**Міністерство освіти і науки України**
**Київський Національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## Дипломної роботи

***магістра***
(назва освітньо-кваліфікаційного рівня)

**галузь знань** *12 Інформаційні технології*
(шифр і назва галузі знань)

**спеціальність** *125 Кібербезпека*
(код і назва спеціальності)

**освітній рівень** ***магістр***
(назва освітнього рівня)

**кваліфікація**
(код і назва кваліфікації)

**На тему:** *Удосконалений метод визначення захищеності персональних даних від довіри в соціальних мережах*

**Виконавець: студент** _____ **курсу, групи** ***КБМ-21***

_____ ***Пісковий Павло Сергійович***
(підпис) (прізвище ім'я по-батькові)

| | **Прізвище, ініціали** | **Оцінка** | **Підпис** |
|---|---|---|---|
| **Науковий керівник** | Лаптєв О.А. | | |
| **Рецензент** | | | |
| **Нормоконтроль** | | | |

**Київ 2022**

**Міністерство освіти і науки України**
**Київський Національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
кібербезпеки та захисту інформації

_____ Н.В. Лукова-Чуйко

«__» _____2021 року

# ЗАВДАННЯ
## на виконання дипломної роботи

**спеціальності** *125 Кібербезпека*
(код і назва спеціальності)

**студенту** ***КБМ-21*** **Пісковому Павлу Сергійовичу**
(група) (прізвище ім'я по-батькові)

**Тема дипломної роботи** *Удосконалений метод визначення захищеності персональних даних від довіри в соціальних мережах*

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.21

### 2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

**Об'єкт досліджень** *процес захисту інформації в соціальних мережах*

**Предмет досліджень** *методи захисту інформації в соціальних мережах*

**Мета** *Удосконалити метод підвищення рівня захищеності персональних даних в соціальних мережах за рахунок додавання специфіки впливу параметру довіри*

**Вихідні дані для проведення роботи**

## 3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

**Наукова новизна** *концепція захисту інформації в соціальних мережах поєднує теоретичні методи та технологічні підходи щодо захисту інформації з урахування параметру довіри до користувачів*

**Практична цінність** *змога оцінити рівень захищеності інформаційного простору соціальних мереж за допомогою такого параметру системи як довіра до користувачів*

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

## 5. ЕТАПИ ВИКОНАННЯ РОБОТИ

| Найменування етапів робіт | Строки виконання робіт (початок-кінець) |
|---|---|
| Уточнення постановки задачі | 29.10.2021 – 05.11.2021 |
| Аналіз літератури | 06.11.2021 – 01.01.2022 |
| Дослідження наявних методів захисту інформації у соц.мережах | 02.01.2022 – 01.03.2022 |
| Розробка методу посилення рівня безпеки інформації у соц.мережах | 02.03.2022 – 01.04.2022 |
| Визначення переваг розробленої методології | 02.04.2022 – 01.05.2022 |
| Оформлення пояснювальної записки | 02.05.2022 – 15.05.2022 |
| Підготовка до захисту дипломної роботи | 16.05.2022 – 19.05.2022 |

## 6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект**

**Соціальний ефект**

## 7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Лаптєв О.А.
(підпис) (прізвище, ініціали)

Завдання прийняв
до виконання _____ Пісковий П.С.
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

# РЕФЕРАТ

Пояснювальна записка: 54 с., 29 малюнків, 28 формул, 46 джерел.

Об’єкт дослідження: процес захисту інформації в соціальних мережах.

Мета роботи: удосконалити метод підвищення рівня захищеності персональних даних в соціальних мережах за рахунок додавання специфіки впливу параметру довіри.

Методи дослідження: методи математичного моделювання, системного аналізу, математичної статистики, математичних моделей захисту даних у соціальній мережі.

У роботі розкрита тема захисту інформації у соціальних мережах. Досліджені та проаналізовані наявні методи та методики захисту інформації, проведений аналіз актуальних проблем у існуючих методах. На основі виявлених результатів та недоліків пропонується метод посилення рівня безпеки інформації у соціальних мережах за рахунок врахування специфічних параметрів, таких як довіра.Також було проаналізовано ефективніть розробленого методу.

Наукова новизна дослідження полягає у тому, що вперше було розроблено концепцію інтегрованого захисту інформації в соціальних мережах, яка поєднує теоретичні методи, прийоми, моделі та технологічні підходи щодо захисту інформації в соціальних мережах з урахування параметру довіри до користувачів.

Напрямки подальших досліджень: дослідження питань, пов'язаних з розробкою нових і удосконалення вже існуючих методик виявлення загроз інформації або персональних даних у соціальних мережах.

Ключові слова: соціальна мережа, захист інформації, довіра, коефіцієнт довіри.

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

СМ – Соціальна мережа

ІБ – Інформаційна безпека

ІС – Інформаційна система

ПЗ – Програмне забезпечення

DLP – Data Loss Prevention

# ВСТУП

Соціальні мережі дуже популярні в сучасному світі. Мільйони людей використовують різні форми соціальних мереж, оскільки вони дозволяють людям спілкуватися з друзями та сім’єю, а також ділитися приватною інформацією.

Існують численні проблеми з безпекою та конфіденційністю, пов’язані з інформацією, яку надає користувач, особливо коли користувач завантажує особистий вміст, наприклад фотографії, відео та аудіо. Зловмисник може зловмисно використовувати надану інформацію в незаконних цілях. Ризики ще вищі, якщо націлені на дітей.

Загрозою у соціальних мережах може бути все, що ставить під загрозу безпеку облікового запису. Розпочати атаку може бути легко, оскільки багато людей зазвичай видають свою особисту інформацію платформам соціальних мереж. Зловмисники можуть легко збирати ці дані та використовувати їх для отримання вигоди [1].

Тому існує потреба в покращенні методів захисту інформації в соціальних мережах.

Метою дипломної роботи є удосконалення методу підвищення рівня захищеності персональних даних в соціальних мережах за рахунок додавання специфіки впливу параметру довіри.

Для досягнення зазначеної мети дипломної роботи сформульовані наступні завдання:

1. Проаналізувати основні методи і підходи до забезпечення ЗІ в СМ.
2. Розробити математичну модель для оцінки стійкості ІБ в СМ.
3. Удосконалення моделі ЗІ в СМ з урахуванням впливу на систему таких елементів системи, як довіра.
4. Оцінка отриманих теоретичних результатів за допомогою математичного моделювання.

Об’єкт дослідження – процес захисту інформації в соціальних мережах.

Предмет дослідження – методи захисту інформації в соціальних мережах.

При вирішенні поставлених завдань у дипломній роботі були використані: методи математичного моделювання, системного аналізу, математичної статистики, математичних моделей захисту даних у соціальній мережі.

Наукова новизна дослідження полягає у тому, що вперше було розроблено концепцію інтегрованого захисту інформації в соціальних мережах, яка поєднує теоретичні методи, прийоми, моделі та технологічні підходи щодо захисту інформації в соціальних мережах з урахування параметру довіри до користувачів.

Практична цінність роботи полягає в тому, що розроблений метод, дає змогу оцінити рівень захищеності інформаційного простору соціальних мереж за допомогою такого параметру системи як довіра до користувачів.

Основні наукові положення і результати роботи доповідалися та обговорювалися на Міжнародній науково-практичній конференції “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” 2021 (PCSITS).

# РОЗДІЛ 1
# АНАЛІЗ СУЧАСНОГО ПІДХОДУ ДО БЕЗПЕКИ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

## 1.1 *Аналіз інформаційних загроз у соціальних мережах*

Соціальна мережа - соціальна структура, утворена людьми або організаціями, в якій підтримуються соціальні відносини. Вона відображає різноманітні зв'язки між ними через різноманітні соціальні відносини, від випадкових знайомств до тісних родинних зв'язків. Аналіз соціальних мереж перетворився на основний метод досліджень в сучасній соціології, антропології, географії, соціальній психології, інформатиці та дослідженні організацій, а також поширену тему для досліджень та дискусій [2].

Сервіси соціальних мереж (СМ) радикально змінюють людські взаємодії, стаючи фактично домінуючим сервісом в Інтернеті сьогодні (рис. 1.1-1.3).


Рисунок 1.1. Статистика соціальних мереж в Україні [3]

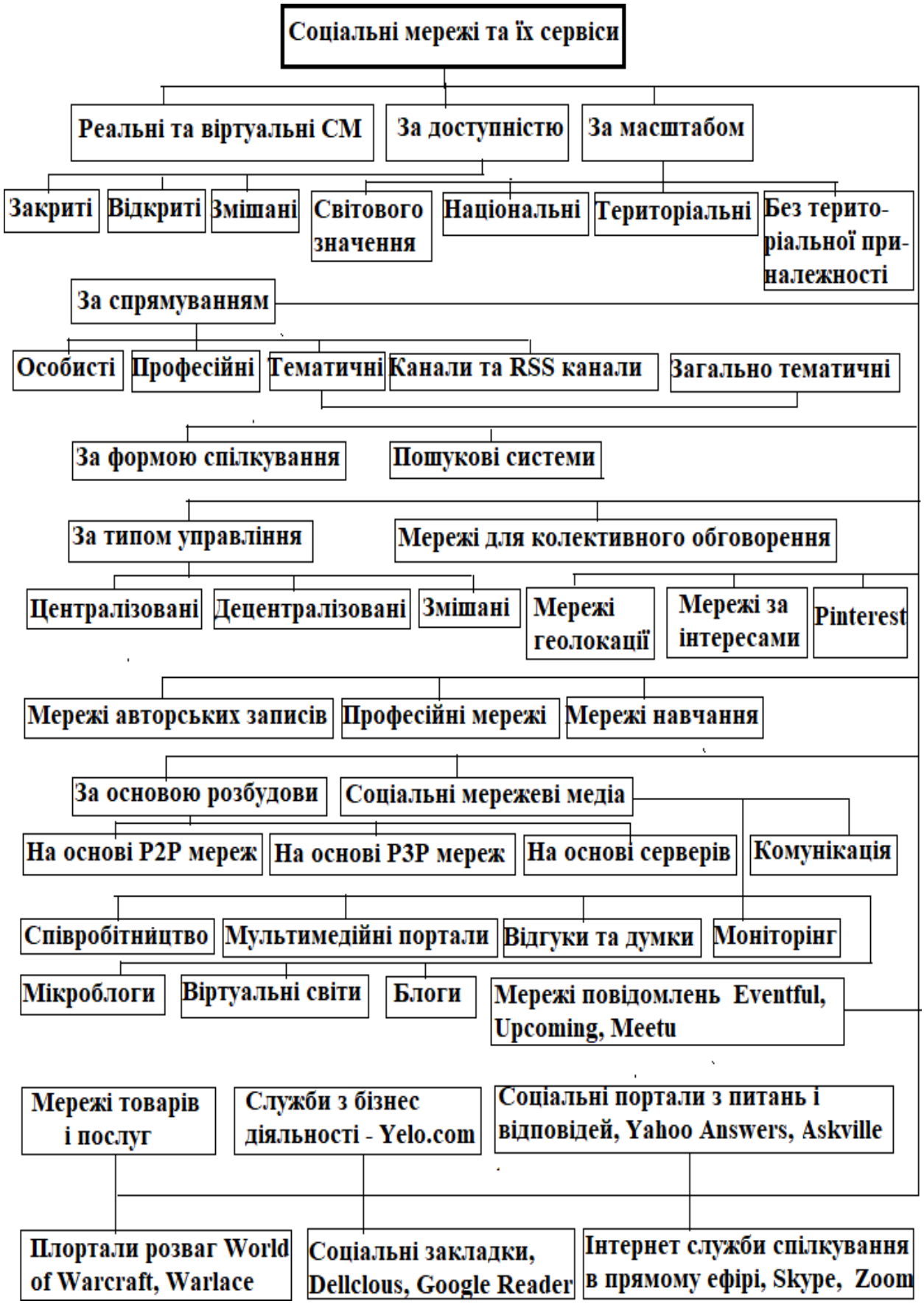



Рисунок 1.2. Витяг із класифікації соціальних мереж (СМ) та їх сервісів

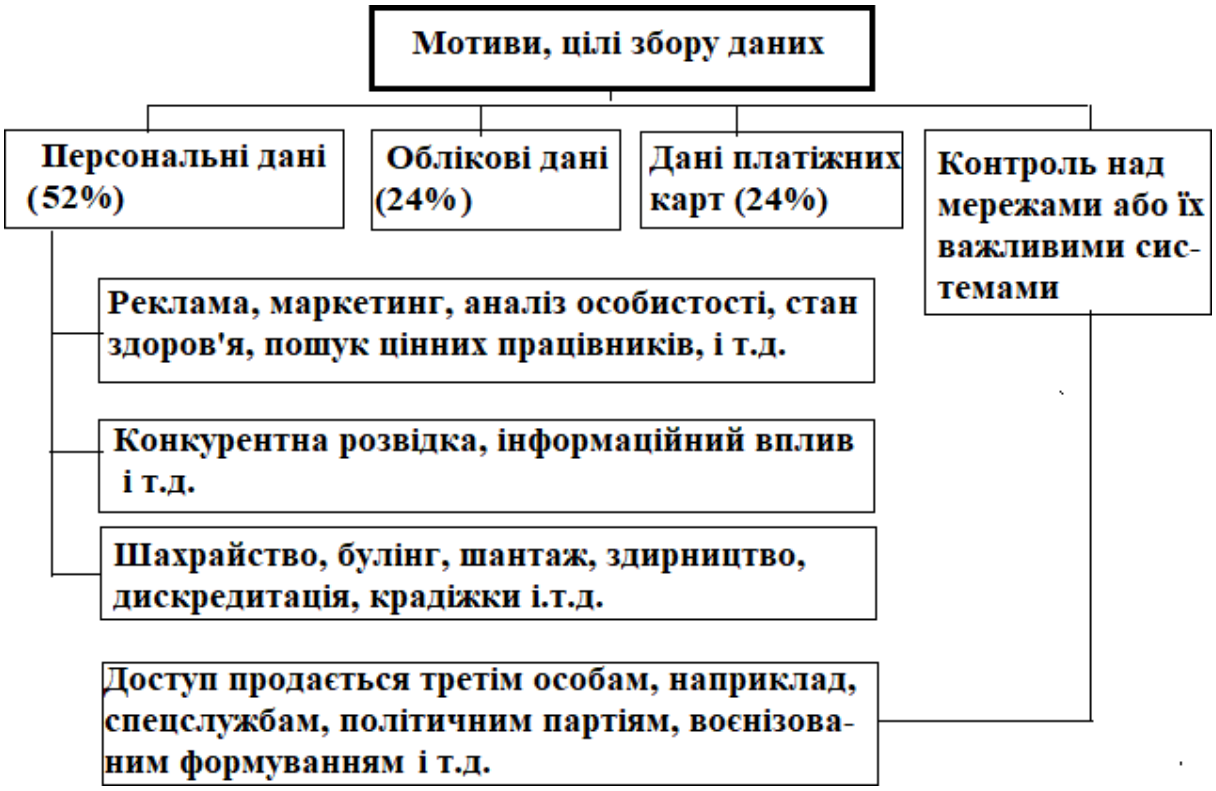



Рисунок 1.3. Мотиви та цілі збору даних

Контроль над мережами та їх важливими системами, такий вид впливу з'явився в останні роки.

