименту

Номер експерименту	β	γ	R_0	I_0
1	0,5	0,51	0	1
2	0,5	0,51	0	1
3	0,5	0,51	$4*10^6$	1

Знову нагадаємо, що параметр β – відображує силу загрози, це ймовірність здійснення атаки, при β = 0– атака відсутня, γ – параметр, що відображує ступінь протидії загрозі, ймовірність захисту абонента, при γ = 0– захисту немає. I_0– кількість абонентів-зловмисників – першопочатковихджерелзагрози, R_0–початкова кількість захищених вузлів.

За допомогою MatLAB отримані розв'язки останньої системи диференціальних рівнянь, тобто розподіли величин $I(t)$ та $R(t)$ за часом. Ці розподіли показують динаміку зміни кількості вузлів мережі, які захищені та є джерелами загроз (додаток Б).

Для порівняння обчислювальних експериментів використовувалися дані, що були отримані в роботі [2] для імітаційної моделі для мережі «ВКонтакте».

На рис. 2.4 приведені результати імітаційного моделювання та аналітичного розв'язку для β = 0,5, γ = 0,51, R_0 = 0, I_0 = 1.

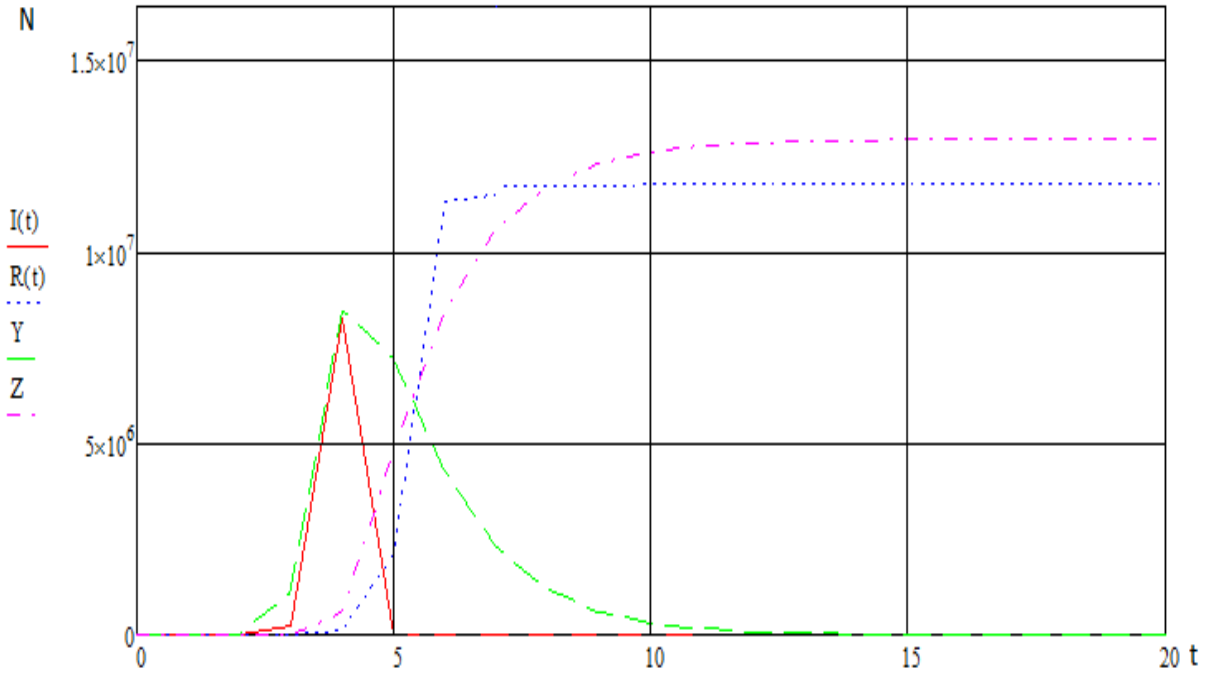


Рис. 2.4. *I* і *R* – аналітичний розв'язок, *Y* і *Z* – результати імітаційної моделі

На рис. 2.5 приведені результати імітаційного моделювання та аналітичного розв'язку для $\beta = 0{,}5$, $\gamma = 0{,}51$, $R_0 = 0$, $I_0 \approx 24000$.

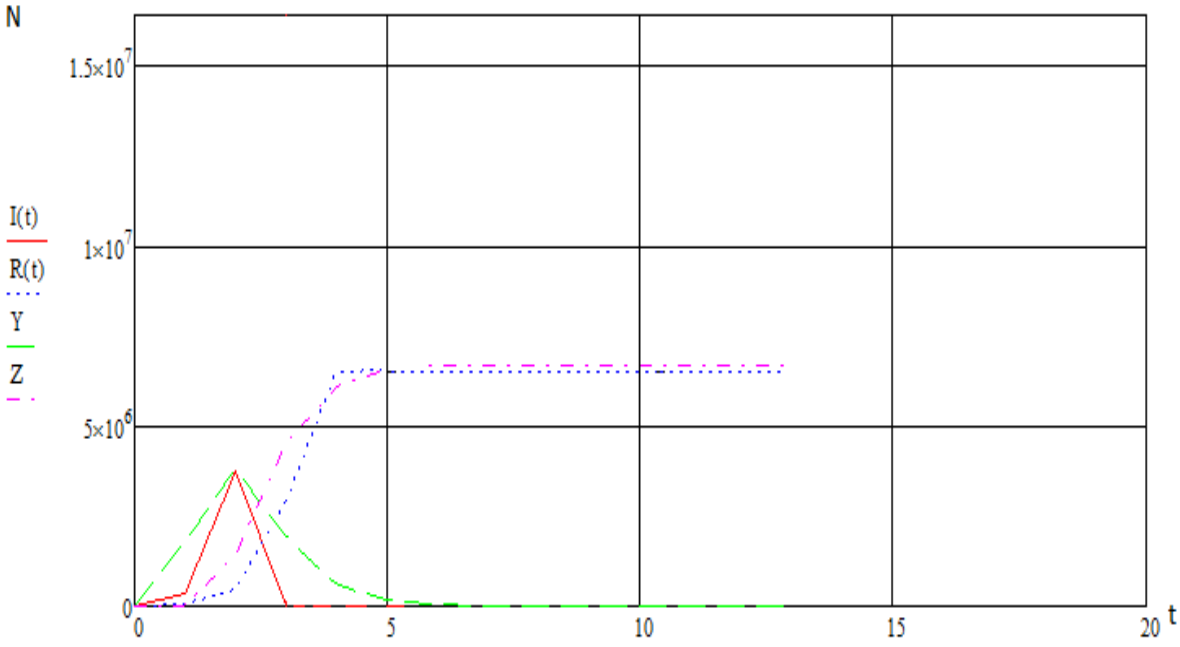


Рис. 2.5. *I* і *R* – аналітичний розв'язок, *Y* і *Z* – результати імітаційної моделі

На рис. 2.6 приведені результати імітаційного моделювання та аналітичного розв'язку для $\beta = 0{,}5$, $\gamma = 0{,}51$, $R_0 \approx 4*10^6$, $I_0 = 1$.

Експеримент 1 (рис. 3.5): $\varphi = 200$, $\beta = 0{,}2$, $\gamma = 0{,}8$, $I_0 = 1$, $R_0 = 0$.

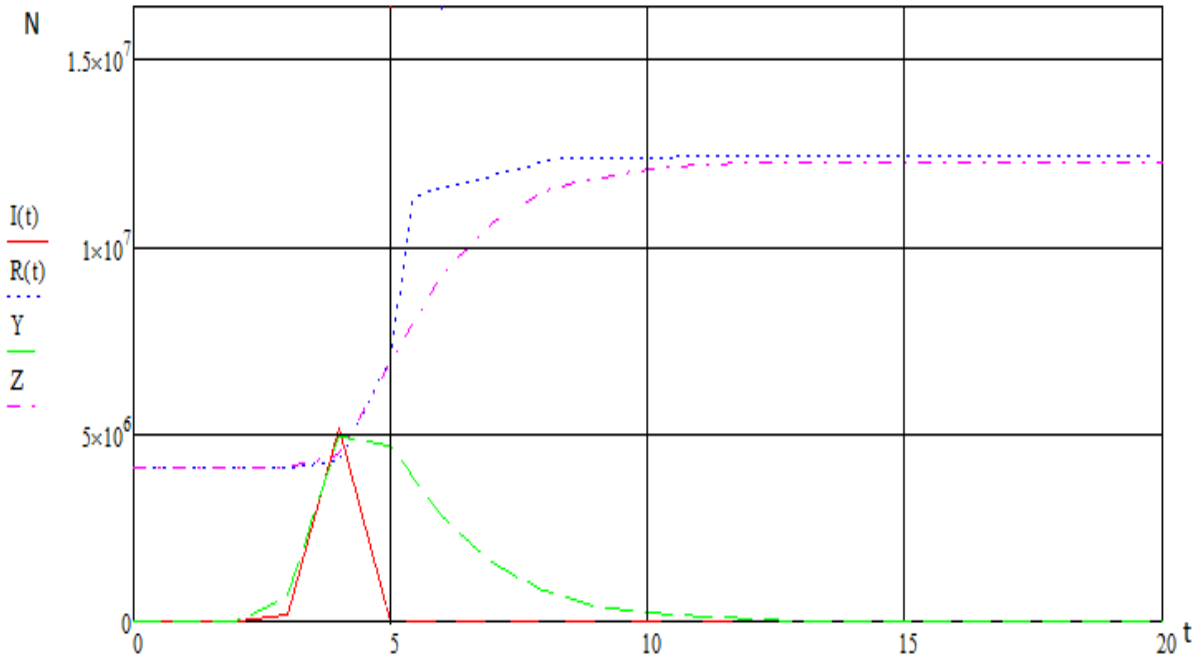


Рис. 2.6. I і R – аналітичний розв'язок, Y і Z – результати імітаційної моделі

Як видно з рисунків величини Zта $R(t)$ з часом виходять на певну «платформу», а Y та $I(t)$ – на нульову «платформу». Це свідчить про певну стабілізацію захисту та знищення заражених вузлів.

За результатамиекспериментів булизроблені наступні висновки:

- результатианалітичногорішення підходятьдля апроксимаціїімітаційнихрезультатів,при цьомупохибка апроксимаціїдляпроцесу захисту$R(t)$ становить не більше10%, для процесуатаки$I(t)$ – не більше 15%;

- при середніхзначенняхсилиатаки ізахисту ($\beta,\gamma \in [0,3;\ 0,7]$) похибказалишається в тому ждіапазоні($\Delta R(t)$ <10%, $\Delta I(t)$ <15%), при сильній атаки ізлабкому захистіінавпаки – може складати близько20%;
- при моделюванніз великою кількістюспочаткуатакуючихвузлів (70 >>1) похибка становить: $\Delta R(t)$ <10%, $\Delta I(t)$ <15%;
- при додаваннів мережувеликої кількостіспочаткузахищених вузлів($\approx 4*10^6$) аналітичне рішеннядаєрезультатз $\Delta R(t)$ <10%, $\Delta I(t)$ <15%;
- порівнюючи дані результати з результатом застосування вихідної системи диференціальних рівнянь, можна говорити про значне збільшення точності прогнозування процесу ЗРЗІ в ІТКМ за рахунок урахування впливу на процес топологічної уразливості мережі.