Інноваційний підхід Facebook до збору інформації зробив цей сайт дуже зручною платформою для компаній, зацікавлених у маркетингу, рекламі та просуванні своєї продукції. Так, користувачі Facebook добровільно надають інформацію про свої дні народження, місце проживання, сім’ю, роботу та інтереси, підтрим ці даних особистих фотографій, повідомлення і статуси. Крім того, платформа також збирає та зберігає інформацію про переваги, повідомлення та дзвінки, списки друзів, родини та колег, історію пошуку та точно знає, які медіа користувачі читають, які заклади вони відвідують найчастіше та з яких пристроїв заходять у СМ.

«Дружній» стиль спілкування, поширений у соціальних мережах, оманливий – він може створити хибне враження, що поруч є лише друзі та доброзичливі люди, з якими можна поділитися інформацією.

Друга загроза — «маскарад» [4,5], тобто можливість підміни ідентичності: невідомо, хто приховує свої дії під іменем друзів чи за фотографіями друзів у соціальному профілі.

Сценарій такого маскараду можливий на корпоративному рівні. Результатом такого зловмисного сценарію може стати фішинг, організація «чорного піару» або «антипіар» [6]. Вже було багато прикладів, коли незрозуміло, хто створює сайт від імені компанії – і це створює проблеми для початкового брендингу.

Третій ризик пов'язаний із зломом записів соціальних мереж. Завдяки злому [4,7,8] злочинець може входити в соціальну мережу (у тому числі від імені особи, яка представляє в ній компанію, організацію), відправити на список друзів фішингові повідомлення і отримати гроші або мотивувати аудиторію на будь-які негативні дії - зокрема, пройти за вказаною URL-адресою і запустити вірус чи якийсь код.

Останнім часом особливої популярності набули сервіси скорочення довжини URL, які дозволяють замаскувати адресу небажаного веб-сайту під коротким посиланням. Сьогодні відбувається потужна боротьба із цими загрозами – сервіси скорочень URL-адрес почали використання покращених алгоритмів виявлення спаму та інших шкідливих речей. Однак для користувачів соціальні веб-загрози нікуди не зникли – переконливі новини та пропозиції від тих, кого ви вже знаєте і кого зламали, часто ведуть до скачування шкідливого ПЗ або спаму в інтернеті».

Не меншою загрозою є звичка використовувати однакові імена користувачів і паролі в корпоративній мережі та на зовнішніх соціальних ресурсах. Як наслідок, злом таких облікових записів користувачів у соціальній мережі значно підвищує ризик проникнення на корпоративні ресурси від імені одного зі співробітників компанії.

І, звичайно, не можна забувати, що соціальні мережі стали розсадником вірусів і троянських програм [9,10].

Загрозою безпеці компанії, не стільки інформаційної, скільки економічної, є компрометуюча поведінка компанії: у соціальних мережах співробітники часто поводяться інакше, ніж у середовищі корпоративного спілкування, а їх шокуючі

публікації та грубі висловлювання можуть викликати певну шкоду репутації компанії. З нею потрібно боротися насамперед організаційними методами [6, 11].

Іншою загрозою соціальних мереж, яка може зашкодити економіці компанії, є зростання трафіку, особливо під час перегляду відеоджерел. Щоб зменшити ці витрати, наприклад, можна обмежити доступ до відеотрафіку для тих категорій працівників, які не потребують цього для роботи.

Соціальні мережі – це сутність сучасних Інтернет-технологій. Вони поєднують в собі всі загрози, властиві Інтернету. Їх можна розділити на такі великі групи:

Веб-атаки. Оскільки соціальні мережі – це веб-додатки, їх можуть використати хакери для організації атак на вразливості браузера. Інструменти для таких атак включають [9,12,13] трояни, підроблені антивіруси, соціальні хробаки, які використовують для поширення у списки друзів та інші. Їх головна мета - проникнути в інформаційну систему відвідувача соціальної мережі і закріпитися в ній. Традиційні інструменти, такі як антивірусне програмне забезпечення, можуть допомогти та заблокувати ці програми в реальному часі.

Компрометація пароля та фішинг [4,5]. Оскільки соціальні мережі використовують паролі, щоб ідентифікувати нас, нам просто потрібно дізнатися чи зламати цю послідовність символів – і зможемо розсилати рекламу від імені інших або робити інші нелегальні дії. Крім того, деякі компанії використовують соціальні мережі для просування своїх продуктів, і крадіжка пароля адміністратора групи може фактично вкрасти саму групу. Традиційно, щоб отримати особисту інформацію, зловмисники використовують фішинг, фішингові сайти, соціальну інженерію тощо. Захистом від цих методів атаки є системи DLP і надійні технології, інтегровані з різним антивірусним ПЗ.

Файли cookie – це невеликі фрагменти інформації про службу, які веб-сервер розміщує на комп’ютері користувача. Використовується для зберігання даних специфічний для даного користувача і використаний веб-сервер різного призначення". організувати щось приклад, ключ сесії (без пароль), зашифрований пароль, логін. Тому вони можуть мати певну цінність для зловмисників [14,15].

Cookie файли можна вкрасти [16]. Найпростіший спосіб зробити це, коли у вас є доступ до місця призначення для користувач комп'ютер. Через Інтернет підключитися складніше. Крадіжка файлів cookie через ваше інтернет-з'єднання називається зломом сеансу. Хакер, який зламав ваш сеанс і перехопив ваші файли cookie, легко зможе ними скористатися.

Файли cookie можна замінити. Заміна файлів cookie – це зміна їх вмісту (наприклад, надсилання суми в інтернет-магазин). Файли cookie замінюються безпосередньо перед відправкою сервер.

Нас, безсумнівно, цікавить перший варіант (з розглянутих), коли наші користувацькі налаштування були вкрадені. У цьому випадку зловмисник зможе отримати доступ до вашого облікового запису, пароля від нього, а також до маси іншої інформації.

Витік інформації. Соціальні мережі можна використовувати для організації витоку важливої для компанії інформації, а також для підриву її репутації. Таку атаку можуть здійснити внутрішні співробітники компанії, незадоволені керівництвом, або спеціально представлені інсайдери. Системи DLP [17] і продукти для аналізу веб-публікацій розроблені для захисту від цих загроз.

Слід зазначити, що нині компанії, які розробляють продукти для захисту корпоративних мереж, мають можливість навмисно фільтрувати Інтернет-додатки, що входять до складу соціальних мереж. Такі продукти дозволяють вимкнути певні програми, групи програм або певні функції соціальних мереж.

Огляд комп'ютерного впливу. Коли ми ми говоримо «комп'ютерна атака», ми маємо на увазі запуск певних програм для отримання несанкціонованого доступу до комп’ютера. Форми організації нападів дуже різноманітні, але загалом усі вони належать до однієї з наступних категорії:

Віддалене вторгнення: програми, які отримують несанкціонований доступ до іншого комп’ютера через Інтернет (або локальну мережу).

Вторгнення на локальний комп’ютер: програми, які отримують несанкціонований доступ до комп’ютера, на якому вони працюють.

Віддалене блокування комп’ютера: програми, які блокують весь віддалений комп’ютер або одну програму в Інтернеті (або мережі) через Інтернет (або вам часто потрібно перезавантажити комп’ютер, щоб відновити функціональність)

Локальне блокування комп’ютера: програми, які блокують комп’ютер, на якому вони запущені

Сканери мережі: програми, які збирають інформацію про мережу, щоб визначити, які комп’ютери та програми, які на них запущені, потенційно уразливі для атак.

Програмні сканери уразливостей: програми, які сканують великі групи комп’ютерів в онлайн в дослідження комп'ютери, чутливий вниз це або інший специфічний жанр напади.

Відновлення пароля: програми, які легко «вгадують» паролі в зашифрованих файлах паролів.

Аналізатори мережі (сніфери): програми, які прослуховують мережевий трафік. Часто в них є можливості автоматичного вибору імен користувачів, паролей та номерів кредитних карток.

Зловмисники використовують різні інструменти впливу на СМ, перелік цих впливів наведено на рис. 1.4.

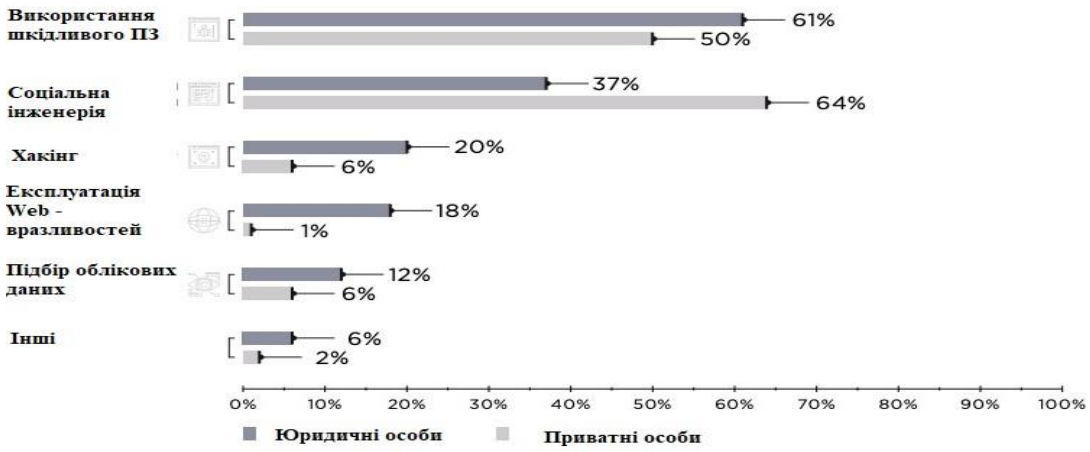



Рисунок 1.4. Відомості про впливи СМ у світі

Кількість можливих атак через соціальні мережі росте кожного дня і так само росте кількість та ефективність механізмів захисту.

## 1.2 *Аналіз математичних моделей безпеки інформації у соціальній мережі*

Методи та засоби ЗІ в СМ показані на рис. 1.5.

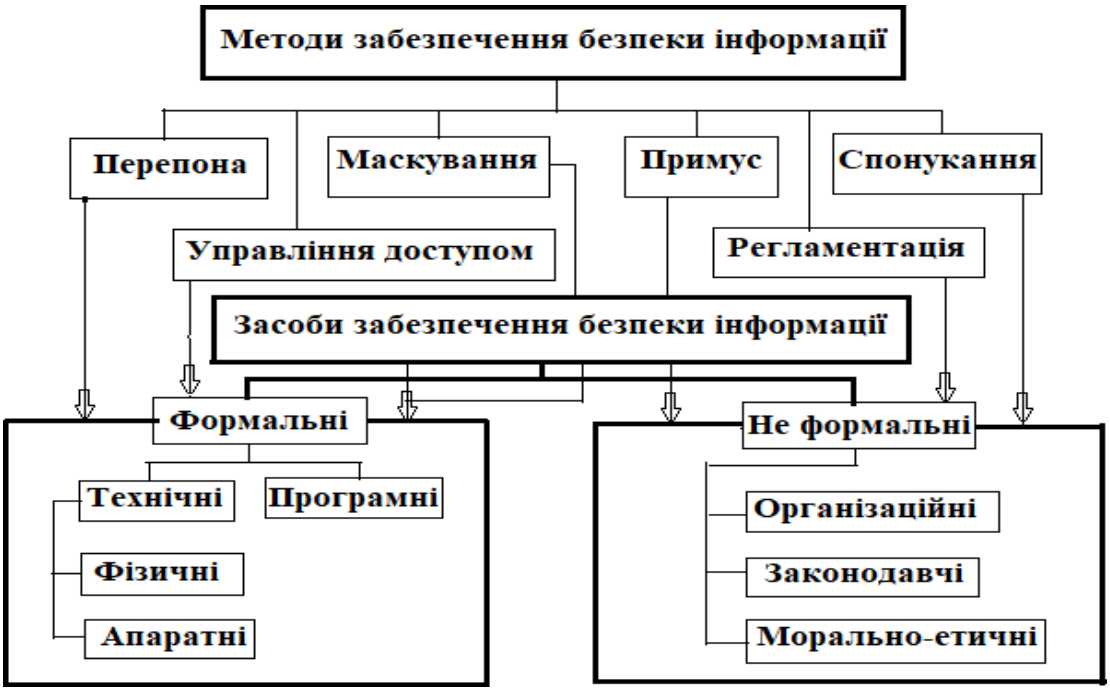



Рисунок 1.5. Методи та засоби захисту інформації в соціальних мережах

Класифікація моделей ЗІ представлена на рис. 1.6.


Рисунок 1.6. Класифікація моделей ЗІ

Рішення інформації безпеки тепер не можуть базуватися на на одній технології: Вони вимагають підхід, на багаторівневий технології в поєднанні з позицією «нульової довіри», щоб стримувати можливі порушення ІБ. Ці багаторівневі технології дозволяють забезпечити високий рівень контролю, видимість і гнучкість.

**Ієрархія засобів захисту баз даних**

Згідно з аналізом літератури [18,19,20,21], мережевий захист можна розділити на сім рівнів складності.

Перший є найбільш основним і обов'язковим. Головний інструмент безпеки - брандмауер. Брандмауер повинен обмежувати використання послуг, які надаються користувачам. Крім того, брандмауер повинен стежити за всіма підключеннями, як з одного, так і з іншого боку.

Другий рівень безпеки передбачає налаштування операційної системи, під якою працює веб-сервер. Кожна операційна система дозволяє створювати контрольні списки безпеки. Ці установки повинні бути сумісні з операційними системами постачальників, які співпрацюють з компанією.

Третій рівень вже орієнтований на мережу. Ви повинні бути оснащені датчиками атак на мережеве обладнання та програмне забезпечення вашого хостинг-провайдера. Найголовніше, щоб отриманий сигнал про небезпеку був належним чином оброблений і нейтралізований небезпеку.

Четвертий рівень безпеки – установка програмного забезпечення на рівні хостингу. Це набагато складніше завдання. По-перше, тут ви можете зіткнутися з застереженнями самої хостингової компанії. По-друге, таке програмне забезпечення набагато складніше, ніж прості датчики. З цієї причини рівень безпеки вищий.

Пятий рівень має два підрівні - А і В. Рівень 5А - це встановлення спеціального програмного забезпечення, яке діє як шар між операційною системою веб-сервера та рештою програм. Цей буфер не дозволяє хакерам атакувати вразливі програми, які беруть під контроль всю операційну систему під час його виконання. Це ні найдешевший версія, так що, як і на попередньому рівні необхідно

забезпечити підтримку програмного забезпечення, яке вони підтримують веб-сервери.

Рівень 5B є встановленням орієнтованих на специфічний програми брандмауера або проксі серверів. Вони націлені на протокол HTTP і запобігають атакам до того, як потенційні зловмисники зможуть отримати доступ до програм, запущених на веб-сервері. Однак проксі-сервер є істотним обмеженням. Налаштування та налаштування проксі – це теж своєрідне мистецтво.

Шостий рівень – це свого роду пік безпеки. Тут дозволені лише надійні операційні системи та програми, що працюють під ними . Іншими словами, всі запущені програми та операційні системи повинні бути належним чином налаштовані або розроблений спеціально для конкретних потреб компанії. Це найдорожчий, але і найефективніший спосіб захисту.

Сьомий рівень - встановлення та налаштування антивірусних програм. Для боротьби з вірусами, троянами тощо. Це захистить вас від вірусних та інших типів атак.

Можливі додаткові рівні безпеки, наприклад, на рівні баз даних, програм, з конфігурацією доступу, захищеними ресурсами, захистом веб-сайту від аналізу вихідного коду тощо.

Двофакторна (або «2FA») автентифікація — це спосіб ідентифікації користувача в онлайн-сервісі за допомогою комбінації двох різних методів аутентифікації. Методи можуть ґрунтуватися на тому, що знає користувач (наприклад, пароль або PIN-код) і те, що він знає (наприклад, апаратний токен або мобільний телефон) або на тому, що є невід'ємною частиною цього (наприклад, відбитки пальців).

У роботах [22-28] розроблено метод моделювання нестаціонарних процесів у системах захисту інформації. На основі методів про будову простого та оберненого диференціальних спектрів.

Математична модель процесів безпеки інформації в об'єкті в векторному вигляді має вигляд:

$$\frac{\bar{d}P}{dt} = f(t, P(t), \lambda(t), \mu(t)), P(0) = P_0, 0 \le t \le T \quad (1.1)$$

Недоліком методу підгонки локальних рівнянь є накопичення похибок у зворотному процесі, оскільки кількість дискретних диференціальних спектрів обмежена в процесі розрахунку кінцевого значення. Для досягнення необхідної точності розрахунків слід вибрати досить невеликий крок, що призводить до необхідності використання великих обчислювальних ресурсів і часу обробки даних.

Модель процесу ЗІ [29-34] представлена на рис. 1.7.

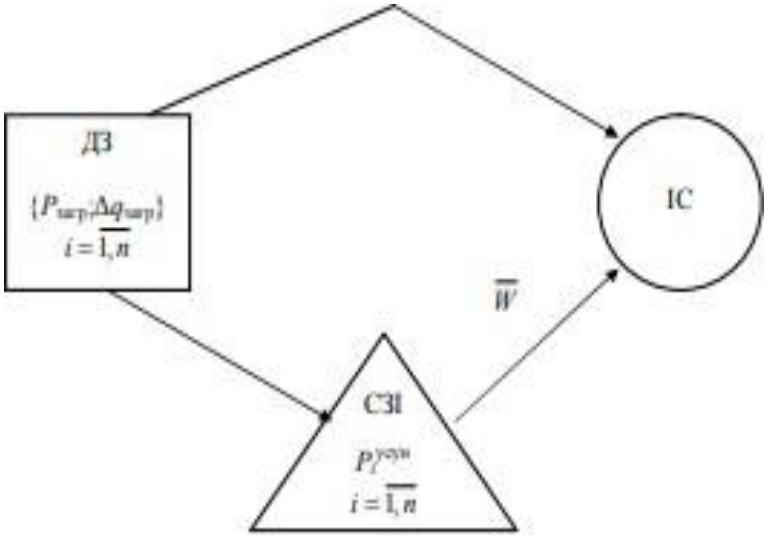



Рисунок. 1.7 Загальна модель процесу захисту інформації

Математична модель:

$$\overline{W} = \sum_{i=1}^{n} P_i^{\text{загр}} \times \Delta q_i^{\text{загр}} \times P_i^{усун} \quad (1.2)$$

Модель захисту інформації з повним перекриттям загроз [35-40] представлена на рис. 1.8.

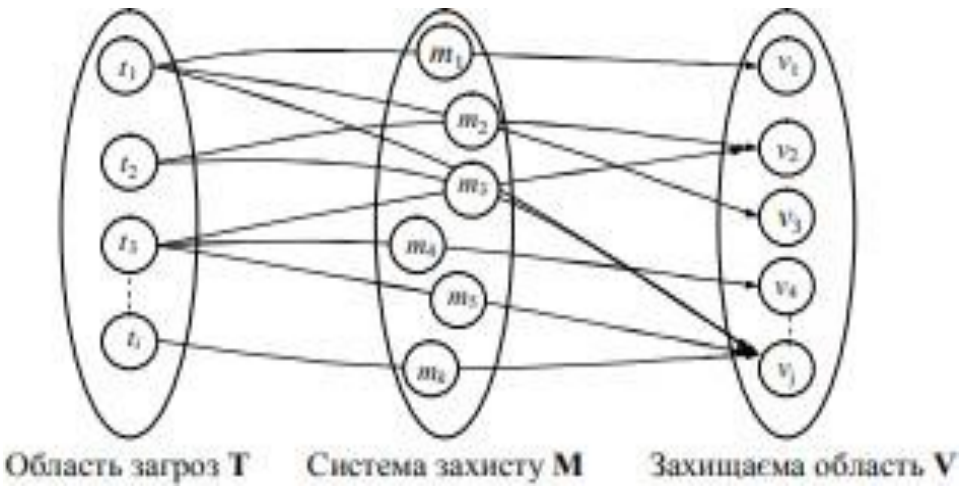


Рисунок 1.8 Модель процесу захисту інформації із перекриттям загроз

Аналітичний вираз, що описує цю модель, оцінка стійкості багаторівневої захисної перешкоди:

$$P_{СЗІ} = 1 - \prod_{i=1}^{m} (1 - P_i)$$

Модель багаторівневого захисту від загроз НСД показана на рис. 1.8

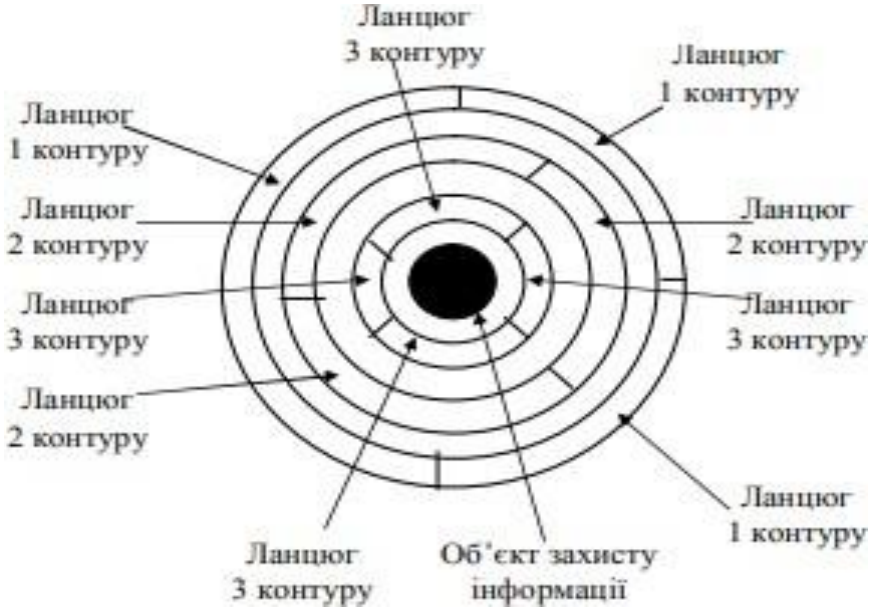



Рис. 1.8 Модель багаторівневого захисту від загроз НСД

***Висновки до розділу 1***

На основі аналізу практики та теорії побудови та використання СМ було виявлено об'єктивне протиріччя між необхідністю підвищення рівня інформаційної безпеки та недосконалістю системи захисту інформації та можливостями існуючих методів, що використовує система ЗІ в СМ.

Аналіз наявних методичних методів безпеки інформації в СМ показали свою обмеженість, зокрема через те, що виявлення зовнішніх впливів не враховує швидкості зміни впливів. Ступінь довіри між користувачами та їхня репутація не враховується. Тому комплексна проблема ЗІ не була вирішена. У сучасних наукових підходах основний акцент робиться на гіпотезі ЗІ, але більшість досліджень носить описовий характер. Практично не розглядається проблема розпізнавання зовнішніх

впливів з метою віднесення їх до загрози та не впроваджуються методи вдосконалення процесу розпізнавання впливів.

Недосконаліть та обмеження існуючих наукових методів захисту інформації в соціальних мережах не дозволяють забезпечити достатній рівень захисту інформації окремих осіб або груп користувачів у соціальних мережах.

# РОЗДІЛ 2
# РОЗРОБКА ПІДХОДУ ДО ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ ВРАХОВУЮЧИ ПАРАМЕТРИ ДОВІРИ

## 2.1 *Розробка методики оцінки захисту інформації в соціальних мережах із урахуванням параметру довіри між користувачами*

Довіра – це складне ментальне відношення юзера X (психічного стану), що характеризує його думки щодо обраного користувача Y щодо очікуваної поведінки/діяльності α, що важливо для досягнення мети G (певного бажаного стану) [25, 41-43]. Користувач X зазвичай делегує виконання α. Ментальними компонентами довіри X до Y являються наступні переконання:

- Переконання в компетентності: користувач X має вірити, що Y справді може виконати роботу та досягти бажаного результату;
- Переконання в намірах: користувач Y може не тільки виконати завдання, але й справді виконає його.
- Переконання в готовності: користувач X вважає (імітує мислення Y), що Y прийняв рішення і збирається це зробити α.
- Переконання в стійкості: користувач X вважає, що Y є стабільним у своїх намірах отримати α, якщо Y є передбачуваним і немає розбіжностей щодо α.
- Переконання в залежності: користувач X вважає, що Y необхідний для виконання завдання або що на нього краще покладатися, ніж не покладатися

Давайте визначимо типи довіри: Довірче положення описує довіру. Людина довіряє сайту надавати якісні послуги від постачальника послуг або постачальника ресурсів (що ми враховуємо). Делегована довіра описує довіру до користувача (представника), який діє та приймає рішення від імені сторони, якій він довіряє. Як окремий випадок надання довіри. Довіра доступу описує довіру, яку (постачальник) довіряє агентам, яким надано доступ до ресурсів. Це контроль доступу. Довіра до

автентичності описує віру в передбачувану автентичність користувача. Використовується в системах аутентифікації. Контекстна довіра визначає ступінь віри учасника в необхідні системи та інституційні механізми для підтримки транзакцій і забезпечення безпеки мережі, якщо щось піде не так (страхування, правова система, правоохоронні органи - також як ситуаційний контекст для довіри)

З лінійними параметрами зовнішніх впливів класичний підхід до захисту інформації використовує таке рівняння:

$$T_i = \left[D_j, D_n, D_m, D_k\right] \quad (2.1)$$

де Ti – сукупність загроз, що виникають внаслідок втрати довіри між користувачами, Dj довіра наданню послуг.

Людина довіряє сторонам надавати якісні послуги постачальник послуг або ресурсів, $D_n$ - довіра делегування описує довіру до користувача (представника), дії та прийняття рішень від назва партії, якій він довіряє. $D_m$ - Довіра доступу описує довіру довіряє користувачеві, якому надано доступ до ресурсів. Це - контроль доступа. Використовується в системі аутентифікація *Dk* - контекстний довіра визначає кімната віра учасник в необхідно системи і інституційні механізми підтримки транзакцій та забезпечення безпеки мережі.

Втрата такої якості, як довіра, є процесом, який має певні часові рамки. Позначте кількість інформації в системі - I. Інформаційний потік поза інформаційною системою обумовлений $dI -$, швидкість зміни цього потоку $-\frac{dI}{dt}$. Якщо потік і швидкість зміни потоку дорівнюють нулю, витоку інформації не відбувається:

$$dI = 0; \frac{dI}{dt} = 0 \quad (2.2)$$

Від чого може залежати витік інформації? Перш за все, від безпеки системи – дії щодо нейтралізації загроз інформаційній безпеці. $Z$ показник безпеки інформаційної системи. Складемо рівняння:

$$\frac{dI}{dt} = Z_p Z + \varepsilon(C_v + C_k)I \quad (2.3)$$

де $Z_p$- коефіцієнт, що відображає вплив заходів захисту інформації; $Cv$- коефіцієнт, що відображає вплив швидкості витоку інформації; $C_k$ −коефіцієнт, що відображає вплив кількості інформації на її витік.

Це рівняння можна інтерпретувати так. Витік інформації залежить від:

- від розміру ІС (отже, до певної міри і від кількості інформації);
- швидкість витоку інформації;
- заходів з нейтралізації загроз ІБ).

Потім розглянемо, що визначає безпеку системи - Z. Визначте безпеку системи як здатність системи протистояти несанкціонованому доступу до конфіденційної інформації. Тому безпека системи буде залежати від:

- від розміру системи (а також від кількості інформації);
- загрози інформаційної безпеки, що виникають внаслідок втрати довіри між користувачами.