Отже, створена імітаційна модель ЗРЗІ 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 ЗРЗІ від топологічної уразливості мережі.

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

ВИСНОВОК ДО РОЗДІЛУ 2

За результатами огляду предметної області цікаво розглянути питання створення імітаційної та 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 часові витрати. Не враховуючи час на збір інформації про топологію мережі, який може складати близько тижня, безпосередньо моделювання ЗЗІ займає кілька годин навіть при використанні розподілених обчислювальних ресурсів. Аналітична модель може дати прогноз ЗРЗІ майже миттєво. З її допомогою можна отримати актуальні дані.

Тому другий розділ присвячений дослідженню моделей загроз розповсюдження шкідливої інформації в ІТКМ.

РОЗДІЛ 3. МОДЕЛЮВАННЯ ЗАГРОЗИ РОЗПОВСЮДЖЕННЯ ШКІДЛИВОЇ ІНФОРМАЦІЇ В ІТКМ

Комп'ютерні засоби моделювання застосовуються для визначення характеристик або значень деяких фізичних величин, які обчислювати неможливо або складно отримати традиційними шляхами. Увага при цьому приділяється швидше обчислювальним потужностям використовуваної апаратури і програм, ніж візуальної ефектності і дружності користувальницьких складових.

На сьогодні можна виділити такі напрямки в моделюванні комп'ютерних мереж, помітні по мети моделювання та поданням мережевих пристроїв

1. Моделювання на параметричному рівні. При цьому підході комп'ютерна мережа розглядається як точна математична модель, що дозволяє отримувати конкретні описові параметри і величини.

2. Моделювання на функціональному рівні. Комп'ютерні мережі, в цьому випадку, досліджуються з точки зору їх функціонування; робота мережевих пристроїв представляється поведінковими моделями, які не передбачають обчислення точних тимчасових або завантажувальних характеристик.

Перший підхід в деякій мірі можна асоціювати з дослідницькою роботою, другий – з навчальною. Параметричний аналіз є більш трудомістким, складним, точним і дозволяє реально оцінювати роботу мережі. Аналіз комп'ютерної мережі на функціональному рівні призначений, головним чином, для виявлення закономірностей її роботи, принципів дії використовуваних мережевих пристроїв і протоколів, дослідження переваг та недоліків концептуальних рішень і топологій.з-х000=т

Імітаційна модель ЗРЗІ в ІТКМ, що розглянута раніше, хоча і враховує топологічні характеристики мережі, але залишається проблема урахування конкретних особливостей топології мереж. Нижче розглядаються деякі міркування щодо спрощеної процедури урахування таких особливостей.

3.1. Формування топології ІТКМ

Підтопологієюбудеморозуміти структуруінформаційних зв'язківміж вузлами мережі. Топологічніхарактеристики(середняступіньзв'язностівузлів, розподіл ступенівзв'язностівузлів, кластернийкоефіцієнтмережі, середня довжина шляхумережі)в роботі розглядаютьсяякосновні технічніуразливостіІТКМдо реалізаційзагроз.Іншіуразливості: використання неліцензійного ПЗ ввузлах, некоректно налаштованіміжмережеві екранії т.д. тут не розглядаються.

Для моделювання ЗРЗІ необхідно мати топологію реального об'єкта. Пряме отримання цієї інформації утруднено у зв'язку з наступним протиріччям. Для підвищення точності результатів моделювання необхідно мати топологію всієї мережі. Отримати таку інформацію без прав адміністратора не представляється 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 та 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. У такому випадку неможливо отримати навіть ідентифікатор вузла. Таких вузлів в мережі незначна частина. Емпірично показано [29], 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 мережі «ВКонтакте» це

значення приблизно складає 10 запитів в секунду). Це обмеження призводить до того, що, враховуючи масштабність ІТКМ (десятки мільйонів вузлів), отримання інформації про топологію мережі перетворюється на тривалий процес (наприклад, для мережі «ВКонтакте» отримання інформації про $16*10^6$ вузлів зайняло близько 20 діб). Враховуючи, що час сесії обмежений (наприклад, для мережі «ВКонтакте» це значення дорівнює одної доби), дана особливість повинна враховуватися при практичній реалізації.

2) Відомі засоби (наприклад, [3]) для вирішення завдання збору інформації про зв'язки вузлів в ІТКМ не ефективні, 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 і облікові записи). У зв'язку з цим, необхідно постійно отримувати актуальну інформацію про ІТКМ для більш точного моделювання ЗРЗІ.

Топологія мережі представляється 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 більш ніж одним ребром. Для спрощення досліджень граф вважається не зваженим, тобто сила інформаційних зв'язків [27] не відображається на ваги відповідних ребер. Вузол є людино-машинною системою, на одному комп'ютері не може перебувати декілька вузлів.

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

Методика формування топології ІТКМ складається з послідовності кроків[2]:

- збір даних про топологію доступній частині мережі;

- формування повного графа мережі з урахуванням до давання недоступної частини на основі обчислених прогнозованих топологічних характеристик (розподіл ступенів зв'язності, середня довжина шляху);
- формування вектора топологічної уразливості вузлів ІТКМ.

3.2. Обслідування мережі

Далі розглянуто розроблений алгоритм формування повного графа мережі [2], який враховує топологічні характеристики доступній частині мережі (розподіл ступенів зв'язності, середня довжина шляху).

Обчислення середнього ступеня зв'язності мережі

Ступінь зв'язності вузла (degree) – кількість суміжних з ним вузлів [2].

Середній ступінь зв'язності мережі (averagedegree) – 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 за відкритими вузлами.

Отримання розподілу ступенів зв'язності вузлів в мережі

Розподіл ступенів зв'язності вузлів – статистична характеристика, що показує кількість вузлів з кожним значенням зв'язності в мережі [19].

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 – характеристика, що показує «щільність» зв'язків навколо вузла [19]. Кластерний коефіцієнт вузла обчислюється як відношення числа існуючих зв'язків між суміжними вузлами до значення загальної кількості можливих таких зв'язків:

$$C_i = \frac{2n_i}{k_i(k_i - 1)}, \qquad (19)$$

деk_i – ступінь зв'язності вузла, n_i – кількість зв'язків між суміжними вузлами.

Розглянемо приклад обчислення кластерного коефіцієнта для вузла1 (рис.3.1). Суцільними лініями показані існуючі зв'язки, пунктирними – потенційні. Ступінь зв'язності k=4. Число можливих зв'язків між його суміжними вузлами одно $k(k–1)/2 = 4(4–1)/2 = 6$. Число існуючих зв'язків – 2. Кластерний коефіцієнт C =2/6 =1/3.

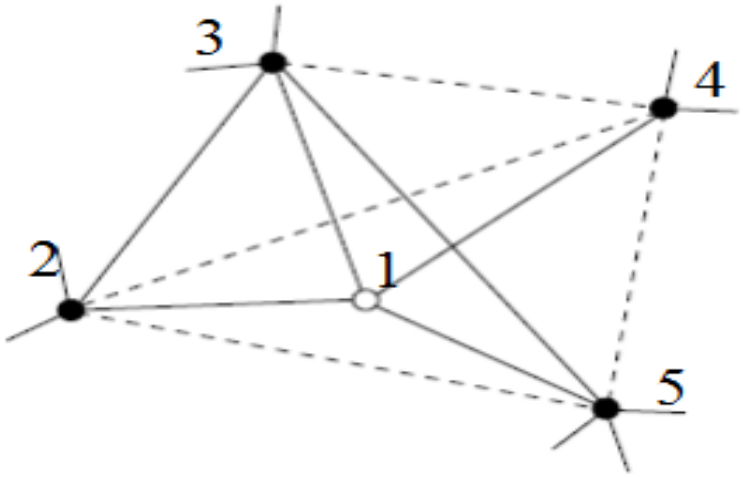


Рис. 3.1. Схематичний малюнок для визначення кластерного коефіцієнта

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, що утворені відкритими та 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, поділеній на їх загальну кількість.

Топологічна уразливість 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:

$$\varphi_i = \frac{k_i (C_i + 1)}{L_i}, \qquad (20)$$

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

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

Накладається умова для застосування останньої формули – в мережі має бути більше одного вузла.

Властивості коефіцієнта φ:

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

Крайній випадок (максимальне значення) – повнозв'язний граф. У ньому $k_i = N-1$ і середня довжина шляху дорівнює одиниці $L_i = 1$.

2) Кластерний коефіцієнт має властивість $0 \le C_i \le 1$ і в повнозв'язкову графі $C_i = 1$. Отже, в цьому випадку $\varphi_i = 2(N-1)$.

3) Зі збільшеннямφ_i зростає вразливістьвузла.

Підрахуноккоефіцієнтатопологічноїуразливостідля всієї мережіздійснюєтьсяза формулою

$$\varphi = \frac{k(C+1)}{L}, \qquad (21)$$

де kдо – середній ступіньзв'язностівузлівв мережі,C– середнійкластернийкоефіцієнтмережі, L – середня довжинашляхумережі.

При дослідженні топологій реальних великомасштабних ІТКМ слід виділити і використовувати основні значущі положення, які відомі з відкритих джерел:

1) середній 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 вищезгаданого та отриманих експериментальних результатів, маємо типове значення коефіцієнта топологічної уразливості у діапазоні від 100 до 500.

Практичне застосування

1) Використовуючи коефіцієнт φ, можна оцінити топологічну вразливість конкретної реальної мережі за останньою, тобто

$$\varphi = \frac{k(C+1)}{L}, \qquad (22)$$

У ході роботи були проаналізовані соціальні мережі Facebook і «ВКонтакте». Для мережі Facebook$\varphi \approx 70$, «ВКонтакте» – $\varphi = 200$. Для мережі Facebook отримали не зовсім типове значення, пов'язано це з методом вибірки, застосованої американськими дослідниками [19], а також тим, що дана мережа найбільша і, дійсно, в цілому менш вразлива, ніж мережа «ВКонтакте». Далі топологічна уразливість φ використовувалася для створення аналітичної моделі розповсюдження забороненої інформації як інтегральна складова топологічних параметрів мережі.

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

Таблиця 3.1

Вектор топологічної уразливості вузлів ІТКМ – вектор виду:

№ вузла	Значення φ
Вузол 1	φ_1
…	…
Вузол N	φ_N

Отриманий вектор можна використовувати при прогнозування і загрози розповсюдження забороненої інформації. На такому прогнозуванні може базуватися подальша стратегія забезпечення захисту, яка може використовувати з одного боку,класифікацію занебезпекоюатакуючівузли, аз іншого боку, вибудувати найбільш ефективну стратегіюпротидії загрозі.

3.3 Аналіз результатів експериментальних досліджень

Моделювання ЗРЗІ на великомасштабній ІТКМ є трудомістким завданням. Її рішення в прийнятні терміни і отримання актуальних результатів можливо тільки при використанні розподілених обчислювальних ресурсів.

Експериментальні дослідження проводилися на двох фрагментах ІТКМ. Перший (фрагмент соціальної мережі «ВКонтакте») отриманий у рамках даної роботи.

Експериментальне дослідження ЗРЗІ в ІТКМ здійснювалося на основі імітаційної моделі, докладно розглянутої у другому розділі роботи.

Імітаційна модель реалізована у вигляді розробленого ПЗ під розподілену обчислювальну систему. Для реалізації паралельних обчислень на графі була використана бібліотека ParallelBoostGraphLibrary [31].