Складемо рівняння:

$$\frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1})\varepsilon \tag{2.4}$$

де $D_i$- коефіцієнт, що показує вплив загроз інформаційної безпеки внаслідок втрати довіри між користувачами на безпеку інформаційної системи.

$C_{d2}$- коефіцієнт, що показує вплив розміру системи на безпеку;

$C_{d1}$ −фактор, що показує вплив безпеки на витік інформації.

Об’єднаємо рівняння (2.2) і (2.3) в систему.

$$\begin{cases} \frac{dI}{dt} = Z_p Z + \varepsilon(C_v + C_K)I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1})\varepsilon \end{cases} \tag{2.5}$$

Знайдемо стаціонарне положення системи, що описується рівняннями (2.5). Умови стаціонарності $dI = 0; \frac{dI}{dt} = 0$. Тому:

$$\begin{cases} Z_p \bar{Z} + \varepsilon(C_v + C_K)\bar{I} = 0 \\ D_i - I(C_{d2} + Cd_1)\varepsilon = 0 \end{cases} \tag{2.6}$$

Графік наведено на рисунку 2.1.

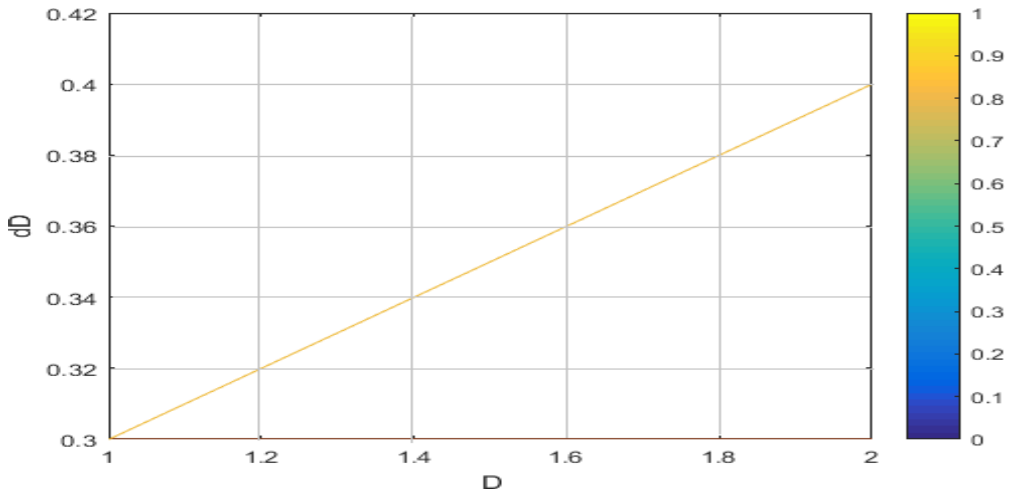



Рисунок 2.1 Графік диференціала функції довіри

Із другого рівняння системи виходить:

$$\bar{I} = \frac{D_i}{(C_{d2}+C_{d1})} \tag{2.7}$$

Тоді з першого рівняння системи рівнянь (2.6) знаходимо $\bar{Z}$.

$$\begin{aligned} Z_p\bar{Z} - \frac{(C_v+C_K)D_i}{(C_{d2}+C_{d1})} &= 0 \\ \bar{Z} &= \frac{(C_v+C_K)D_i)}{(C_{d2}+C_{d1})Z_p} \end{aligned} \tag{2.8}$$

Отже, умови стаціонарного положення системи представляються системою рівнянь 2.9 та зображені на рисунку 2.2.

$$\begin{cases} \bar{I} = \frac{D_i}{C_{d2}+C_{d1}} \\ \bar{Z} = \frac{(C_v+C_K)D_i}{(C_{d2}+C_{d1})Z_p} \end{cases} \tag{2.9}$$

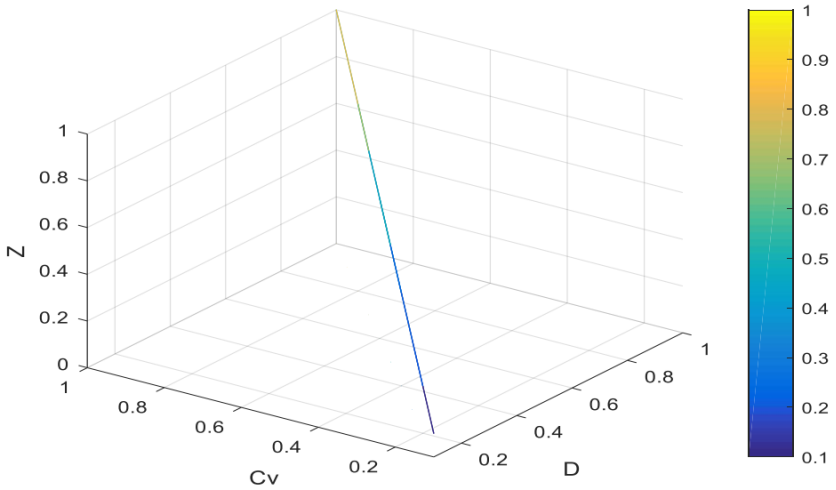



Рисунок 2.2 Результати розрахунку системи рівнянь (2.9)

Розв’яжемо систему рівнянь (2.5) методом «малих відхилень» $I = \bar{I} + I; Z = \bar{Z} + Z$:, тоді система рівнянь матиме вигляд:

$$\begin{cases} \frac{dI}{dt} = Z_p(\bar{Z} + Z) + \varepsilon(C_v + C_K)(\bar{I} + I) \\ \frac{dZ}{dt} = D_i - (\bar{I} + I)(C_{d2} + C_{d1})\varepsilon \end{cases} \quad (2.10)$$

Рішення системи рівнянь (2.10) представлено на рис 2.3.

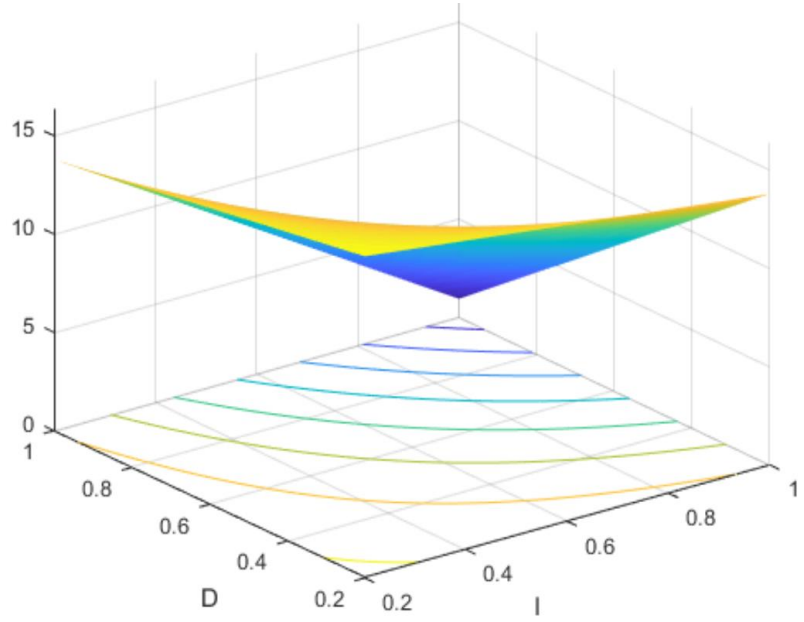



Рисунок 2.3 Результат системи рівнянь (2.10)

При лінійній залежності коефіцієнтів параметрів соціальної мережі ця залежність також майже лінійна.

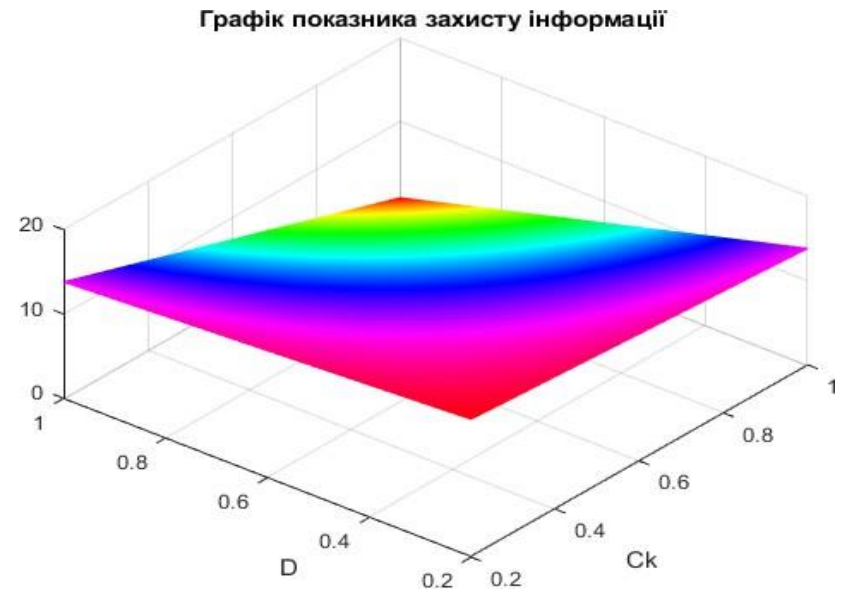
$$\begin{cases} \frac{dI}{dt} = (C_{d1} + C_{d2})Z - \varepsilon(C_v + C_K)I \\ \frac{dZ}{dt} = -I(C_{d2} + C_k) + D_i \end{cases} \varepsilon \quad (2.11)$$

Диференціюючи перше рівняння системи (2.11), отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})\left(Z_p + D_i\right) - (C_v + C_K)\frac{dI}{dt} \quad (2.12)$$

$$\frac{d^2I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})\left(Z_p + D_i\right)I = 0 \quad (2.13)$$

Результати розрахунку за системою рівнянь (2.13), наведеною на рис. 2.4.




Рискунок 2.4 Графік залежності коефіцієнта ЗІ від коефіцієнту, впливу кількості інформації на її витік

Як бачимо на графіку зі зростаючим $C_k$ −коефіцієнтом, що відображає вплив обсягу інформації на її витік, довіра до інформації знижується, що підтверджує достовірність результатів. При лінійній залежності коефіцієнтів параметрів соціальної мережі ця залежність також майже лінійна.

$$T = \frac{2\pi}{\sqrt{(C_{d1}+C_{d2})(Z_p+D_i)-\frac{(C_v+C_K)^2}{4}}} \tag{2.14}$$

Результати розрахунку за рівнянням (2.14), наведені на рис. 2.5.

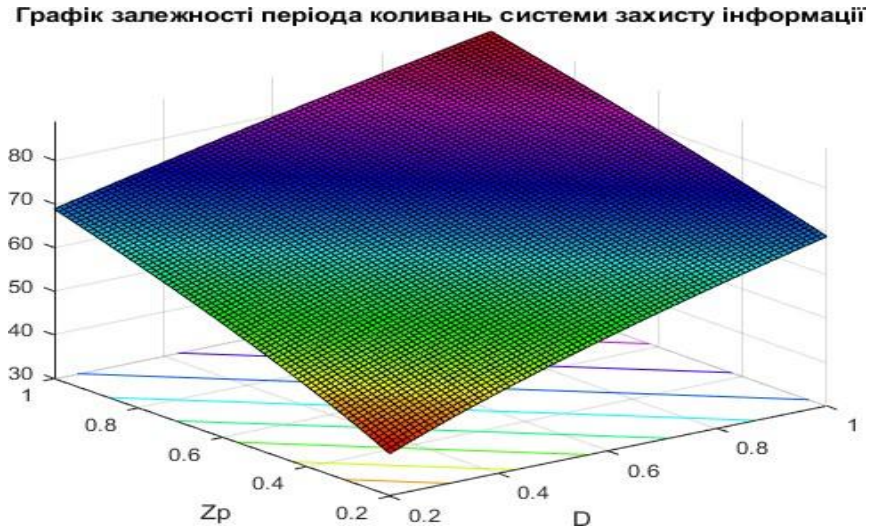


Рисунок 2.5 Графік залежності періоду коливань від коефіцієнта довіри та коефіцієнта захисту інформації.

З нелінійними параметрами зовнішніх впливів аналіз графічних залежностей лінійної системи вказує на нелінійність системи. Тому в систему рівнянь (2.1) введемо нелінійні компоненти (2.2):

$$\begin{cases} \frac{dI}{dt} = Z_p Z + \varepsilon(C_v + C_K)I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1})\varepsilon \end{cases} \tag{2.15}$$

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K)I + L_2(I^2) + \cdots + L_k(I^k) \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) + K_2(Z^2) + \cdots + K_n(Z^n) \end{cases} \tag{2.16}$$

де $L_2, L_3$тощо $K_2, K_3$тощо деякі лінійні оператори. Розглянемо нелінійність системи, що дозволяє знайти рішення для кожного рівняння системи методом послідовних наближень, припустивши:

$$\begin{gathered} I = I_1 + I_2 + \cdots + I_k \\ Z = Z_1 + Z_2 + \cdots + Z_n \end{gathered} \tag{2.17}$$

Припустимо

$$dI = 0, \frac{dI}{dt} = 0, \text{ та} \quad dZ = 0, \ \frac{dZ}{dt} = 0$$

$$I = I_0 \mathrm{Sin}\, \omega t, \ Z = Z_0 \mathrm{Sin}\, \omega t \tag{2.18}$$

Отримуємо систему рівнянь:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K)I - L_2(I_0^2 \mathrm{Sin}^2\, \omega t) - \cdots - L_k\left(I_0^k \mathrm{Sin}^k\, \omega t\right) \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) - K_2(Z_0^2 \mathrm{Sin}^2\, \omega t) - \cdots - K_n(Z_0^n \mathrm{Sin}^n\, \omega t) \end{cases} \tag{2.19}$$

Давайте перепишемо систему і представимо її так:

$$\begin{gathered} \begin{cases} \frac{dI}{dt} = \alpha Z + \beta_1 I - \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \\ \frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \end{cases} \\ \alpha = Z_p, \beta_1 = C_v + C_K, \beta_2 = -(C_{d2} + C_{d1}), \gamma = D_i \end{gathered} \tag{2.20}$$

Система рівнянь (2.20) перетворюється на наступну систему:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_K) \times I - \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \\ \frac{dZ}{dt} = -(C_{d2} + C_{d1}) \times I + D_i - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \quad (2.21)$$

Розв'язуючи систему рівнянь (2.21) щодо коефіцієнта захисту, отримуємо модель системи захисту інформації в соціальній мережі залежно від фактора довіри до інформації та довіри до користувачів.