Бібліотека розповсюджується вільно і за своїми функціональними можливостями не має альтернатив.

ParallelBoostGraphLibrary (PBGL) надає гнучку та ефективну реалізацію концепції графів. Входить до зібрання бібліотек boost, розширюють функціональність C++, які вільно поширюються за ліцензією BoostSoftwareLicense разом з вихідним кодом.

Бібліотекадозволяє вибратиуявленняграфа,тип даних іалгоритмз великого наборуалгоритмів.

Тут представлені результати моделювання моделювання ЗРЗІ в ІТКМ.

Запропонований алгоритм розподіленого моделювання був апробований на двох представлених вище топологічних фрагментах мереж після застосування до нихалгоритму формування повного графа мережі. Експерименти проводилисяз різними початковими умовами. Спочатку було проаналізовано вплив параметрів βіγ на характер процесу,результати експериментів наведені на рис. 3.2 та 3.3(«ВКонтакте»).

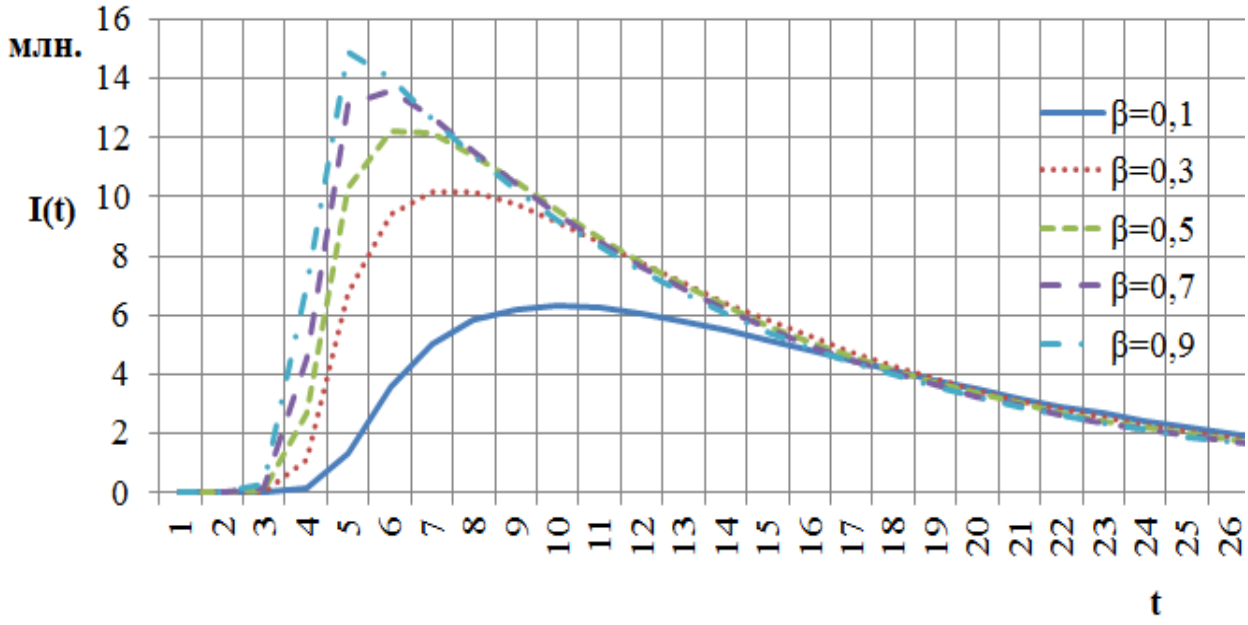


Рис. 3.2. Результати моделювання з параметрами γ = 0,1, I_0= 1, R_0= 0

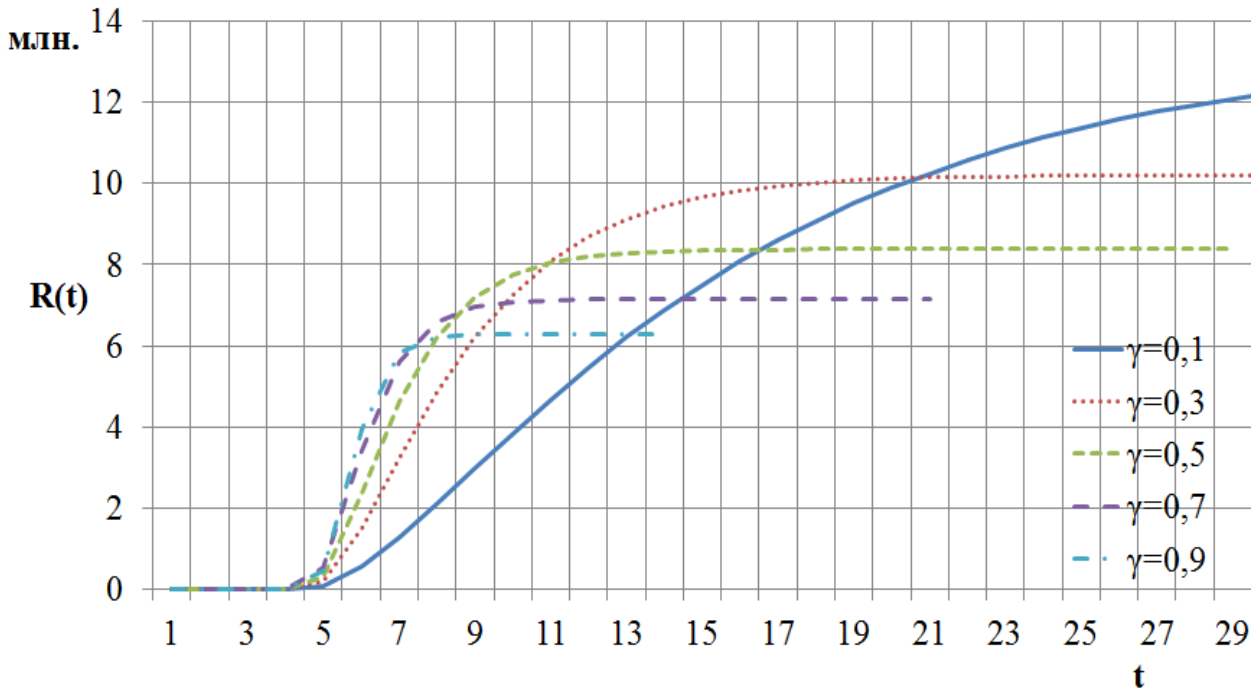


Рис. 3.3. Результати моделювання з параметрами β= 0,2, I_0= 1, R_0= 0

У ході роботи раніше була розглянута аналітична модель ЗРЗІ в ІТКМ. В рамках даної моделі передбачені два випадки: $\beta \neq \gamma$ і $\beta = \gamma$. Тому при моделюванні використовувалися такі окремі випадки: β = 0,2 і γ = 0,8, β = 0,5 і γ = 0,5. Кількість початково атакуючих вузлів I_0 розглядалося виходячи з того факту, що це може бути одна людина або декілька. В якості декількох розповсюджувачів вибиралося порядку 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.

За допомогою MatLAB отримані розв'язки останньої системи диференціальних рівнянь, тобто розподіли величин $I(t)$ та $R(t)$ за часом. Ці

розподіли показують динаміку зміни кількості вузлів мережі, які захищені та є джерелами загроз (додаток В).

Графіки результатів проведеного моделювання поширення забороненої інформації на топологічному фрагменті соціальної мережі «ВКонтакте» наведено на рис. 3.4-3.6.

Експеримент 1 (рис. 3.5): φ= 200, β= 0,2, γ= 0,8, I_0 = 1, R_0 = 0.

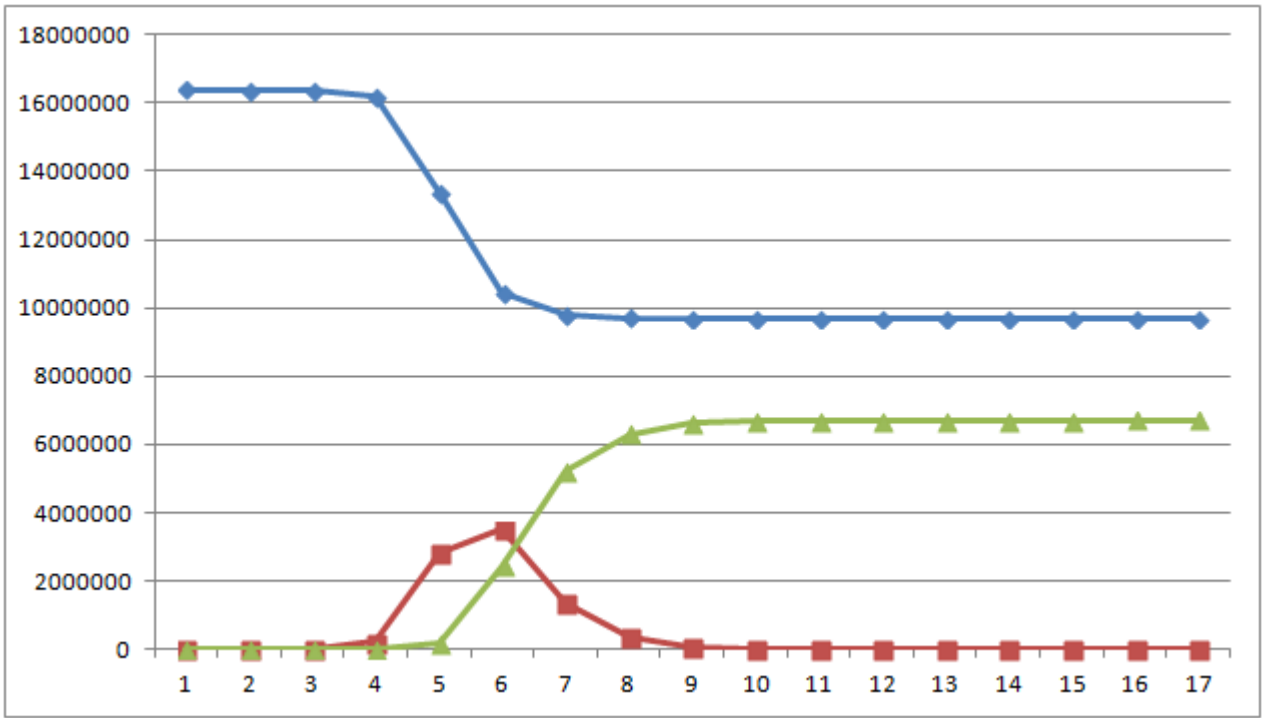


Рис. 3.4. Результати експерименту 1

Експеримент 2 (рис. 3.5): φ= 200, β= 0,2, γ= 0,8, I_0 = 1, R_0 = 0,25 N.

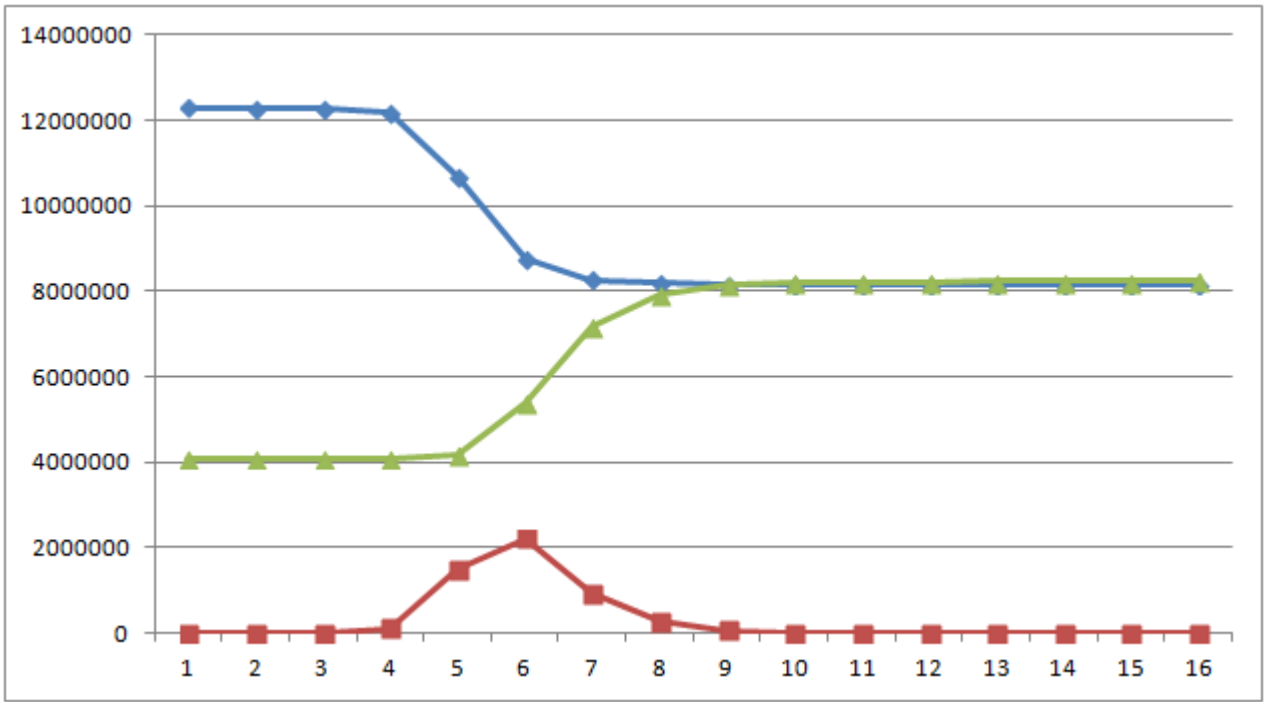


Рис. 3.5. Результати експерименту 2

Експеримент 3 (рис. 3.6): φ= 200, β= 0,2, γ= 0,8, I_0 = 1, R_0 = 0,75N.

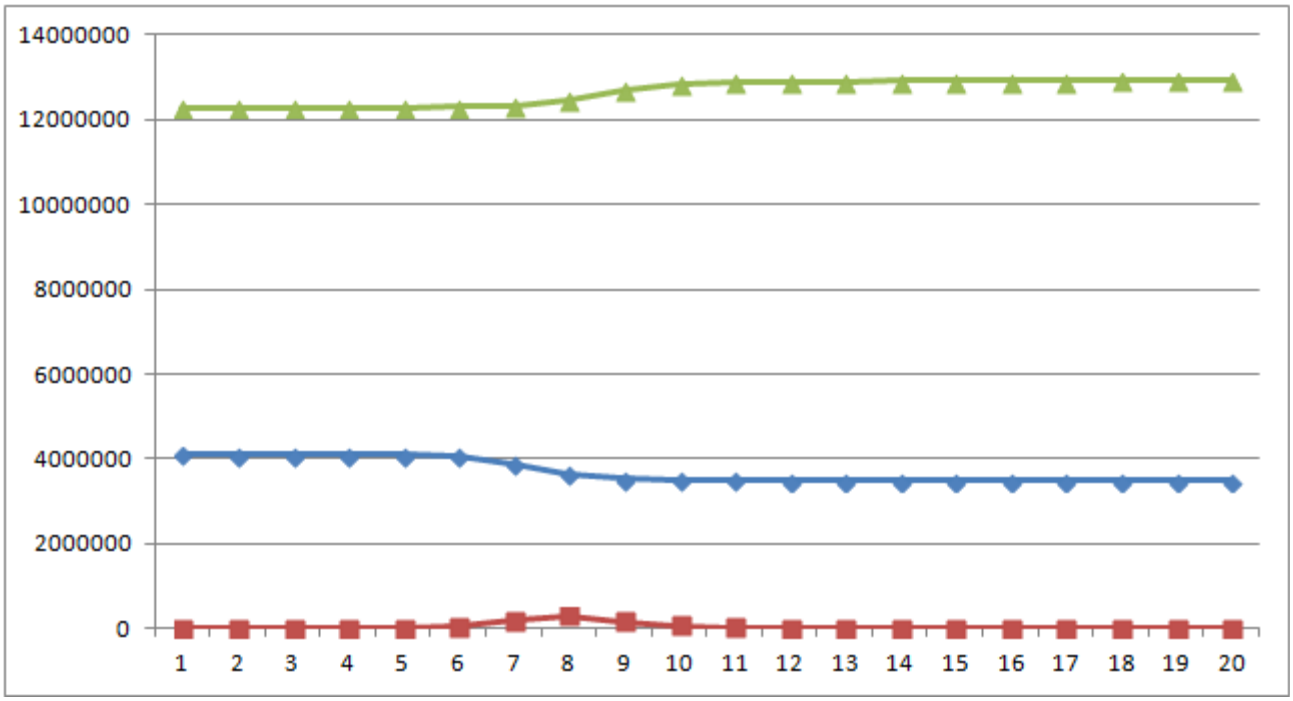


Рис. 3.6. Результати експерименту 3

За результатами даних експериментів можна зробити наступні висновки:

1) Уже один атакуючий вузол може визвати «спалах» в мережі, навіть при великому значенні імовірності захисту.

2) З ростом числа початково захищених вузлів, максимальне число атакуючих вузлів зменшується.

3) При зростаннічислапочатковоатакуючихвузлівспостерігається «спалах» вже на перших етапах.

3.4. Методика створення системи протидії ЗРЗІ за результатами моделювання

3.4.1. Система протидії ЗРЗІ

Сучасні загрози створюються таким чином, щоб обійти захист. Боротися з ними складно, так як вони розроблені професіоналами, які переслідують конкретні цілі, і, як правило, вже не виявляються за допомогою сигнатур. Розробники досліджують середу, в яку збираються вторгнутися, наявні в ній засоби захисту, і тут не допоможуть навіть «пісочниці», так як вони вміють їх обходити. Розробка шкідливого ПЗ виконується з дотриманням усіх стандартів і технологій, що використовуються при створенні комерційних продуктів, до технічного завдання, робочим проектом, тестуванням, підтримкою і оновленням. При цьому хакерами для тестування використовуються і хмарні технології. Сучасне шкідливе ПЗ є багатокомпонентним, і кожна компонента сама по собі не є небезпечною. У якийсь момент компоненти збираються разом, і тоді слідує повноцінна атака.

Які ж методи можуть бути використані для побудови дієвого захисту? Класичні полягають у тому, щоб застосовувати брандмауери, IDS/IPS і інші методи. У той же час, можна використовувати самі передові засоби захисту, але вони не допоможуть, якщо не реалізовані належні процедури та політики. Більшість компаній прагнуть приховати факти проникнень, боячись репутаційних ризиків. Однак при такому підході ймовірність успішних атак

на інші компанії зростає, тому набагато корисніше для всіх обмінюватися такою інформацією.

Методика захисту від вторгнень повинна включати наступне: найбільш повно знати про ситуацію, яка передувала атаці, виявити і максимально блокувати атаку в її ході та проаналізувати, як це все відбувалося, після атаки. Як можна цього досягти? Йдеться про показники, що дозволяють визначити компрометацію, наприклад, про репутацію джерела трафіку, про певні характеристики трафіку, що вказують на можливість атаки, його відхилення від звичайного поведінки і т.д. Потрібно збирати інформацію про показники компрометації з інших джерел і проводити їх аналіз. Для захисту в ході атаки не можна обмежуватися тільки аналізом сигнатур, потрібно використовувати і додаткові методи виявлення, наприклад, фільтри на основі репутації, нечіткі відбитки, виявлення на основі аналізу поведінки. Потрібно також мати повну картину хто і що робить в мережі. Це дозволить зрозуміти, яким чином атака проникла в мережу, які системи є потенційно зараженими, перш ніж вона виконається.

Створення імітаційних моделей ЗРЗІ в ІТКМ, що враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем, дозволяє суттєво зменшити ефективність атак.

Графікирезультатів проведеногомоделювання поширеннязабороненої інформаціїнатопологічномузрізісоціальної мережі Facebookнаведені у [8].Характерпроцесу поширеннязабороненої інформаціїна цій мережітакий же, які на мережі «ВКонтакте».Цей фактвказує на те, що різні соціальні мережімають схожутопологію.

У ході експериментальних досліджень були отримані також результати, що стосуються топології ІКТМ [3].

Нижче у таблиці [2] представлені основні топологічні характеристики для випадкових графів і двох видів складних мереж (complexnetworks), які були розглянуті в першому розділі.

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 3.2

Результати експериментів

Параметр	Випадкові графи	Smallworld	Scale-Free
Средня довжина шляху L	$\frac{\ln k}{\ln N}$	$\frac{\ln k}{\ln N}$	$\frac{\ln N}{\ln \ln N}$
Кластерний коефіцієнт C	$\frac{k}{N}$	$C_{p\to 1} \approx \frac{k}{N}$	$5\frac{k}{N}$
Розподіл степенів вершин	Закон Пуассона	Закон Пуассона	Спеневий закон

За наявності адміністративного ресурсу можна реалізувати автоматизовану систему протидії загрозі поширення забороненої інформації.

Автоматизована система протидії загрозі поширення забороненої інформації може бути реалізована у рамках підсистеми адміністрування.

У великих мережах функції адміністрування можуть бути розподілені між: багатьма адміністраторами. Зокрема, бувають адміністратори баз даних, захисту даних, архівування, електронної пошти та ін.

Головні завдання та групи функцій адміністративної підсистеми такі:

- моніторинг та мережеметрія;
- планування робіт у мережі;
- керування інформаційними потоками та реконфігурування мережі;

- інформаційно-довідкова служба;
- гарантування безпеки даних, контроль за правильністю повноважень, розпізнавання;
- електронна пошта.

Саме реалізація наведених завдань надасть можливість протидії загрозам поширення забороненої інформації.

Узагальнена послідовність кроків при реалізації такої системи подається нижче. Розглянуті функції реалізуються за допомогою типових засобів. Отже, **алгоритм протидії ЗРЗІ** полягає в реалізації наступних функцій.

Ідентифікація забороненої інформації

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

Крок 1. Введення даних – типове повідомлення, що містить інформацію, заборонену до поширення. База даних таких повідомлень формується з списку екстремістських матеріалів та 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.

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

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

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

Попередження

Крок 4а. Складання правил фільтрації повідомлень на основі формального опису. Здійснюється шляхом компіляції регулярних виразів за допомогою засобів, призначених 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 та ін.

Крок 6а. Моделювання загрози розповсюдження забороненої інформації.

Крок 7а. Підвищення пріоритету процесу фільтрації відповідно з результатами моделювання загрози розповсюдження забороненої інформації.