Перетворення рівняння виглядає так:

$$Z(t) = \int N(t) - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} \frac{e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} dt - \int N(t) - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} \frac{e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} dt \quad (2.22)$$

Розв'язавши це рівняння для коефіцієнта захисту, отримаємо вираз:

$$\begin{aligned} Z(t) = \int & \left[ -\frac{1}{\omega} \sum_{k=2}^{\infty} \left( k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \right. \\ & \left. - \beta_1 D_i + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \right] \times \\ & \times \left[ (-C_{d2} - C_{d1}) \times \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \right] \times \\ & \times \left( \left( 1 - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2} t}{2}} \frac{e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \right) - \right. \\ & \left. - \left( 1 - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} \frac{e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \right) \right) dt \end{aligned} \quad (2.23)$$

Даний вираз (2.23) являється виразом моделі захисту інформації в соціальній мережі із залежністю від фактора довіри.

Для перевірки отриманих результатів виконаємо моделювання за конкретною моделлю. Моделювання буде виконуватися шляхом зміни загального $D_i$та часткового коефіцієнта довіри. $C_{d1}, C_{d2}$.

Результати моделювання наведені на рисунку 2.6.

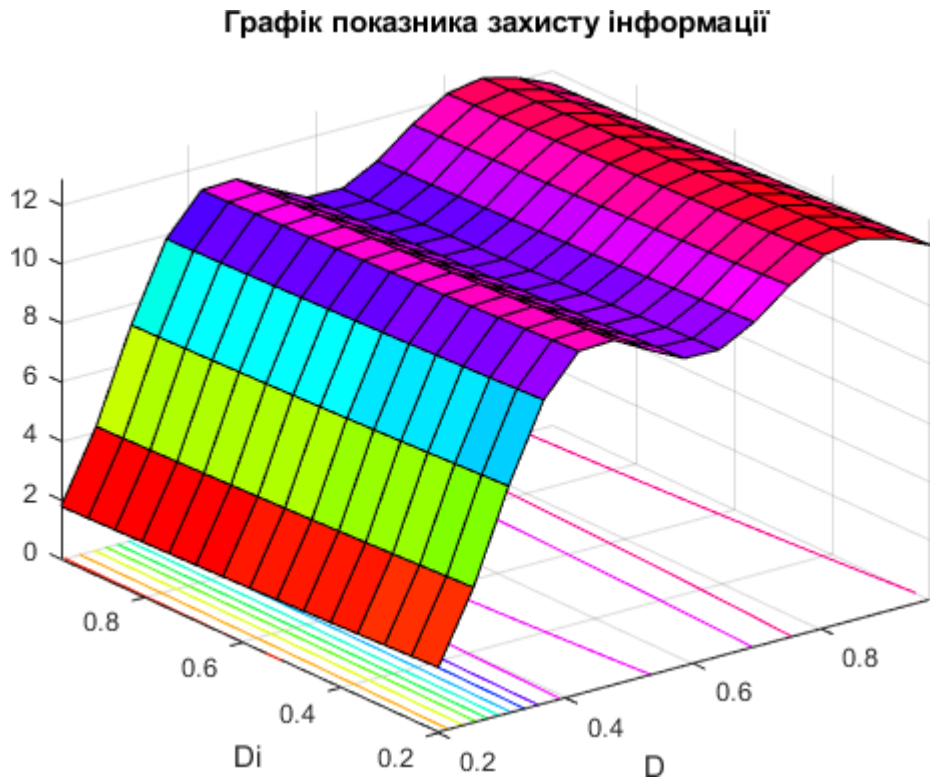



Рисунок 2.6 Графік залежності захисту інформації від довіри до користувачів і загальної довіри до інформації

З графіка, показаного на рис. 2.6, ми бачимо, що загальний коефіцієнт довіри має набагато більший вплив на захист інформації, ніж показники довіри кожного користувача. Фактори довіри, що впливають на захист інформації, не повинні впливати на всю систему захисту інформації в соціальних мережах так само, як загальний фактор довіри до інформації. Це узгоджується з фізичним і практичним значенням фактора впевненості. Це означає, що отримані результати є правильними і підтверджують правильність запропонованої моделі.

## 2.2 *Побудова фазового портрета системи захисту інформації з урахуванням зовнішніх впливів*

Розглянемо систему, в якій ми хочемо змоделювати атаку на систему, імунну відповідь системи. Рішення буде реалізовано в MatLab / Multisim. Передбачається, що динаміка шкідливого об'єкта відповідає логістичній моделі [44]. Розвиток

шкідливої інфекції залежить від на вихідний рівень, імуноіндукований спад і ефект власної щільності, тоді як зміна імунної відповіді залежить від вихідного рівня, природного зниження, стимуляції, що призводить до посилення реакції та нанесенню шкоди шкідливим об’єктом [45,46,5]. Нарешті, відносні характеристики пошкодженого органу залежать від щільності шкідливого об’єкта і його природний дегенерація. Далі динаміка системи описується за допомогою наступної диференціальної системи рівняння:

$$\begin{aligned} \frac{dP}{dt} &= \beta P - \gamma IP - \beta_0 P^2 \\ \frac{dI}{dt} &= \mu - \alpha I + bIP - \eta\gamma IP \end{aligned} \tag{2.24}$$

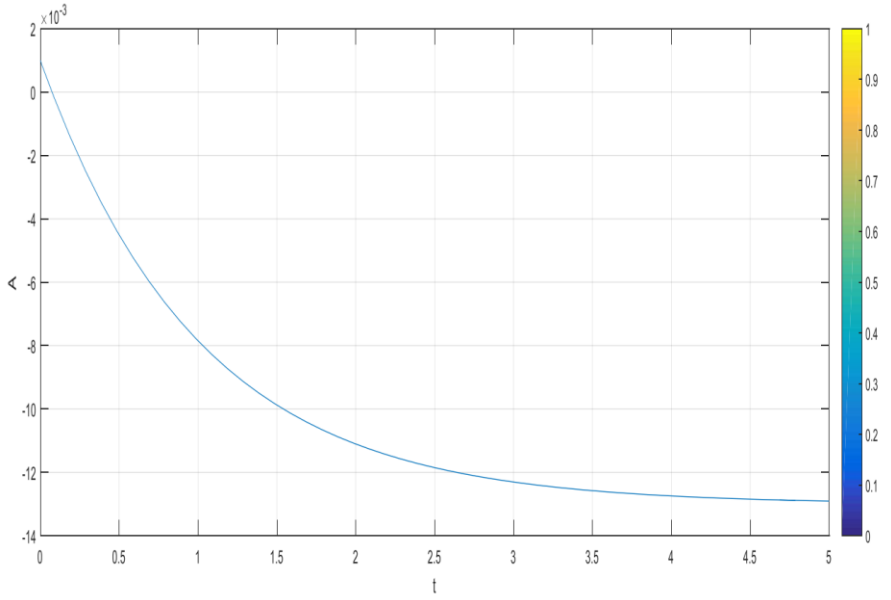
де P(t)- щільність шкідливих об'єктів, I(t) - імунний стан системи $\beta$- швидкість росту шкідливого об'єкта, $\gamma$- швидкість розпаду шкідливого об'єкта в результаті його взаємодії з імунною системою, а $\beta_0$- коефіцієнт внутрішньовидової інтерференції шкідливих об'єктів проектів. $\mu$- швидкість росту імунної системи, а - швидкість її природного зниження, б - стимуляція швидкості росту імунної системи через взаємодію з зшкідливими об'єктами, $\eta$- швидкість її зниження в результаті впливу з 3 шкідливий об'єкт. $\alpha$- швидкість зростання пошкодженого вузла за рахунок шкідливого об'єкта.

Для початкового аналізу створимо структурну схему системи з урахуванням системи рівнянь (2.24). Приймаємо такі умови:

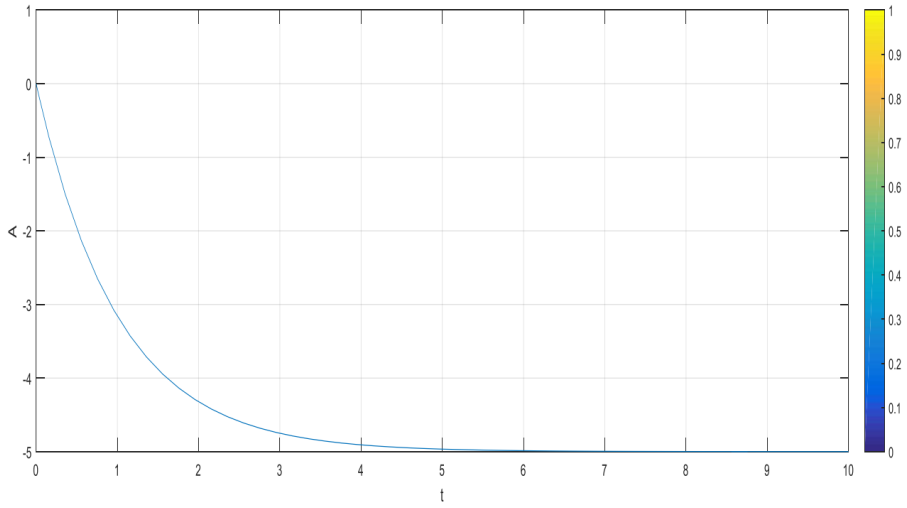
$$\mathrm{P} = 0, \mathrm{I} = \beta/\gamma), \gamma = 0.4, \beta = 0.6, \beta_0 = 0.2, \alpha = 0.3, \eta = 0.2, b = 0.4, \mu = 0.5$$

Далі на базі прийнятих умов перейдемо до моделювання самої схеми і відповідного графіку. У процесі моделювання ми будемо змінювати параметри взаємодій та систем захисту для визначення зони стійкості системи до впливів. Після моделювання, представимо фазовий портрет системи у разі зміни зовнішніх впливів.

Графіки значення амплітуди впливів від часу проведення впливів та максимального значення амплітуди впливів від часу проведення впливів представлені на рисунку 2.7 (а і б).




а)




б)

Рисунок 2.7. Мінімальне значення амплітуди впливів від часу проведення впливів - а) (всі параметри 0,1) і максимальне значення амплітуди впливів від часу проведення впливів - б)

Фазовий портрет системи захисту інформації у разі зміни зовнішніх впливів та графік процесу переходу системи захисту інформації в соціальну мережу наведені на рис. 2.8-2.10.

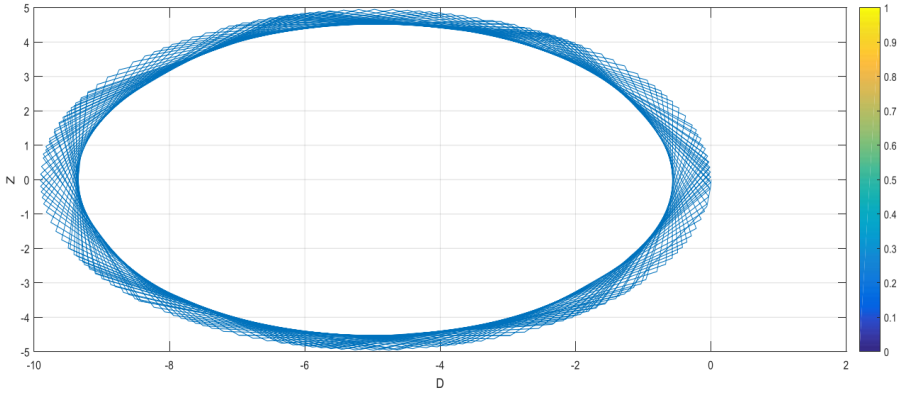



Рисунок 2.8. Фазовий портрет системи захисту при D = 0,1 і максимальному значенні впливу, всі інші параметри системи захисту - 1

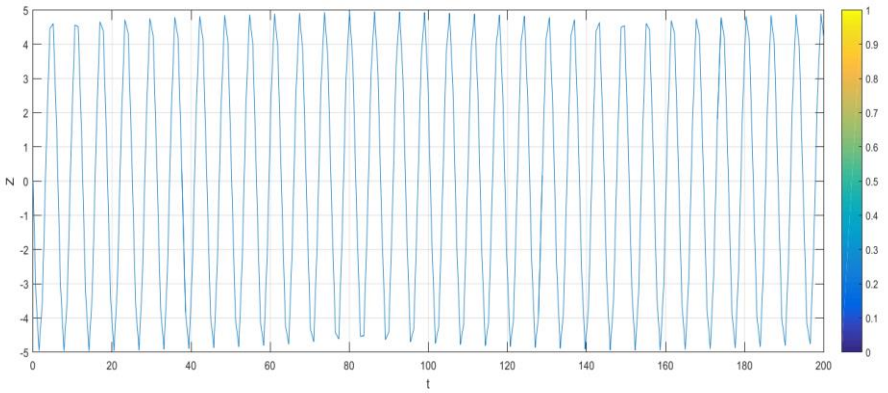



Рисунок 2.9 Перехідний процес системи захисту при D = 0,1 і максимальному значенні ефекту, всі інші параметри системи захисту – 1

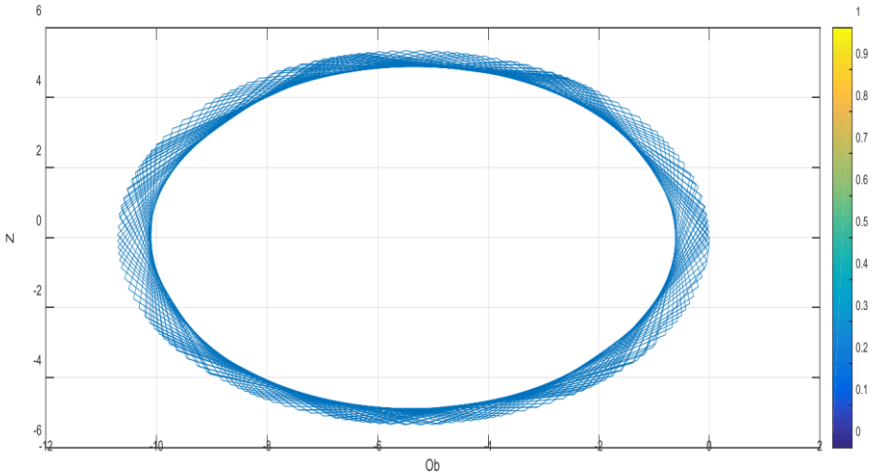


Рисунок 2.10 Фазовий портрет захисту при D = 0,5 і максимальному значенні удару, всі інші параметри захисту - 1

Аналіз графіків фазового портрета системи захисту від зміни параметрів довіри показує замкнуту лінію графіка стабільності системи захисту інформації та представлено у вигляді еліпса. Це центрові положення рівноваги і вони є стабільними.