Ліквідація наслідків

Крок 4б. Конструювання ряду пошукових запитів за формальними правилами, і підстроювання параметрів пошуку (пріоритет, глибина і тд.).

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

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

Крок 7б. Відправка повідомлення про проведені заходи в контролюючі органи.

Тепер залишається скористатися зібраною інформацією.

3.4.2. Прогноз

Для прогнозування загроз у сфері інформаційної безпеки є декілька підходів. Зокрема, теорія ритмів вважає, що всі процеси природного, економічного, технологічного та інших характерів підкоряються певним загальним закономірностям.

Ряд авторів пропонують використовувати для прогнозування загроз статистичні методи. Головною перевагою цих методів є адаптація математичних і статистичних апаратів до об'єкта. Статистичні методи

універсальні, оскільки для проведення аналізу не потрібно знання про можливі атаки і використовуваних ними вразливості. Але при використанні цих методів виникає ряд проблем:

• «статистичні» системи не чутливі до порядку проходження подій;

• важко поставити граничні (порогові) значення відслідковуються системою виявлення атак характеристик;

• «статистичні» системи можуть бути з плином часу «навчені» порушниками.

Ще один метод прогнозування – метод експертних оцінок. Це метод доцільно застосовувати в тому випадку, коли відсутні статистичні дані. При цьому експертам пропонується відповісти на питання про стан або майбутній поведінці інформаційних активів, що характеризуються невизначеними параметрами або невивченими властивостями.

Існує три методи прогнозування, заснованих на експертних оцінках:

1. Метод колективної експертної оцінки. В даному випадку відбувається узагальнення результатів роботи групи експертів в області інформаційної безпеки. Для отримання об'єктивного результату необхідно обробити індивідуальні, незалежні оцінки, винесені експертами. Таким чином відбувається різнобічний аналіз проблеми.

2. Метод Делфі експертних оцінок. Даний метод ґрунтується на процесі «мозкового штурму», виробленого групою фахівців. Даний метод застосовується при необхідності швидкого ухвалення рішення. Дельфійський метод використовується для експертного прогнозування шляхом організації системи збору та математичної обробки експертних оцінок.

3. Компетентність експертної групи. В даному випадку відбувається дискусія з питання, з метою знаходження єдино правильного його вирішення. Цей метод відрізняється від попереднього тим, що крім вираження своїх ідей, експерт може також критикувати чужі. Перевагою даного методу є простота реалізації і зменшення ймовірності помилок.

Таким чином, метод колективних оцінок є найбільш універсальним і використовується в магістерській роботі.

Знання експертів формуються в базу даних. База даних допоможе в пошуку аналогічних подій і методів їх вирішення, а також мінімізації втрат. Такий метод прогнозування має багато спільного з прогнозуванням методом аналогій. Головним достоїнством такого прогнозування є відсутність помилкових тривог.

Основним недоліком цього методу є можливість відображення невідомих атак. При цьому навіть невелика зміна вже відомої атаки може стати серйозною проблемою.

Використовуючи розроблену аналітичну модель, можна отримати прогноз по динаміці ЗРЗІ 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 самих великомасштабних 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 та захисту).

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

ВИСНОВКИ ДО РОЗДІЛУ 3

Імітаційна модель ЗРЗІ в ІТКМ, що розглянута в другому розділі, хоча і враховує топологічні характеристики мережі, але залишається проблема урахування конкретних особливостей топології мереж. У третьому розділу розглядаються деякі міркування щодо спрощеної процедури урахування таких особливостей.

Розглянуто розроблений алгоритм формування повного графа мережі, який враховує топологічні характеристики доступній частині мережі (розподіл ступенів зв'язності, середня довжина шляху).

Проведений аналіз результатів експериментальних досліджень.

ВИСНОВКИ

Основним результатом даної роботи є вдосконалена модель загрози розповсюдження забороненої інформації в ІТКМ.

В результаті виконання роботи були отримані наступні результати:

- проведено інформаційний огляд сучасних моделей розповсюдження шкідливої інформації в мережах;
- досліджено множину функцій захисту від забороненої інформації;
- проведено огляд сучасних епідеміологічним моделей;
- проведено експериментальне дослідження обраного варіанту моделі;
- досліджено питання топологічної уразливості ІТКМ;
- сформовано основні принципи протидії та прогнозування ЗРЗІ.

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

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

Використано алгоритм формування вихідних даних про топологію мережі (множини вершин і зв'язків між ними доступною частини мережі).

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамов, К.Г., Монахов, Ю.М., Медведникова, М.А., Трусова, А.И., Бодров, И.Ю. Статистическиепараметрытопологиисоциальныхсетей [Текст] / К.Г. Абрамов [и др.]; Математика и математическоемоделирование. Трудынаучно-практическойконференции, Мордовскийгосударственныйпедагогическийинститутимени М.Е. Евсевьева. – 2011.

2. Абрамов, К.Г., Малышев, Р.В., Монахов, Ю.М. К вопросу о топологических характеристиках социальной сети «ВКОНТАКТЕ» [Текст] / К.Г. Абрамов, Р.В. Малышев, Ю.М. Монахов; Перспективныетехнологии в средствахпередачиинформации: Материалы 10-ой международнойнаучно-технической конференции, Владим. гос. ун-т. – 2013. – т. 2. – С. 115-118.

3. Абрамов, К.Г., Монахов, Ю.М. Моделираспространениявредоносныхпрограмм в топологическигетерогенныхсоциальныхсетях [Электронный ресурс] / К.Г. Абрамов, Ю.М. Монахов; Труды НТС. Комитет по информатизации, связи и телекоммуникациямАдминистрацииВладимирскойобласти. – 2010. – Режим доступа: http://ksi.avo.ru/

4. Антонюк А.А. О функцияхзащитыинформации // Проблемыпрограммирования, 2005, №4, с.51-55.

5. Безруков, Н.Н. Компьютернаявирусология [Текст] / Н.Н. Безруков; – К.:Укр. сов. энцик., 1991. – 416 с.

6. Биячуев, Т.А. Безопасностькорпоративныхсетей [Текст]: учеб. пособие / Т.А. Биячуев; под ред. Осовецкого Л.Г. – СПб.: СПбГУ ИТМО, 2004. – 161 с.

7. Брэгг, Р., Родс-Оусли, М., Страссберг, К. Безопасностьсетей. Полноеруководство [Текст] / Р. Брэгг, М. Родс-Оусли, К. Страссберг; – М.: Эком, 2006. – 912 с.

8. Гошко, С.В. Энциклопедия по защите от вирусов [Текст] / С.В.

Гошко; – М.: СОЛОН-Р, 2005. – 352 с.

9. Груздева, Л.М., Абрамов, К.Г., Монахов, Ю.М. Экспериментальноеисследованиекорпоративной сети передачиданных с адаптивнойсистемойзащитыинформации [Текст] / Л.М. Груздева, К.Г. Абрамов, Ю.М. Монахов; Приборостроение. – М., 2012. – Т. 55, № 8. – С. 57-59.

10. Губанов, Д.А., Новиков, Д.А., Чхартишвили, А.Г. Социальные сети: моделиинформационноговлияния, управления и противоборства [Текст] / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили; под ред. чл.-корр. РАН Д.А. Новикова – М.: Издат. физико-математическойлитературы, 2010. – 228 с.; – ISBN 9785-94052-194-5.

11. Гусева, А.И. Технологиямежсетевыхвзаимодействий [Текст] / А.И. Гусева; – М.: Бином, 1997. – 238 с.

12. Касперски, К. Компьютерныевирусы: изнутри и снаружи [Текст] / К. Касперски; – Спб.: «Питер», 2005. – 528 с.

13. Качалин, А.И. Моделированиепроцессараспространениясетевыхчервей для оптимизациизащитыкорпоративной сети [Текст] / А.И. Качалин; Искусственныйинтеллект, № 2. – 2006. – С. 84-88.

14. Лукацкий, А. Обнаружение атак [Текст] / А. Лукацкий; – СПб.: БХВ-Петербург, 2001. – 624 с.

15. Столлингс, В. Основызащитысетей. Приложения и стандарты [Текст] / В. Столлингс; – М.: Издательскийдом «Вильямс», 2002. – 432 с.

16. Чипига, А.Ф., Пелешенко В.С. Формализация процедур обнаружения и предотвращениясетевых атак [Электронный ресурс] / А.Ф. Чипига, В.С. Пелешенко; Режим доступа: http://www.contrterror.tsure.ru/site/magazine8/05-17-Chipiga.htm

17. Andersson, H., Britton, T. StochasticEpidemicModelsandTheirStatisticalAnalysis [Text] / H. Andersson, T. Britton; LectureNotesinStatistics. – Springer-Verlag, 2000.

18. Dorogovtsev, S.N., Mendes, J.F.F. Scalingpropertiesof scale-freeevolvingnetworks: continuousapproach [Text] / S.N. Dorogovtsev, J.F.F. Mendes; Phys. Rev., E 63. – 2001.

19. Dorogovtsev, S.N., Mendes, J.F.F. EvolutionofNetworks: FromBiologicalNetworkstothe Internet and WWW [Text] / S.N. Dorogovtsev, J.F.F. Mendes; – Oxford, USA: OxfordUniversityPress, 2003. – 280 p. – ISBN 978-0198515906.

20. Ferrara, E., Fiumara, G., TopologicalfeaturesofOnlineSocialNetworks. CommunicationsonAppliedandIndustrialMathematics [Text] / E. Ferrara, G. Fiumara; – 2011.

21. Gjoka, M., Kurant, M., Butts, C.T., Markopoulou, A. MultigraphSamplingofOnlineSocialNetworks [Text] / M. Gjoka [etal.]; IEEE J. Sel. AreasCommun. onMeasurementof Internet Topologies – 2011.

22. Grimaldi, R. P. DiscreteandCombinatorialMathematics [Text] / R.P. Grimaldi; anappliedintroduction. – 4th edition. – NewYork, 1998.

23. Hofmeyr, S.A., Forrest, S., Somayaji, A. Intrusiondetectionusing sequencesofsystemcalls [Text] / S.A. Hofmeyr, S. Forrest, A. Somayaji; JournalofComputerSecurity. – Amsterdam: IOS Press, 1998. – Vol. 6, no 3. – P. 151-180.

24. Kenah, E., Robins, J. M. Network-based analysisofstochastic SIR epidemicmodelswithrandomandproportionatemixing [Text] / E. Kenah, J. M. Robins;
DepartmentsofEpidemiologyandBiostatisticsHarvardSchoolofPublicHealth. – 2007.

25. Kuperman, M., Abramson, G. Smallworldeffectinandepidemiologicalmodel [Text] / Kuperman M., Abramson G.; PhysicalReviewLetters. – 2001. –Vol.86, no 13.

26. Leveille, J. EpidemicSpreadinginTechnologicalNetworks [Text] / J. Leveille; InformationInfrastructureLaboratory HP LaboratoriesBristol. – 2002. – P. 65-76.

27. Newman, M.E.J. Thespreadofepidemicdiseaseonnetworks [Text] / M.E.J. Newman; PhysicalReview E. – 2002. – P. 16-128.

28. Pastor-Satorras, R., Vespignani, A. Epidemicdynamicsinfinitesize scale-freenetworks [Text] / R. Pastor-Satorras, A. Vespignani; Phys. Rev. E. – 2002.