Це означає, що можна зробити висновок, що при зміні параметра у відносних одиницях фазовий портрет системи захисту інформації в соціальних мережах подається у вигляді еліпса, що свідчить про стабільність системи захисту.

Таким чином, аналіз графічних результатів перехідних станів і фазових портретів при зміні параметрів довіри та амплітуди зовнішніх впливів на захист інформації в соціальній мережі, дозволяє зробити висновок, що розроблена теоретична модель відображає захист системи. . За результатами розробленої моделі можна визначити ступінь стабільності системи захисту інформації в соціальній мережі.

***Висновки до розділу 2***

Основою забезпечення безпеки окремих осіб або груп користувачів у соціальних мережах має бути концепція, що поєднує моделі та методи, що описують захист інформації в мережах з урахуванням динамічних особливостей безпеки системи та конкретних параметрів соціальної мережі. Реалізація такої концепції потребує розробки методів підвищення рівня безпеки інформаційного простору соціальних мереж; удосконалення математичної моделі та методів підвищення рівня інформаційної безпеки зз урахуванням впливу окремих елементів системи (довіра та репутація користувачів, кореляція їх поведінки, кластеризація структури мережі) на систему інформаційної безпеки. Оцінка вірогідності концепції має базуватися на математичній моделі оцінки рівня стабільності захисту інформації в соціальних мережах.

Концепція захисту інформації в соціальних мережах — це сукупність стратегічних підходів, перспективних математичних моделей, методів і прийомів, що дозволяють реалізувати принципи створення надійної системи захисту інформації від користувачів мережі. Запропонована математична модель ІБ в соціальних мережах базується на зв’язку між ІБ та конкретними параметрами мережі. Властивості інформаційної безпеки (конфіденційність, доступність, цілісність) вважаються динамічними функціями зі зворотним зв’язком. Введені динамічні характеристики безпеки системи та її індекс - захищеність системи, дозволяють побудувати базову лінійну систему динамічних рівнянь зі зворотним зв'язком, яка враховує загрози інформаційній безпеці, розмір системи, заходи захисту інформації, безпеку системи, обсяг інформації та конфіденційності.

Запропонована математична модель оцінки стійкості системи захисту інформації в соціальних мережах базується на аналізі параметрів системи захисту під час та після зовнішніх впливів на систему захисту з урахуванням динаміки зміни параметрів впливу. Модель дозволяє вивчити параметри захисту системи та здійснити необхідні дії для підвищення безпеки інформаційної системи з урахуванням нелінійної взаємодії компонентів системи безпеки та зовнішніх впливів.

# РОЗДІЛ 3
# ОЦІНКА БЕЗПЕКИ ІНФОРМАЦІЇ З ВРАХУВАННЯМ КОМПЛЕКСНОГО ВПЛИВУ ПАРАМЕТРІВ МЕРЕЖІ НА СИСТЕМУ

## 3.1 *Розробка методів оцінки інформаційної безпеки із урахуванням впливу комплексу параметрів мережі*

Для розробки методу розрахунку ЗІ від комплексного впливу параметрів мережі на систему захисту інформації соціальної мережі ми використовуємо такі рівняння:

$$\begin{cases} \frac{dI}{dt} = \alpha Z + \beta_1 I - \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \\ \frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \end{cases} \quad (3.1)$$

де $\alpha = Z_p, \beta_1 = C_v + C_K, \beta_2 = -(C_{d2} + C_{d1}), \gamma = Y13,$

$$Y13 = \frac{\sum_{i=1}^{n} (C'_D(i) - C_D(i))}{(n-1)(n-2)} + D + DR + (t^*(r+1)\wedge(-f)) - \left(\frac{\sum_{v \in V} C_{v1}}{n^2}\right) + (P-N)^*(P+N) + ((\alpha+\beta+\theta+\rho)V) + + \left(\frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i}\right) + (\log(n)/\log(n) * \log(n)) \quad (3.2)$$

$$Z(t) = \int \left[ -\frac{1}{\omega} \sum_{k=2}^{\infty} \left( k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \right.$$

$$-\beta_1 \times \left( \frac{\sum_{i=1}^{n} (C'_D(i) - C_D(i))}{(n-1)(n-2)} + D + DR + (t^*(r+1)\wedge(-f)) - \left(\frac{\sum_{v \in V} C_{v1}}{n^2}\right) + \right.$$

$$+(P-N) * (P+N) + ((\alpha+\beta+\theta+\rho)V) + \left(\frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i}\right) +$$

$$\left. +(\log(n)/\log(n) * \log(n))) + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \times \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \right] \times$$

$$\times \left( \left( 1 - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2}} \frac{e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \right) - \left( 1 - e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} \frac{e^{\frac{\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2} t}{2}}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} \right) dt \right.$$

Де R- репутація користувачів,

r- кількість користувачів 3, з якими цей користувач може ділитися інформацією,

t- користувач мережі, який перебуває на певному вузлі, n - кількість вузлів у мережі, $\sum_{v\in V} C_{v1}$- загальна кількість з'єднань в мережі,

$C_D$' (i) - максимальна центральність вершин у мережі;

$C_D$(i ) −центральність мережі;

n- кількість вузлів у мережі.

$P$-позитивний вплив між користувачами,

$N$- негативний вплив між користувачами,

$V_i$- коефіцієнт, що відображає вплив загроз інформаційної безпеки, що виникають у результаті взаємодії між користувачами, на безпеку інформаційної системи, параметр $\alpha$- описує тенденцію суб'єкта до взаємодії, параметр $\beta$- описує привабливість або популярність,

$\theta$- щільність графіка (оцінка - кількість L ребер),

$\rho$- характеристики тенденцій моделі для діадної симетрії, $x_i$- кількість з'єднань, які мають пік мережі в момент t, $Z_p$- коефіцієнт, що відображає вплив заходів захисту інформації;

$Cv$- коефіцієнт, що відображає вплив швидкості витоку інформації;

$C_k$ −фактор, що відображає вплив обсягу інформації на її витік, $D_i$ −фактор, що відображає вплив загроз інформаційної безпеки внаслідок втрати довіри між користувачами на безпеку інформаційної системи.

$C_{d2}$- коефіцієнт, що відображає вплив розміру системи на безпеку;

$C_{d1}$ −фактор, що відображає вплив безпеки на витік інформації,

I-кількість інформації в мережі,

Z - індекс безпеки IT-системи,

$D_i$ −фактор, що відображає вплив загроз інформаційної безпеки внаслідок втрати довіри між користувачами на безпеку інформаційної системи;

$DR$- фактор, що відображає вплив загроз інформаційної безпеки внаслідок втрати репутації серед користувачів на безпеку IT-системи; $(t * (r +$

$1)\hat{}(-f))$ −фактор, що відображає вплив загроз інформаційної безпеки, що виникають у результаті поширення інформації серед користувачів, на безпеку інформаційної системи;

$\left(\frac{\sum_{v\in V} C_{v1}}{n^2}\right)$ −коефіцієнт, що відображає вплив загроз безпеки інформації від фактору кластеризації мережі для безпеки інформаційних систем;

$(P-N)*(P+N)$- фактор, що відображає вплив загроз інформаційної безпеки, що виникають у результаті взаємодії користувачів, на безпеку інформаційної системи;

$(\alpha+\beta+\theta+\rho)V$- фактор, що відображає вплив загроз інформаційної безпеки, що виникають у результаті взаємодії користувача, на безпеку інформаційної системи;

$$\left(\frac{1}{n_i}+\frac{x_1}{\sum_{i=1}^{n} x_i}\right)-$$ коефіцієнт, що відображає вплив загроз безпеки

інформації з розвитку мережі, що стосується безпеки інформаційної системи;

$\ln(n)/\ln\ln(n)$- коефіцієнт, що відображає вплив загроз інформаційної безпеки від довжини шляху між користувачами на безпеку інформаційної системи.

Для підтвердження отриманих результатів проведемо остаточне моделювання. Для цього ми об’єднаємо всі розроблені та вдосконалені моделі в один методичний комплекс.

Ми будемо проводити моделювання з урахуванням специфіки соціальної мережі, такої як репутація, довіра, фактор взаємодії, обсяг інформації тощо.

Для отримання результатів спостережень значення всіх коефіцієнтів будуть враховані у відносних одиницях. Це означає, що зміна цих параметрів буде від 0 до 1.

З урахуванням зміни параметрів від 0 до 1, проведемо моделювання і зобразимо графік формул виведених вище, а саме 3.1, 3.2, 3.3, а також проаналізуємо отриманий графік. Результат моделювання представлений у вигляді графіка оцінки інформаційної безпеки з урахуванням комплексного впливу параметрів мережі на систему захисту наведено на рис. 3.1.

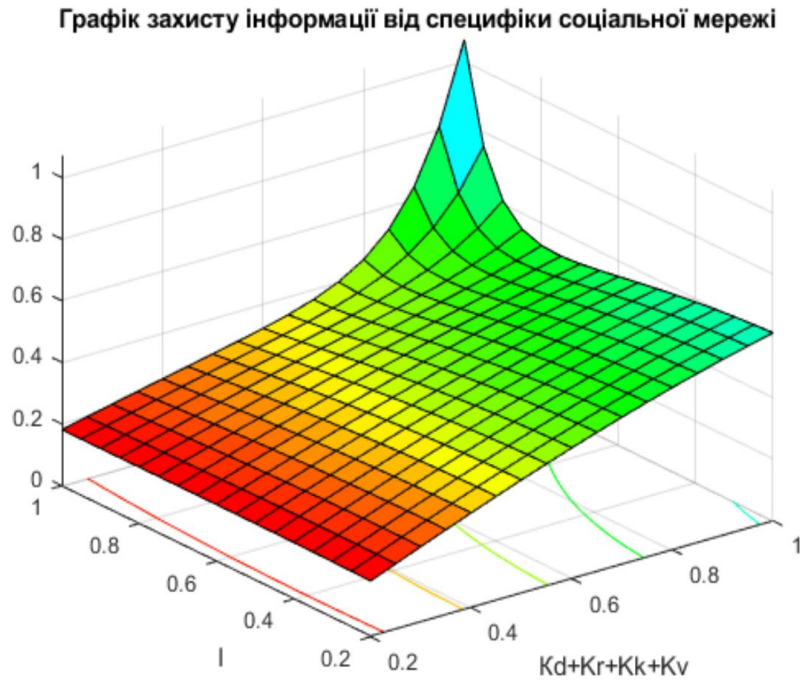



Рисунок 3.1. Графік захисту інформації в соціальній мережі з урахуванням комплексного впливу параметрів мережі на систему захисту інформації

Аналіз підсумкового графіка, який відображає захист інформації в соціальній мережі з урахуванням комплексного впливу параметрів мережі на систему захисту інформації, дозволяє зробити висновок, що із зростанням кінцевого комплексу шляхом вибору значень параметри соціальної мережі для забезпечення захисту інформації в соціальній мережі. При максимальних значеннях коефіцієнтів комплексний коефіцієнт захисту інформації дорівнює одиниці, що є дуже сприятливим результатом.

Крім визначення параметрів інформаційної безпеки в мережі. Розроблена методологія дозволяє оцінити стійкість системи захисту інформації до зовнішніх впливів. Результати моделювання системи інформаційної безпеки були б неповними без можливості визначення стійкості системи безпеки Інформація. Стабільність системи безпеки інформації ми будемо визначити для невизначених процесів і фаза портрети. Тимчасовий процесів і фазові портрети будуть визначені методом моделювання на розроблених моделях в навколишньому середовищі MatLab.

Результати, отримані в результаті моделювання, наведені на рис. 3.2 і 3.3. Фазові портрети системи захисту інформації, отримані в результаті моделювання.

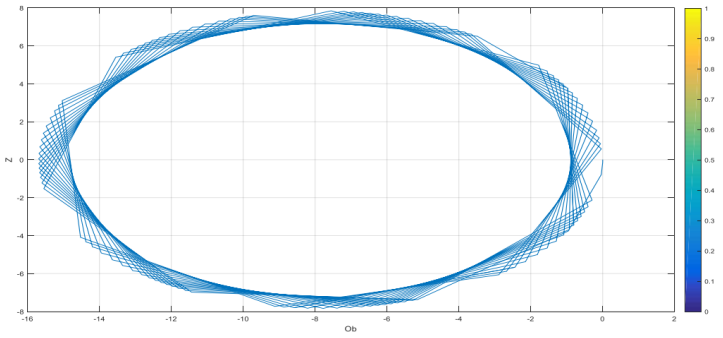



Рисунок 3.2. Фазовий портрет системи безпеки із значенням впливів і значенням усіх параметрів системи безпеки - 0,1

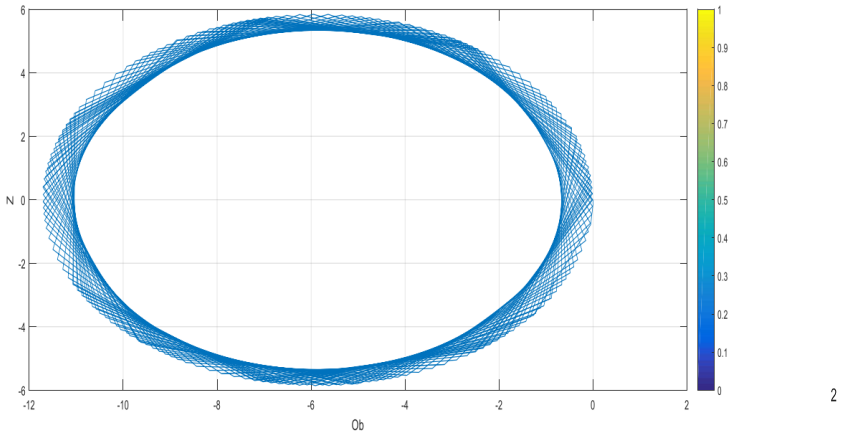



Рис. 3.3. Фазовий портрет системи безпеки із значенням впливів і значеннями всіх параметрів системи безпеки – 1

Аналіз рис. 3.2 і 3.3 показав, що розроблені методологічні основи захисту інформації в соціальній мережі дозволяють не тільки відбирати необхідні параметри для безпека, і вже і оцінювати стабільність системи захист інформації.

На рисунках 3.2 і 3.3. показано замкнуті еліптичні вказівні лінії стабільність системи вниз зовнішній квитанції. Фаза портрет представлений у вигляді еліпса, що свідчить про стійкість системи ЗІ.

Крім визначення параметрів ІБ в мережі, розроблена методологія дозволяє оцінити стійкість системи захисту інформації до зовнішніх впливів. Результати

моделювання системи інформаційної безпеки були б неповними без можливості визначення стійкості системи безпеки Інформація. Стабільність системи безпеки інформації ми будемо визначити перехідні процеси та фазові портрети. Перехідні процеси будуть визначатися шляхом моделювання на розроблених моделях у середовищі MatLab.

Перехідні коливання безпеки інформації в соціальній мережі, отриманої в результаті моделювання, під впливом зовнішніх факторів показано на рисунку 3.4 - 3.8.

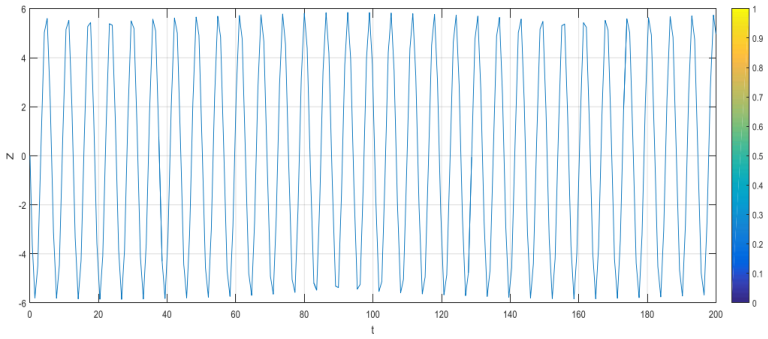



Рисунок 3.4 Процес переходу системи захисту із значенням впливів і значенням усіх параметрів системи захисту – 1

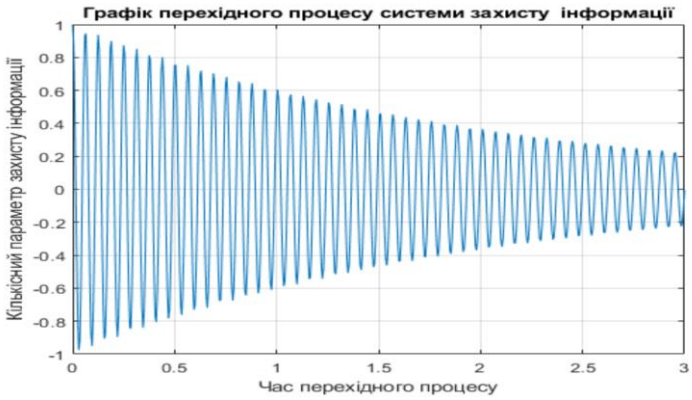



Рисунок 3.5 Перехідний процес системи захисту за відсутності впливів і значень параметрів 0.1

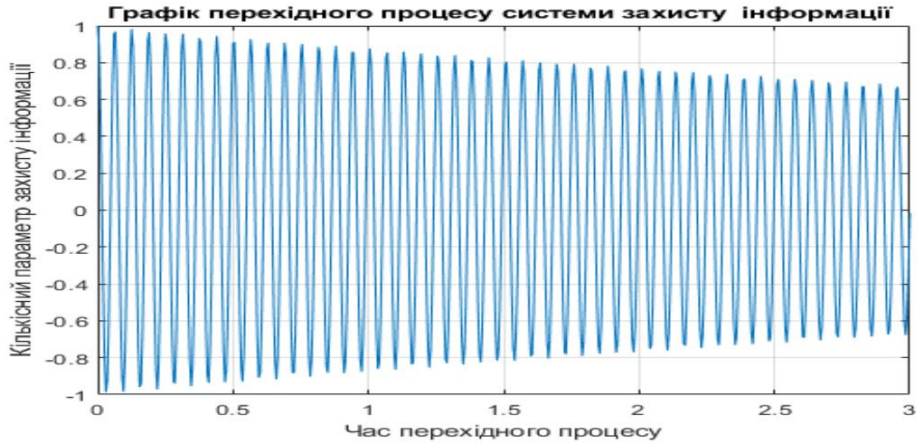



Рисунок 3.6 Процес переходу СЗ зі значенням впливів і параметрів

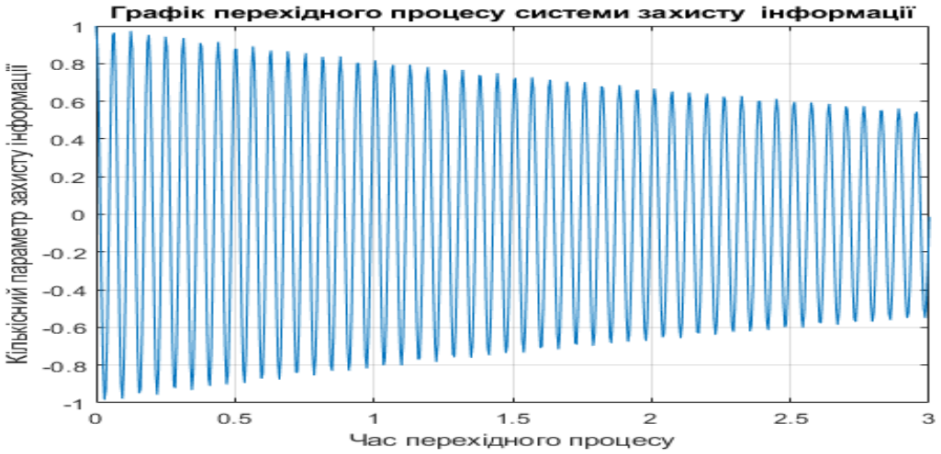



Рисунок 3.7 Процес переходу системи захисту з максимальним значенням впливу та значенням довіри 0,1, значенням репутації 0,01, без взаємодії та кореляції

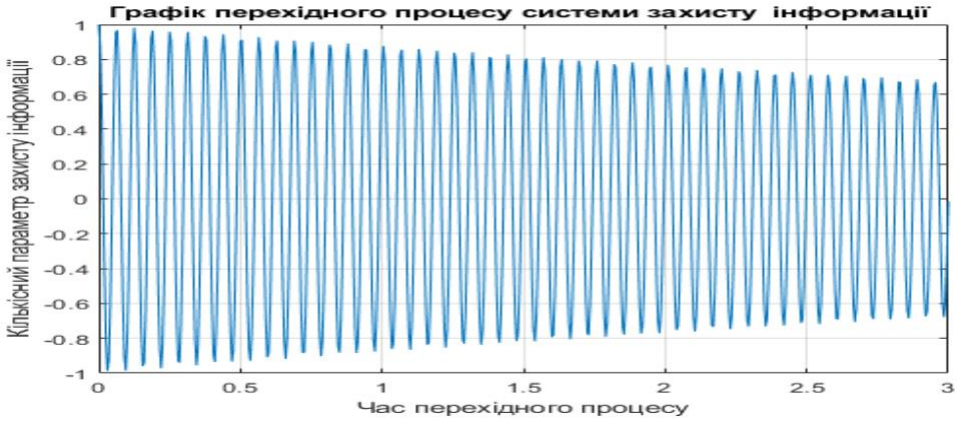



Рисунок 3.8 Процес переходу системи захисту до значень впливу та довіри 0,1, репутації 0,01, кореляції 0,1

Аналіз діаграм на рис. 3.4 - 3.8 показав, що розроблені методологічні основи захисту інформації в соціальній мережі дозволяють не тільки вибрати необхідні параметри захисту, але й оцінити стійкість системи захисту інформації для процесів системного переходу. На рис. 3.4 - 3.8 показані перехідні процеси, що мають демпфуючий характер, що свідчить про стійкість системи до зовнішніх впливів.

Підсумовуючи наведені вище розрахунки та етапи захисту інформації в соціальних мережах, можна визначити загальну методологію:

Методика розрахунку захисту інформації в соціальних мережах від комплексного впливу параметрів мережі на систему захисту складається з наступних етапів:

1. Етап визначення параметрів системи охорони та зовнішньої квитанції.
2. Вдосконалений етап моделювання процесу захисту інформації в соціальних мережах моделі.
3. Фаза будівництва перехідних процесів через зовнішній вплив на систему захисту інформації.
4. Останній етап визначення фазового портрета системи інформаційної безпеки з метою оцінки стійкості системи інформаційної безпеки до зовнішніх впливів.

Таким чином, розроблена методика розрахунку захисту інформації в соціальних мережах від комплексного впливу параметрів мережі на систему захисту, дозволяє оцінити стійкість системи захисту інформації під впливом зовнішніх впливів.

## 3.2 *Визначення переваг розробленої методології забезпечення інформаційної безпеки у соціальній мережі*

Методологічні основи інформаційної безпеки в соціальних мережах — це сукупність концептуальних, теоретичних і технологічних основ. Концептуальна основа складається з концептуальних положень, визначень, принципів, поглядів і рішень, сформульована наукова проблема. Теоретичні основи складаються з

математичних моделей, методів і прийомів, які присвячені розв'язанню цієї наукової чи науково-прикладної проблеми. Технологічні основи складаються з практичних методів, технологій, особливостей їх застосування, а також практичних рекомендацій щодо впровадженнятеоретичні та практичні результати методичний .

Тому структура методологічних основ інформаційної безпеки в соціальних мережах матиме такий вигляд (рис. 3.9).

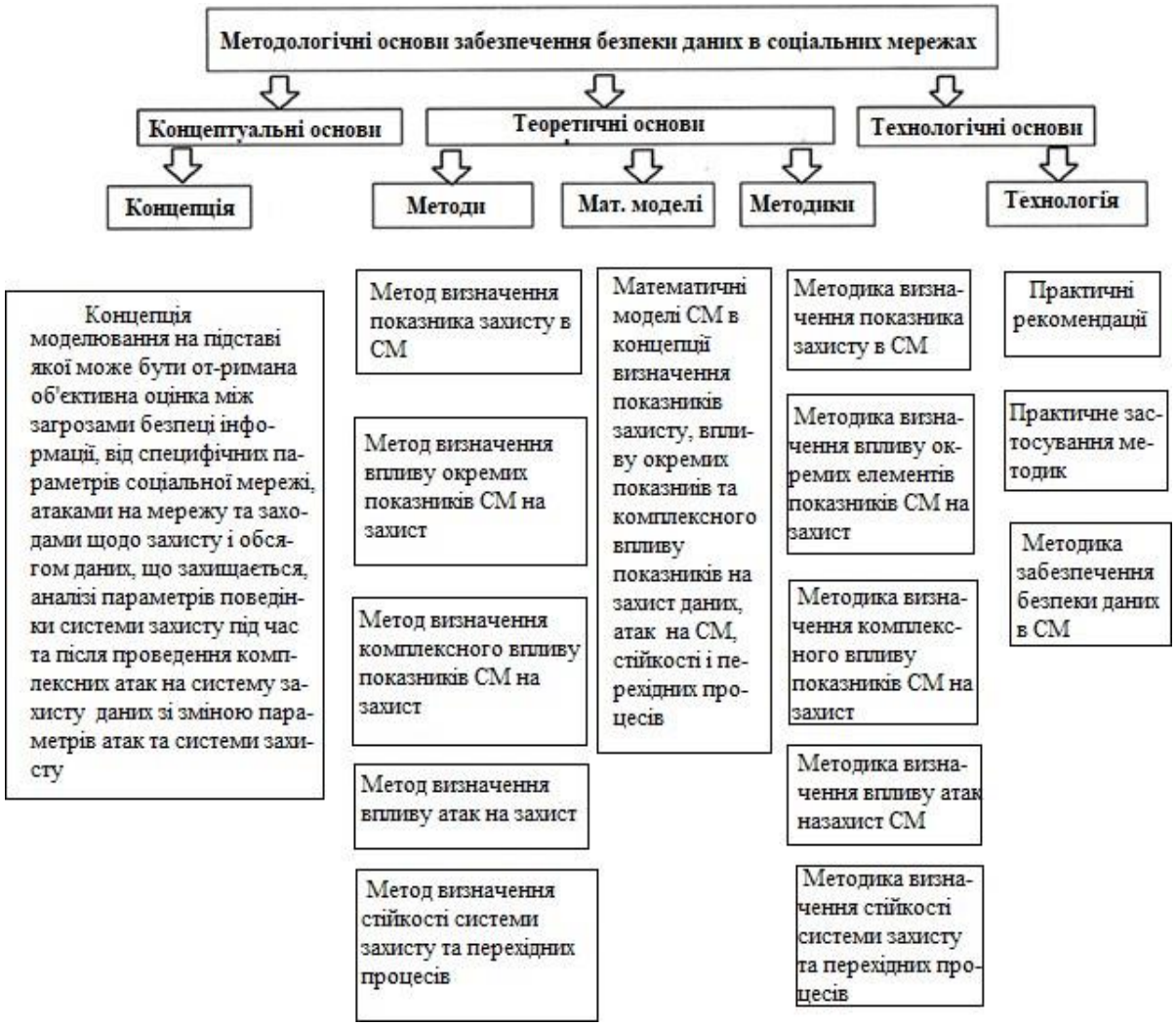



Рисунок 3.9 Методичні основи інформаційної безпеки в СМ

Концептуальні кодекси визначають стратегічні шляхи вдосконалення та розвитку методологічної бази. Вони задають основні напрямки розвит ку методики забезпечення інформаційної безпеки в соціальних мережах. Основні переваги розроблений методологічний основи програмне забезпечення безпеки інформація в соціальних мережах про стратегічні напрями розвитку інформаційної безпеки в СМ

має теоретичні основи, які включають концепцію, методи, математичні моделі та методики підтримки інформаційної безпеки в спільнотах. мережі.

Так для визначення переваги розберемо більш детально цей напрям методологічної інформаційної безпеки в суспільстві мережі.