29. Roberts, M.G., Heesterbeek, JAP Mathematicalmodelsinepidemiology [Text] / M.G. Roberts, Heesterbeek JAP; In JA. Filar (Ed.) MathematicalModels. Oxford: EOLSS PublishersLtd, 2004.

30. Volz, E. SIR dynamicsinrandomnetworkswithheterogeneousconnectivity [Text] / E. Volz; JournalofMathematicalBiologymanuscript. – 2007.

31. Williamson, M.M., Léveillé, J. Anepidemiologicalmodelofvirusspreadandcleanup [Text] / M.M. Williamson, J. Léveillé; InformationInfrastructureLaboratory HP LaboratoriesBristol HPL. – 2003.

Додаток А

Формули та фрагмент коду для розрахунків на MatLab

Вихідна система

$$\begin{cases} \dfrac{dI}{dt} = (0{,}0072\varphi + 8{,}48)\beta \dfrac{S(t)I(t)}{N} - \gamma I(t), \\ \dfrac{dR}{dt} = \gamma I(t), \\ \dfrac{dS}{dt} = -(0{,}0072\varphi + 8{,}48)\beta \dfrac{S(t)I(t)}{N}. \end{cases}$$

$$I(0) = 1,\ R(0) = 0,\ S(0) = 104,\ 0 \le t \le 20,$$

$$N = 105,\ \varphi = 150,\ \beta = 0.5,\ \gamma = 0.51.$$

Модернізована система

$$\begin{cases} \dfrac{dx_1}{dt} = (0{,}0072\varphi + 8{,}48)\beta \dfrac{x_1(t)x_3(t)}{N} - \gamma x_1(t), \\ \dfrac{dx_2}{dt} = \gamma x_1(t), \\ \dfrac{dx_3}{dt} = -(0{,}0072\varphi + 8{,}48)\beta \dfrac{x_1(t)x_3(t)}{N}. \end{cases}$$

$$x_1(0) = 1,\ x_2(0) = 0,\ x_3(0) = 104,\ 0 \le t \le 20,$$

$$N = 105,\ \varphi = 150,\ \beta = 0.5,\ \gamma = 0.51.$$

Код для MatLab

```
function F = fun(t,x)

F = [((0.0072*FI+8.48)*BET/N)*X(1)*X(3)-GAM*X(1); GAM*X(1);

(-(0.0072*FI+8.48)*BET/N)*X(1)*X(3)];


T0 = 0, T1 = 20, FI = 150, BET = 0.5, GAM = 0.51, N = 105, X0 = [1;0;104];

[t,X] = ode23('fun',[T0 T1],X0);
```

Додаток Б

Результати імітаційного моделювання

t	$Y*10^{-6}$	$Z*10^{-6}$	$I*10^{-6}$	$R*10^{-6}$
0	0	0	10^{-6}	0
1	0	0	10^{-6}	0
2	0,1	0	0,5	0
3	2,0	0,1	2,0	0,1
4	8,0	3,0	8,0	0,2
5	7,0	5,0	3,0	2,0
6	6,0	7,0	0,1	10,0
7	4,5	8,0	0	11,0
8	2,5	10,0	0	11,2
9	1,0	12,0	0	11,5
10	0,6	12,5	0	12,0
11	0,45	12,8	0	12,0
12	0,3	13,0	0	12,0
13	0,25	13,0	0	12,0
14	0,05	13,0	0	12,0
15	0	13,0	0	12,0
16	0	13,0	0	12,0

Результати імітаційного моделювання та аналітичного розв'язку для β = 0,5, γ = 0,51, R_0 = 0, I_0 = 1.

t	$Y*10^{-6}$	$Z*10^{-6}$	$I*10^{-6}$	$R*10^{-6}$
0	0	0	0,024	0
1	2,0	0,2	0,5	0
2	3,5	2,0	3,5	0,2
3	2,0	4,1	0,3	2,1
4	1,0	6,0	0,2	5,2
5	0,5	7,0	0,1	7,0
6	0,2	7,1	0,1	7,0
7	0,1	7,2	0	7,0
8	0,05	7,2	0	7,0
9	0	7,2	0	7,0
10	0	7,2	0	7,0
11	0	7,2	0	7,0
12	0	7,2	0	7,0
13	0	7,2	0	7,0
14	0	7,2	0	7,0
15	0	7,2	0	7,0
16	0	7,2	0	7,0

Результати імітаційного моделювання та аналітичного розв'язку для β = 0,5, γ = 0,51, $R_0 = 0$, $I_0 \approx 24000$.

t	$Y*10^{-6}$	$Z*10^{-6}$	$I*10^{-6}$	$R*10^{-6}$
0	0	4,0	10^{-6}	4,0
1	0	4,0	0,1	4,0
2	0,2	4,0	0,2	4,0
3	2,5	4,1	2,0	4,1
4	5,0	4,5	5,0	4,5
5	4,5	7,0	0,1	7,0
6	3,5	8,0	0,1	12,0
7	2,5	10,0	0	12,2
8	1,0	11,5	0	12,5
9	0,5	12,0	0	12,5
10	0,2	12,4	0	12,5
11	0,15	12,4	0	12,5
12	0,1	12,4	0	12,5
13	0	12,4	0	12,5
14	0	12,4	0	12,5
15	0	12,4	0	12,5
16	0	12,4	0	12,5

Результати імітаційного моделювання та аналітичного розв'язку для β = 0,5, γ = 0,51, $R_0 \approx 4*10^6$,I_0 = 1.

Додаток В

Результати імітаційного моделювання

	φ= 200, β= 0,2, γ= 0,8, $\times 10^{-6}$								
t	I_0 = 1, R_0 = 0			I_0 = 1, R_0 = 0,25 N			I_0 = 1, R_0 = 0,75N		
	ПУВ	АВ	ЗВ	ПУВ	АВ	ЗВ	ПУВ	АВ	ЗВ
1	16,2	0,1	0,1	12,2	0,1	4,1	4,0	0	12,3
2	16,1	0,1	0,1	12,2	0,1	4,1	4,0	0	12,3
3	16,1	0,5	0,2	12,2	0,1	4,1	4,0	0	12,3
4	16,0	0,8	0,5	12,1	0,2	4,2	4,0	0	12,3
5	13,3	2,8	0,6	10,7	1,5	4,3	4,0	0,1	12,3
6	10,2	3,3	2,3	8,8	2,0	5,2	4,0	3,3	12,4
7	9,9	1,2	5,2	8,2	1,0	7,2	3,9	1,2	12,4
8	9,8	0,4	6,1	8,1	0,2	7,9	3,8	0,4	12,5
9	9,8	0,1	6,3	8,1	0,1	8,1	3,6	0,1	12,7
10	9,8	0	6,3	8,1	0	8,1	3,6	0	12,8
11	9,8	0	6,3	8,1	0	8,1	3,6	0	12,8
12	9,8	0	6,3	8,1	0	8,1	3,6	0	12,8
13	9,8	0	6,3	8,1	0	8,1	3,6	0	12,8
14	9,8	0	6,3	8,1	0	8,1	3,6	0	12,8

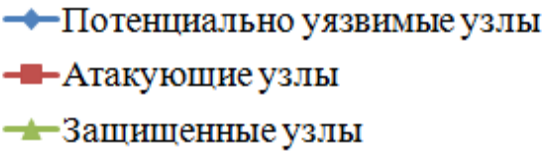
ПУВ – потенційно уразливі вузли;

АВ – атакуючі вузли;

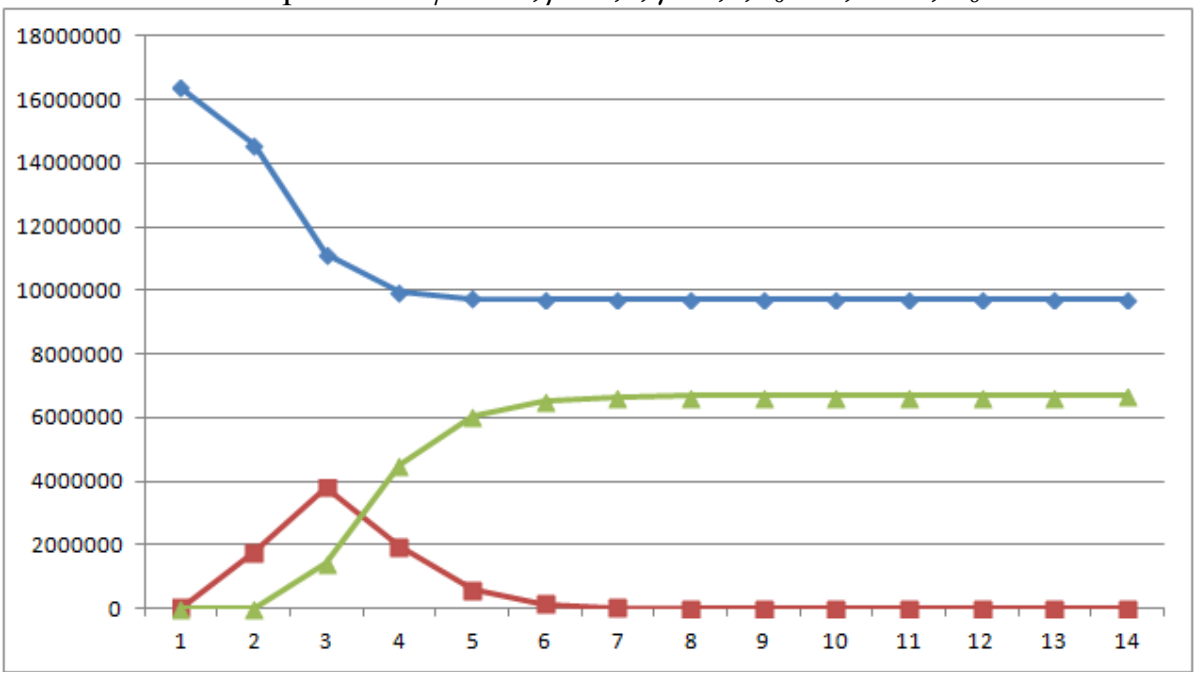
ЗВ – захищені вузли.

Додаток Г

Результати імітаційного моделювання з [3]

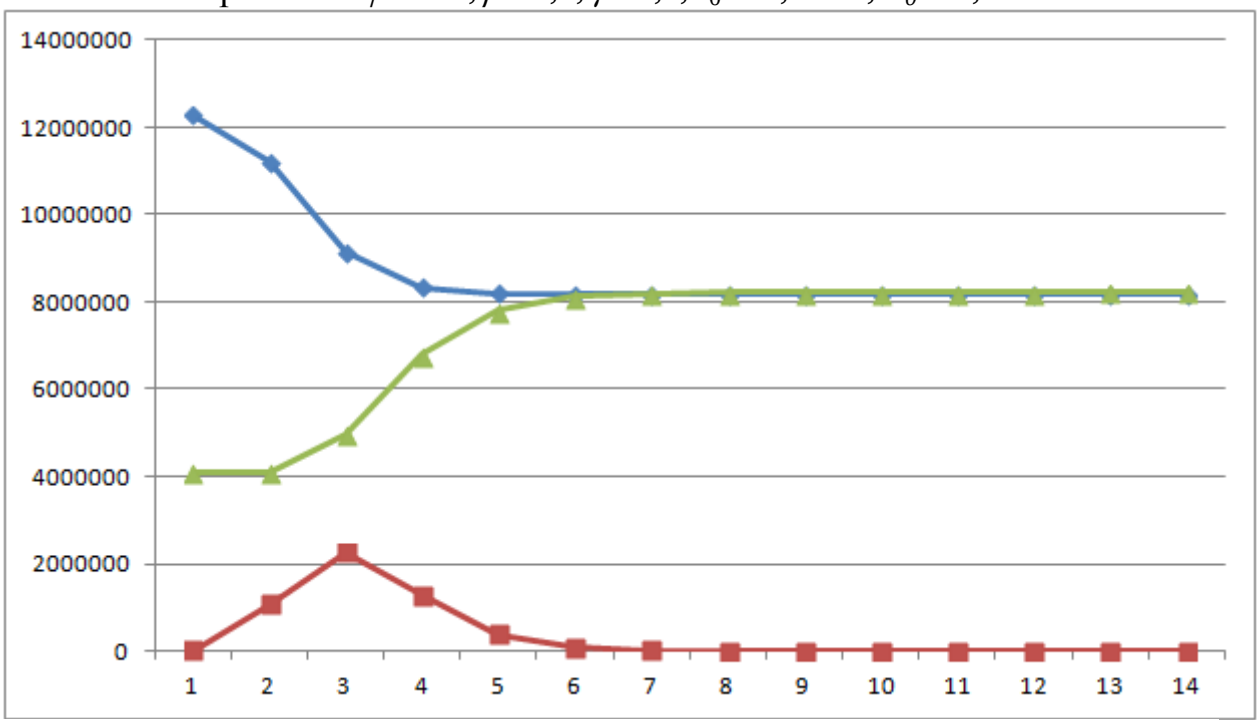


Експеримент 4: φ= 200, β= 0,2, γ= 0,8, I_0 = 0,001N, R_0 = 0.



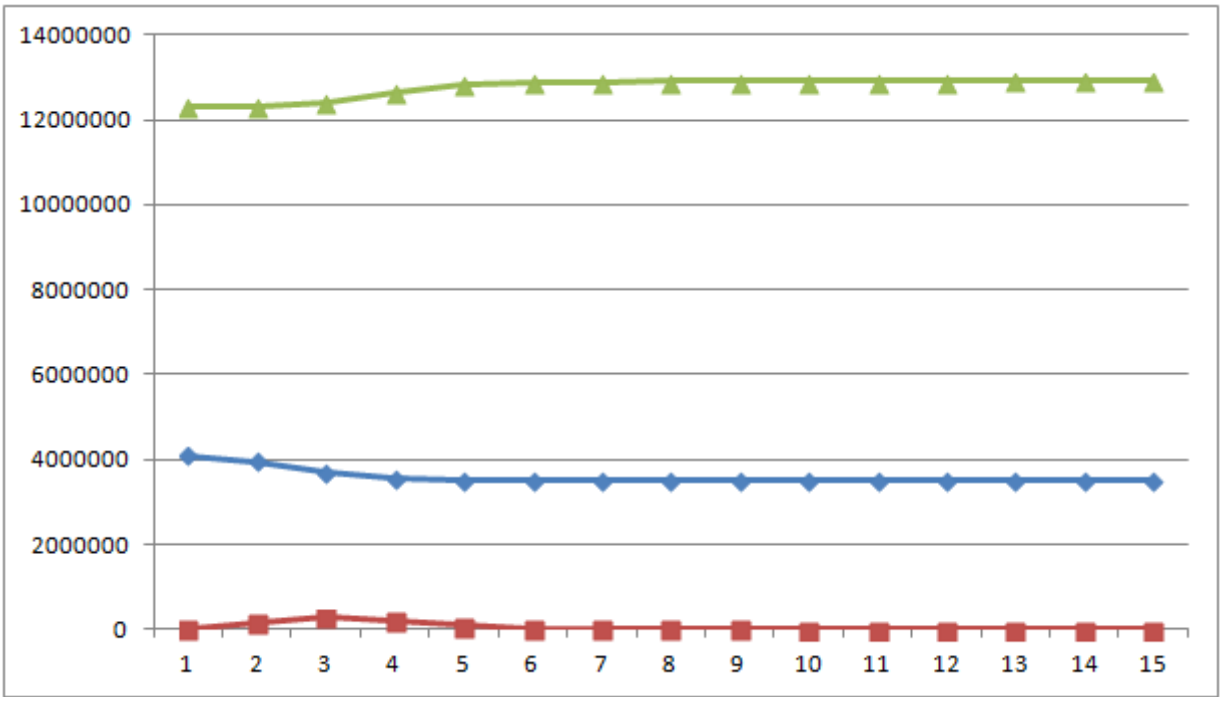
Результати експерименту 4

Експеримент 5: φ= 200, β= 0,2, γ= 0,8, I_0 = 0,001N, R_0 = 0,25N.



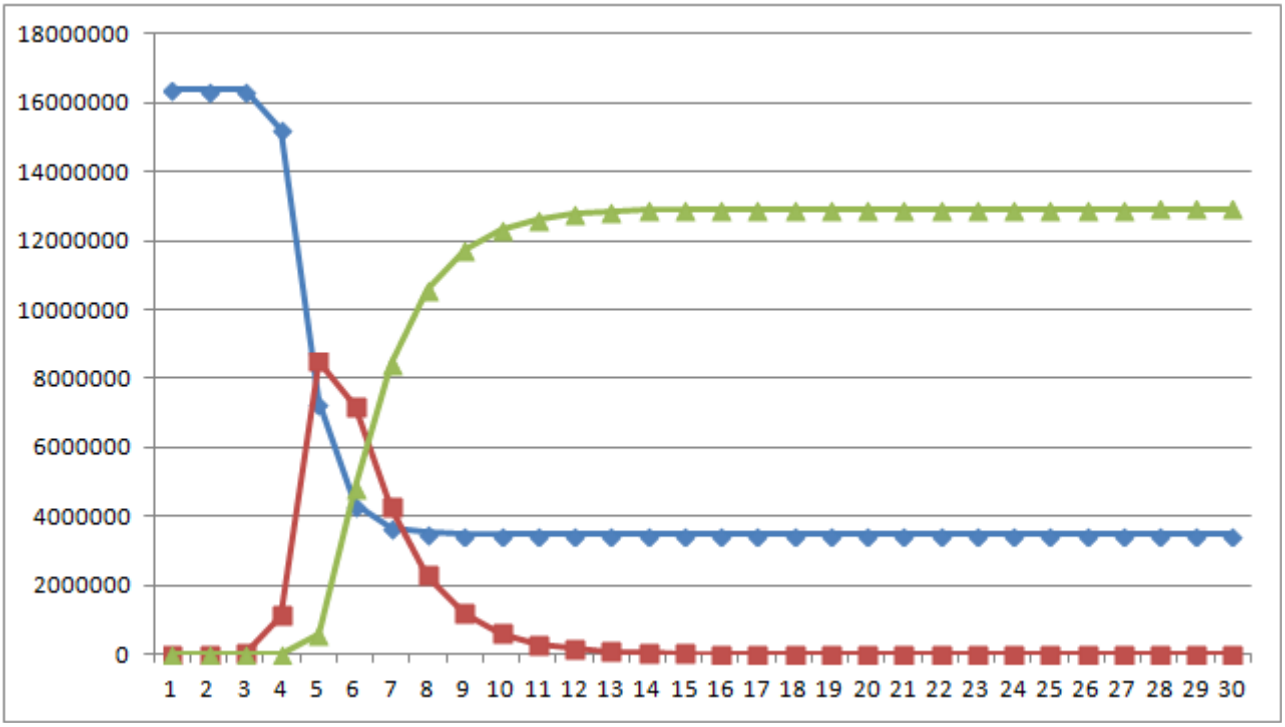
Результатыэксперименту 5

Експеримент 6: φ= 200, β= 0,2, γ= 0,8, I_0 = 0,001N, R_0 = 0,75N.



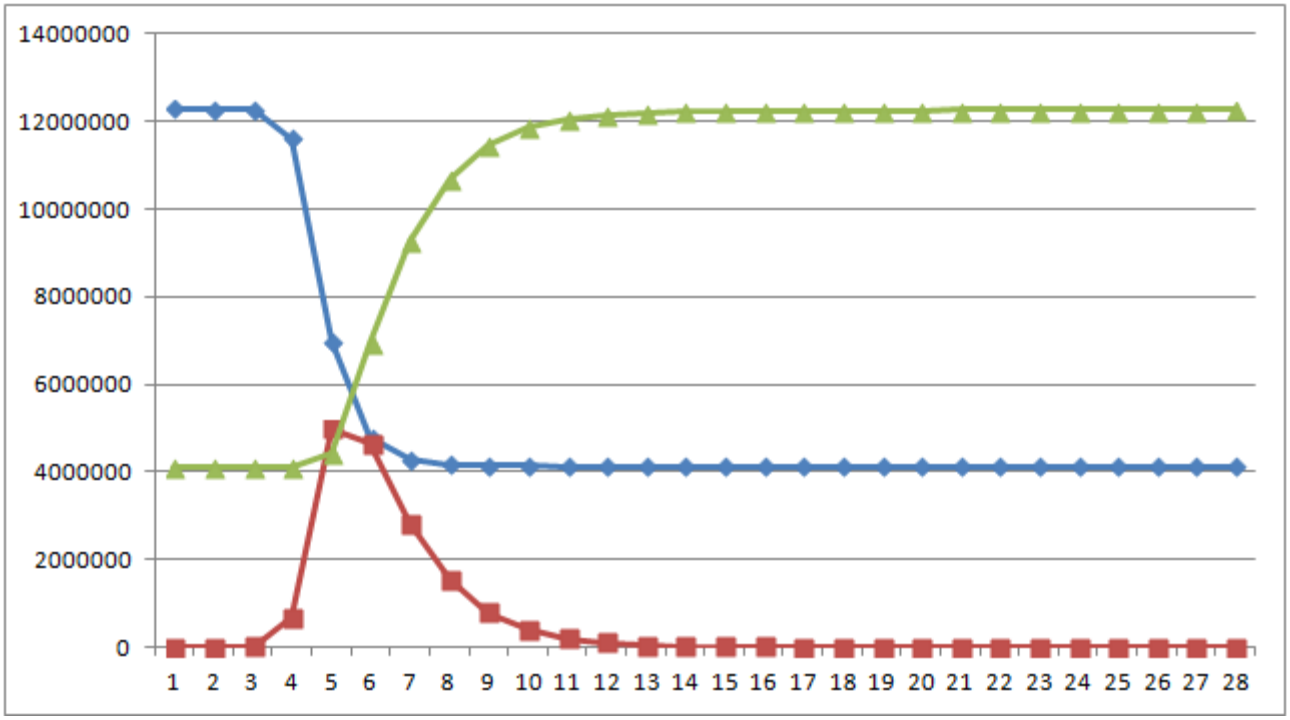
Результати експерименту 6

Експеримент 7: φ= 200, β= 0,5, γ= 0,5, I_0 = 1, R_0 = 0.