Як було показано в попередніх розділах, інформаційна безпека в соціальних мережах забезпечується «класичними методами» з використанням маршрутизаторів, брандмауерів, антивірусного програмного забезпечення, підмереж безпеки, методів доступу тощо без урахування впливу певних параметрів СМ (конфіденційність, репутація користувачів мережі, взаємодія з користувачем). , довіра між користувачами, спільна думає користувачів мережі, сильний і слабкий знайомі, потужність користувач, тобто центральність вузлів, швидкість поширення інформації в мережі, параметри розширення мережі, кількість спільнот у мережі, канали поширення, ідентифікація користувача тощо), крім оцінки стабільності системи захисту, перехідні процеси є емпіричними. Стосовно загальних аспектів і методів виявлення загроз і захисту інформації користувача, більшість досліджень носить описовий характер і розглядається окремо від різних математичних і технічних досліджень. поради.

Розроблені методологічні основи інформаційної безпеки в соціальних мережах відразу виграють від удосконалення методу захисту інформації з урахуванням роботи кожного конкретного параметра.

Соціальні мережі та їх комплексне функціонування, а також вплив взаємодій зі зміною параметрів впливу та параметрів мережі, їх нелінійна взаємодія.

Визначення параметрів системи захисту інформації від параметрів мережі та параметрів впливу усуває недолік методу «класичного захисту».

За одностайною думкою соціологів, «нема довіри між користувачами СМ і немає захисту інформації», якщо перекласти на математику, якщо довіра між користувачами дорівнює нулю, то захист інформації дорівнює нулю. Це означає, що СМ не працює. Якщо репутація деяких користувачів дуже низька, ігнорування їх іншими користувачами виключає їх із соціальних процесів у СМ тощо.

Таким чином, розроблений метод захисту інформації в соціальних мережах, на відміну від існуючих, використовує комплексні значення параметрів і впливів мережі, що дозволяє одночасно вибирати показники захисту мережі, фазові портрети, перехідні процеси та наочно представляти їх у вигляді графіків, діаграми, таблиці тощо.

Проведене дослідження, яке було розкрито в попередніх розділах, наочно доводить: переваги ведення бухгалтерського обліку в розвиток системи безпеки інформації в Конкретні параметри СМ, користувачі, включаючи вплив на систему безпеки, визначення параметрів стабільності та перехідних процесів процесів.

Ще однією перевагою розробленої методології отримання інформації є метод визначення шкідливого впливу на параметри захисту інформації в соціальних мережах, який, на відміну від існуючих, відрізняється використанням системи диференціальних рівнянь з урахуванням складних параметрів атаки - безпеки в соціальних мережах.

Визначення вдарити усі окремо параметр СМ на системи захист і комплексний вплив усіх параметрів з урахуванням можливих впливів дозволяють прогнозувати та розраховувати конкретні параметри СМ, що важливо при створенні нових СМ та модернізації існуючих.

Забезпечення захисту інформації в соціальних мережах полягає в наступному.

Творцю СМ достатньо визначити параметри захисту інформації, конкретні параметри мережі, параметри впливу на систему захисту, застосувати певну методику для отримання необхідних результатів, які очевидні, добре зрозумілі, не потребують використання. складного апаратного та програмного забезпечення для обчислювального процесу.

***Висновки до розділу 3***

Розроблені методологічні основи інформаційної безпеки в соціальних мережах завдяки вдосконаленій методиці математичного опису параметрів взаємодії з

подальшим аналізом параметрів системи захисту дозволяють надійно захистити інформацію від різних видів і параметрів впливу на систему захисту.

Додатковою перевагою є розроблений метод захисту інформації в соціальних мережах при визначенні стійкості системи захисту з побудовою фазових портретів системи захисту та ретельним аналізом перехідних процесів для виявлення впливу на систему захисту.

Деякими перевагами методологічних основ захисту інформації в СМ є покращений метод безпеки інформації із визначенням впливу деяких параметрів мережі, а також:

1. Виконання математичного моделювання захисту даних в соціальних мереж з метою отримання необхідного рівня безпеки інформаційного простору СМ.
2. Оцінка захисту користувачів під час та після складних атак на систему захисту даних, змінивши параметри атаки та системи безпеки.
3. Підвищення рівня захисту інформаційного простору соціальних мереж шляхом побудови фазового та перехідного портрета системи захисту дані.
4. Оцінка рівня захищеності інформаційного простору соціальних мереж за допомогою окремих елементів системи: довіра, репутація, стосунки, взаємодія, центральність, коефіцієнт кластеризації, поширення інформації, розширення мережі, золота середина.
5. Аналіз безпеки даних у нелінійній взаємодії компонентів безпеки.

Модель дає змогу прогнозувати розвиток соціальних мереж.

Розроблені таким чином методологічні основи забезпечення інформаційної безпеки в соціальних мережах в рамках розробленої концепції перевершують методи і прийоми, що використовуються досі у СМ і наукових дослідженнях.

# ВИСНОВКИ

У науковій роботі була розкрита тема захисту інформації у соціальних мережах. Досліджені та проаналізовані наявні методи та методики захисту інформації, проведений аналіз актуальних проблем у існуючих методах. На основі виявлених результатів та недоліків був запропонований метод посилення рівня безпеки інформації у соціальних мережах за рахунок врахування специфічних параметрів, таких як довіра. Також було проаналізовано ефективність розробленого методу.

Розроблені методологічні основи інформаційної безпеки в соціальних мережах завдяки вдосконаленій методиці математичного опису параметрів взаємодії з подальшим аналізом параметрів системи захисту дозволяють надійно захистити інформацію від різних видів і параметрів впливу на систему захисту.

Подальшою роботою в даній сфері є дослідження питань, пов'язаних з розробкою нових і удосконалення вже існуючих методик виявлення загроз інформації або персональних даних у соціальних мережах.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Cyber security 101. The basics of social media [Електронний ресурс] – Режим доступу до ресурсу: https://fraudwatch.com/cyber-security-101-the-basics-of-social-media-threats/
2. Соціальна мережа [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0
3. Соцмережі-2021: ТікТок старшає, Facebook — переважно жіночий, а стрічку ми гортаємо 400 мільйонів років [Електронний ресурс] – Режим доступу до ресурсу: https://hromadske.ua/posts/socmerezhi-2021-tiktok-starshaye-facebook-perevazhno-zhinochij-a-strichku-mi-gortayemo-400-miljoniv-rokiv
4. Ахрамович В. М. Степеневі соціальні мережі. Colloquium–journal Warszawa, Polska. 2020. №5 (57). pp. 27–29.
5. Ахрамович В.М., Чегренець В.М. Управління ризиками інформаційної безпеки комерційного банку. Сучасний захист інформації. К. ДУТ. 2019. №2. с. 54–59.
6. Ахрамович В.М. Моделі довіри та репутації користувачів в соціальних мережах. Сучасний захист інформації. К. ДУТ. 2019. №4. с. 45–51.
7. Albert–László Barabási & Réka Albert. Emergence of scaling in random networks (eng.) // Science : journal. 2016. vol. 286 №. 5439. pp. 509—512.
8. Ballester C., Zenou Y. Key Player Po licies When Contextual Effects Matter. Jour nal of Mathematical Sociology. 2018. №. 38. pp. 233–248.
9. Halgin, Daniel & Brass, Daniel & Borgatti, Stephen. Social Network Research: Confusions, Criticisms, and Controversies, 2014.
10. Стефурак О.Р.,Тихонов Ю.О., Лаптєв О.А., Зозуля С.А. Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. Сучасний захист інформації. 2020. №2 (42). с. 19-26.

11. Заплотинський Б.А. Основи Інформаційної Безпеки, НУ “Одеська Юридична Академія”, Київський Інститут Інтелектуальної Власності та Права, Київ, 2017.
12. Тарасов Д.О. Формальні моделі систем захисту інформаціїі реляційних баз даних. Вісник НУ “Львівська політехніка” №489. - Львів 2003. - с. 296-306.
13. Синергетика для інженерів програмного забезпечення [Електронний ресурс] – Режим доступу до ресурсу: https://archer.chnu.edu.ua/xmlui/bitstream/handle/123456789/2833/%D0%A1%D0%86%D0%9F%D0%97.pdf?sequence=1&isAllowed=y
14. Ахрамович В.М., М., Тихонов Ю.О., Степаненко В. І. Дослідження розподілених соціальних мереж з точки зору специфічних характеристик безпеки. Зв’язок. К. ДУТ. 2019. №5. с. 13–18.
15. Ахрамович В. М. Концепція безпечної архітектури соціальної мережі, що захищає конфіденційність. Sciences of Europe. Praha, Czech Republic. 2020. № 49. pp. 10–17.
16. Cookie Hijacking: More Dangerous Than it Sounds [Електронний ресурс] – Режим доступу до ресурсу: https://securityintelligence.com/articles/guide-to-cookie-hijacking/
17. WHAT IS DATA LOSS PREVENTION (DLP)? [Електронний ресурс] – Режим доступу до ресурсу: https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/
18. Barabási A.–L., Albert R., Jeong H. Scale–free characteristics of random networks. The topology of the world–wide web. Physica A. 2019. V.281. pp.69–77.
19. Carl Timm, Richard Perez. Seven Deadliest Social Network Attacks. Syngress Publishing. 2019. L.A.Cutillo,R.Molva,andT.Strufe, Safebook:Aprivacy – preservingonline social network leveraging on real–life trust. Communications Magazine, IEEE. Dec. 2019. vol. 47. pp. 94–101.
20. Kotenko I. V., Chechulin A. A., Shorov A. V., Komashinsky D. V. Analysis and evaluation of web pages classification techniques for inappropriate content blocking. 14th Industrial Conference on Data Mining, LNAI. New York e.a.: Springer–Verlag. 2019. Vol. 8557. pp. 39–54.

21. Kubarev A. V. The classification characteristics based approach to formalization of information systems vulnerabilities. Voprosy kiberpezopasnosti. 2017. №2.
22. Грищук Р.В. Диференціально–ігрова модель гарантовано захищеної розподіленої системи захисту інформації. Захист інформації. 2016. № 1 (50). с. 20–28.
23. Грищук Р.В. Диференціально–ігрова модель кількісної оцінки захищеності технічних об'єктів. Захист інформації. 2018. Спеціальний випуск (40). с. 24–29.
24. Грищук Р.В. Диференціально–ігрова модель системи захисту інформації при нестаціонарній природі потоків захисних дій та інформаційних атак. Інформаційна безпека. 2019. № 2 (4). с. 23–29.
25. Грищук Р.В. Диференціально–тейлорівська модель перебування технічного об'єкта під впливом методів несанкціонованого доступу. Захист інформації. 2019. №1 (42). с. 19–27.
26. Грищук Р.В. Концепція побудови диференціально–ігрових гарантовано захищених розподілених систем захисту інформації. Сучасний захист інформації. 2017. № 1 (6). с. 4–9.
27. Капица С.П., Курдюмов С.П., Малинецький Г.Г. Синергетика та прогнози майбутнього. М. Наука. 2016. 288 с.
28. Підходи до захисту інформації при користуванні соціальними мережами [Електронний ресурс] – Режим доступу до ресурсу: http://dspace.nlu.eu.ua/bitstream/123456789/8420/1/Karmannuy_Kovgoa.pdf
29. Грищук Р.В. Метод диференціально–ігрового Р–моделювання процесів нападу на інформацію. Інформаційна безпека. 2019. № 2. с. 128–132.
30. Грищук Р.В. Спектральна модель процесу нападу на інформацію. Захист інформації. 2019. № 2 (43). с. 71–81.
31. Грищук Р.В., Даник Ю. Г. Основи кібернетичної безпеки. Монографія. Житомир. ЖНАЕУ. 2016.
32. Nefise Şirzad, A REVIEW ON ONLINE REPUTATION MANAGEMENT AND ONLINE REPUTATION COMPONENTS, Doğuş Üniversitesi Dergisi, 2022, pp. 219-242

33. B.Raja Koti, G.V.S.Raj Kumar, K.Naveen Kumar, Y.Srinivas, Influence of social information networks and their propagation. Security in IoT Social Networks, Intelligent Data-Centric Systems, 2021, pp. 83-108
34. Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., Stiller, B. (2017). A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts. In: Tuncer, D., Koch, R., Badonnel, R., Stiller, B. (eds) Security of Networks and Services in an All-Connected World. AIMS 2017. Lecture Notes in Computer Science, 2017, vol 10356. Springer, Cham.
35. Barabasi A.L., Bonabeau E. Scale Free Networks. Scientific American. 2019. pp. 50–59.
36. Basilisa Mvungi, Mizuho Iwaihara. Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. Computers in Human Behavior. Dec. 2019. pp. 20–34.
37. Benson Vladlena, George Saridakis, Hemamali Tennakoon, Jean Noel Ezingeard, The role of security notices and online consumer behaviour: An empirical study of social networking users, International Journal of Human Computer Studies. Aug. 2015. pp. 36–44.
38. Bonacich P. F. Power and centrality. A family of measures. Amer. J. Sociol. 2017. V. 92. pp. 1170–1182.
39. Bonacich P. F. Simultaneous group and individual centralities. Soc. Networks. 2017. V. 13. pp. 155–168.
40. Bondar I. V. Construction method for information security threat models of automated systems. 2019. pp. 7 – 10.
41. Cellmer S., Rapinski Z., Rzepeca J. Pseudolites and their Applications. INGEO 2011 – 5th International Conference on Engineering Surveying. Brijuni, Croatia. 2011. pp. 269 – 278.
42. Davidović T. & Teodorović, Dušan & Selmic, Milica. Bee Colony Optimization – part I: The algorithm overview. Yugoslav Journal of Operations Research. 2015. №25. pp. 33 – 56.

43. ECC Report 168. Regulatory Framework for Indoor GNSS Pseudolites. Electronic Communications Committee (ECC). Miesbach. 2011. p.20.
44. Ахрамович В.М., Тихонов Ю.О., Чегренець В.М., Свертока В.В. Методика виявлення каналів поширення інформації в соціальних мережах. Magyar Tudományos Journal. Budapest, Hungary. 2020. №37. pp 54–59.
45. Ахрамович В.М., Чегренець В.М. Дослідження безпеки даних користувачів в Інтернет–соціальних мережах. Magyar Tudományos Journal. Budapest, Hungary. 2019. №36. pp 58–61.
46. Ахрамович В.М., Чегренець В.М. Дослідження науково– методичного апарату захисту даних особистості в соціальний мережах. Sciences of Europe. Praha, Czech Republic. 2019. № 46. pp. 36–39.