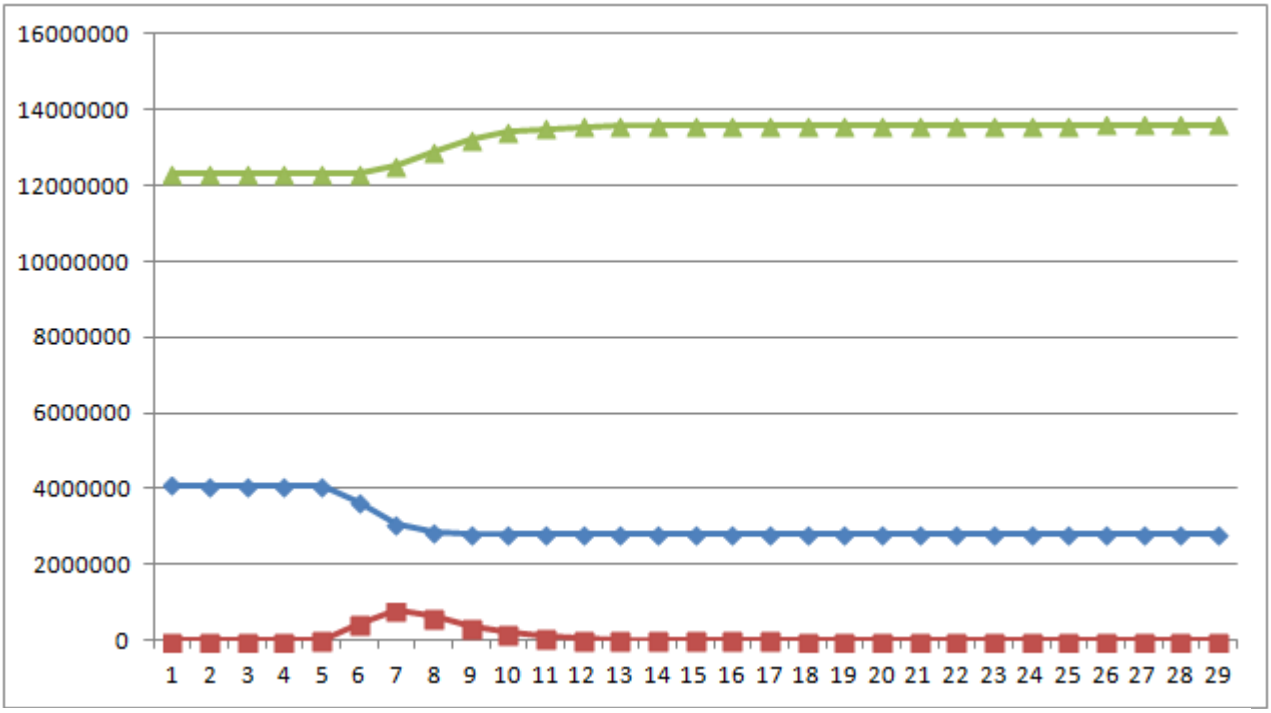
Результати експерименту 7

Експеримент 8: φ= 200, β= 0,5, γ= 0,5, I_0 = 1, R_0 = 0,25N.



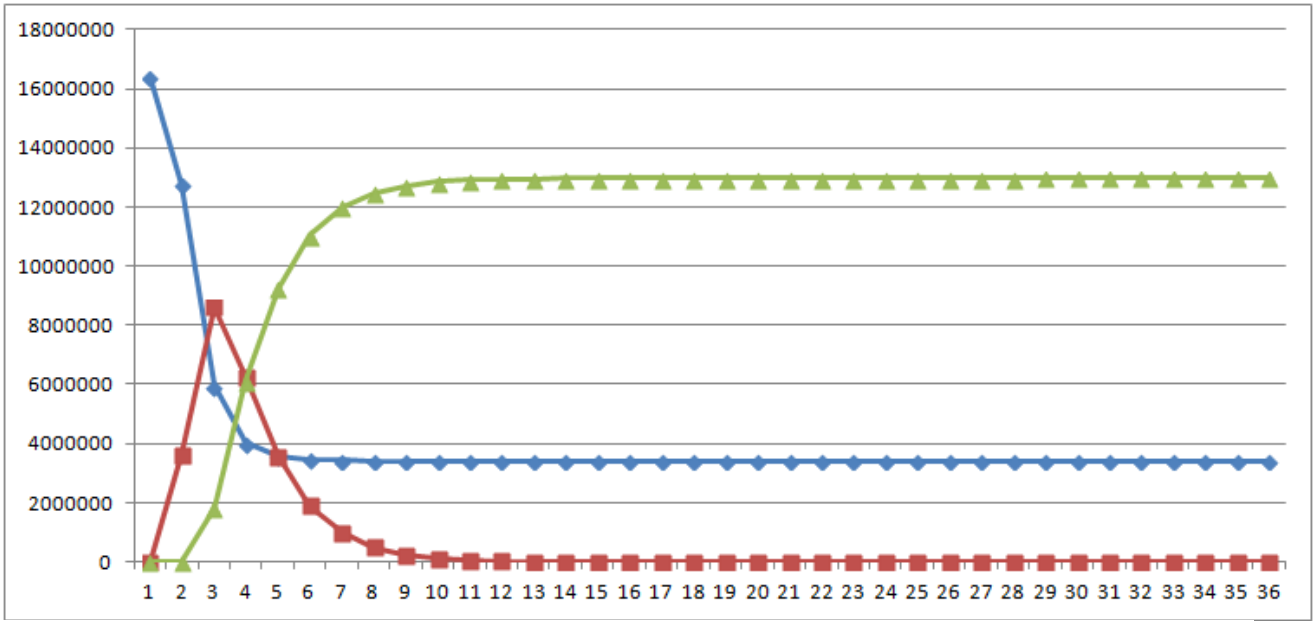
Результати експерименту 8

Експеримент 9: φ= 200, β= 0,5, γ= 0,5, I_0 = 1, R_0 = 0,75N.



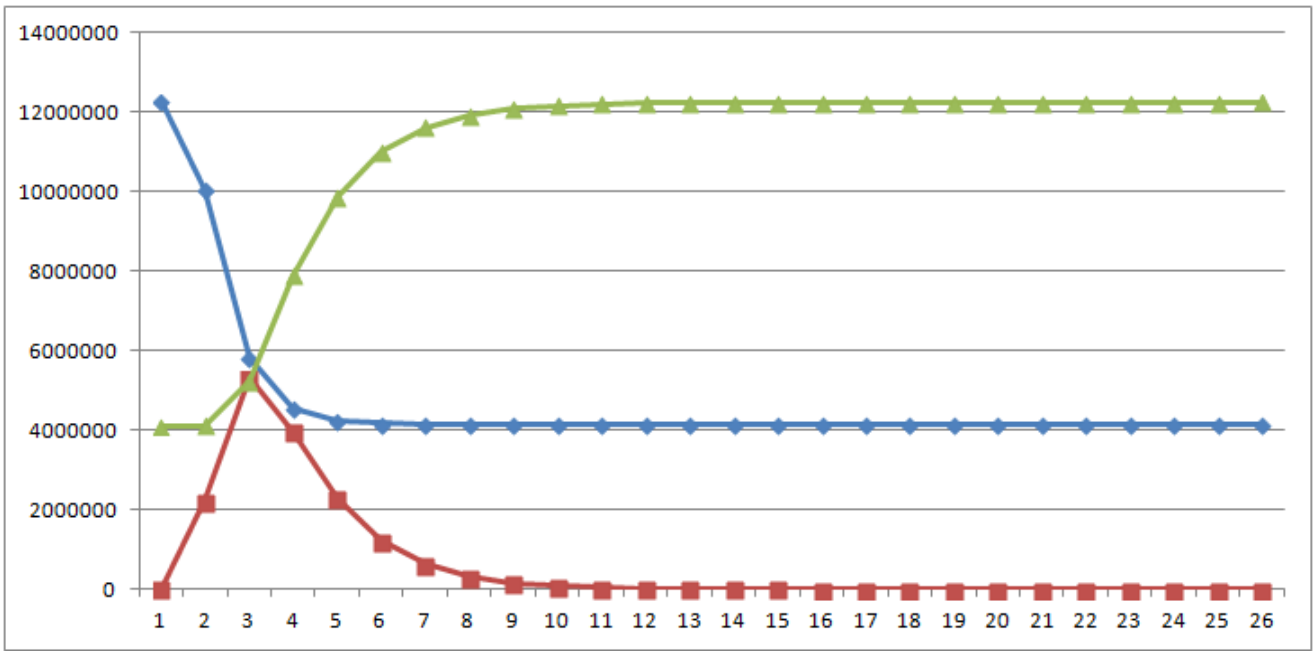
Результати експерименту 9

Експеримент 10: φ= 200, β= 0,5, γ= 0,5, I_0 = 0,001N, R_0 = 0.



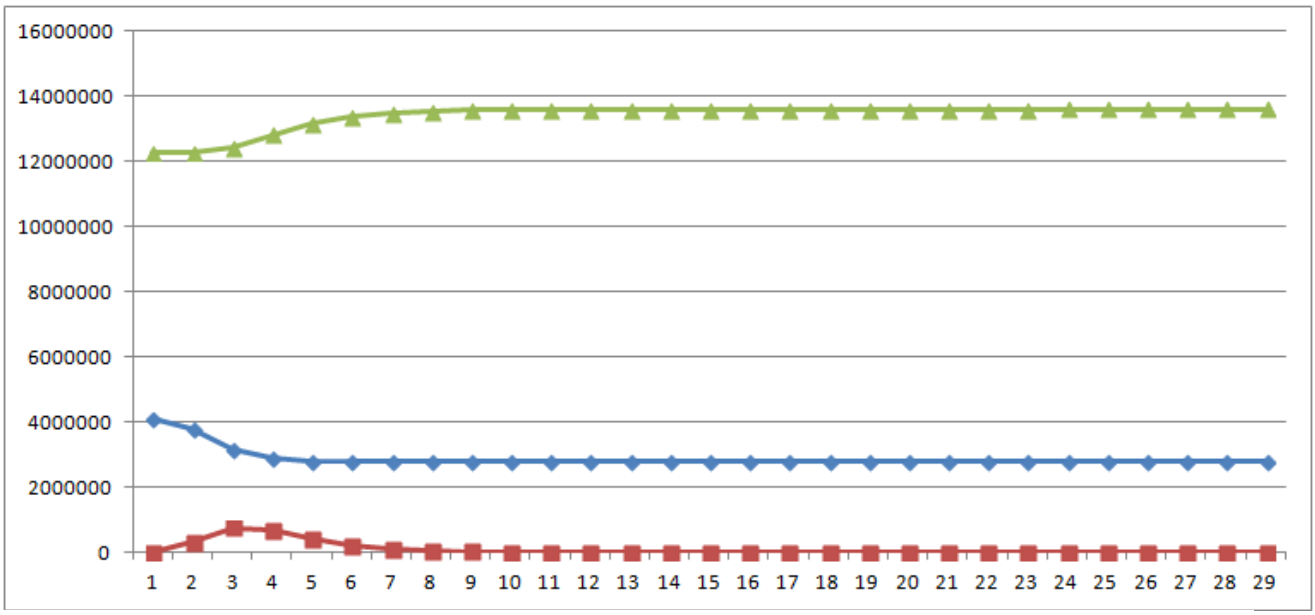
Результати експерименту 10

Експеримент 11: φ= 200, β= 0,5, γ= 0,5, I_0 = 0,001N, R_0 = 0,25N.



Результати експерименту 11

Експеримент 12: φ= 200, β= 0,5, γ= 0,5, I_0 = 0,001N, R_0 = 0,75N.



Результати експерименту 12