МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

АХРАМОВИЧ ВОЛОДИМИР МИКОЛАЙОВИЧ

УДК 004.738.5

МЕТОДОЛОГІЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАРЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

05.13.21 «Системи захисту інформації»

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана на кафедрі систем інформаційного та кібернетичного захисту Державного університету телекомунікацій Міністерства освіти і науки України.

Науковий консультант: доктор технічних наук, снс **Лаптєв Олександр Анатолійович,** Державний університет телекомунікацій, професор кафедри систем інформаційного та кібернетичного захисту, навчально-наукового інституту захисту інформації.

Офіційні опоненти: доктор технічних наук, професор **Казакова Надія Феліксівна**, Одеський державний екологічний університет, завідувач кафедри інформаційних технологій;

доктор технічних наук, професор **Євсеєв Сергій Петрович**, Харківський національний економічний університет імені Семена Кузнеця, завідувач кафедри кібербезпеки та інформаційних технологій;

доктор технічних наук, доцент **Опірский Іван Романович**, Національний університет «Львівська політехніка», професор кафедри захисту інформації.

Захист відбудеться «21» квітня 2021 року об 11 годині на засіданні спеціалізованої вченої ради Д 26.861.06 у Державному університеті телекомунікацій за адресою: 03110, м. Київ, вул. Солом'янська, 7, конференц-зал.

З дисертацією можна ознайомитись у бібліотеці Державного університету телекомунікацій за адресою: 03110, м. Київ, вул. Солом'янська, 7.

Автореферат розісланий «13» березня 2021 року.

Учений секретар
спеціалізованої вченої ради
кандидат технічних наук Н.М. Довженко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У сучасному світі інформація потребує надійного захисту: від несанкціонованого доступу і поширення, випадкового видалення або зміни. Всі розвинені країни Європи стурбовані проблемою інформаційної безпеки, а також захистом персональних даних громадян. Це обумовлено тим, що інформатизація і оцифровка інформації набули широкого поширення у всіх сферах діяльності людини. У тому числі і зберіганні особистих та робочих даних.

Соціальні мережі (СМ) є одним з основних методів комунікацій, пошуку зв'язків та обміну як загальнодоступною, так і конфіденційною інформацією. Соціальні мережі, становлять постійно зростаючу частку серед загальних мереж. Крім того, сама мережа набуває нових властивостей, діючи як самостійний фактор.

Оскільки інформація в глобальній мережі існує поза простором і часом, сама мережа стає активним агентом впливу на людину, зберігаючи, насамперед, загальнодоступними великі обсяги даних. За останні роки почало суттєво змінюватись бачення проблеми кібербезпеки. Тому що людина дедалі більше перестає бути лише суб’єктом кіберзлочинів. Вона перетворюються на об’єкт сама по собі, а не тільки її фінансові та економічні інтереси та можливості.

Особливо ця проблема загострюється з посиленням цифрового гуманістичного характеру освіти, зростанням ролі соціальних мереж у житті людини в цілому.

Захист особистих даних в умовах сучасного інформаційного життя являється чи не найважливішим аспектом у задоволенні безпечного використання усіх можливостей нинішніх технологій. Тому проблема дослідження параметрів соціальних мереж для подальшого їх використання щодо вирішення задач захисту інформації та персональних даних є важливою та актуальною.

Обмін структурними та тематичними даними потенційно дозволяє використовувати соціальні мережі для вирішення широкого кола проблем обміну інформацією, а також захисту даних.

В області дослідження захисту інформації у соціальних мережах відомі роботи науковців: Котенка І.В., Новикова В.Б., Толубка В.Б., Хорошка В.О., Савченка В.А., Лаптєва О.А., Воронцова В.В., Грищука Р.В., Молодецької К.В., Губанова Д.А, Євсеєва С.П., Чхартишвили А.Г., Чуракова А.Н., Ланде Д.В., Фурашева В.М., Додонова О.Г., Пигонцова Г.Г., Горбуліна В.П., Ньюмана М.Е., Гірвана М., Леонсіо Антоніо Кутільо, Міхаеля Дюрру і інших.

Більшість наукових досліджень мають описово-дослідницький характер. Розглянуті дослідження призначені для вирішення окремих завдань захисту

інформації та баз даних і не можуть бути використані як методологічна основа для розроблення системи забезпечення безпеки даних.

Таким чином, на даний час в практиці і теорії побудови та експлуатації соціальних мереж існує об'єктивне протиріччя між необхідністю підвищення рівня захищеності інформації та недосконалістю системи захисту інформації і можливостями існуючих методів, які використовуються системою захисту інформації в соціальних мережах. Для розв'язання вказаного протиріччя в дисертаційній роботі сформульовано актуальну науково-прикладну проблему щодо *розробки методологічних основ захисту інформації в соціальних мережах з урахуванням впливу на захист специфічних параметрів мережі*.

Зв'язок роботи з науковими програмами, планами, темами. Тематика дисертаційної роботи і отримані результати безпосередньо відповідають пріоритетності розвитку інформаційних та комунікаційних технологій в Україні до 2020 р. згідно із Законом України «Про пріоритетні напрями розвитку науки і техніки», від 11.07.2001 № 2623–III, зі змінами внесеними згідно із Законом України «Про інформацію» від 02.10.1992 №2658–XII, Законом України «Про доступ до публічної інформації» від 13.01.2011 № 2939–VI, Законом України «Про захист даних» від 23.02.2012 № 4452–VI.

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету телекомунікацій і є частиною досліджень в рамках науково-дослідних робіт: «Застосування активних імпульсних радіолокаційних засобів для запобігання несанкціонованого доступу на об'єкт інформаційної діяльності» (Державний реєстраційний номер 00117U004418, ДУТ, м. Київ), яку виконував Державний університет телекомунікацій у 2017 – 2020 р.; «Методика формування моделі державного регулювання кібернетичної безпеки фондового ринку на основі диференціальних рівнянь із запізненням» (Державний реєстраційний номер 0118U100299, ДУТ, м. Київ), яку виконував Державний університет телекомунікацій у 2018 – 2020 р.; «Шляхи підвищення ефективності захисту командно-телеметричної інформації безпілотних літальних апаратів» (Державний реєстраційний номер 0120U100244, ДУТ, м. Київ) – закінчення (січень 2024 року).

Мета і завдання дослідження. Мета дисертаційної роботи полягає у підвищенні рівня захищеності інформації в соціальних мережах за рахунок врахування специфіки параметрів соціальних мереж: довіри, репутації, нелінійної взаємодії параметрів системи захисту інформації, аналізу поведінки системи захисту інформації під час зовнішніх впливів.

У відповідності до поставленої мети, для вирішення науково прикладної проблеми, в роботі сформульовано такі завдання:

1. Провести аналіз, тенденції подальшого розвитку основних методів та підходів до способів забезпечення захисту інформації в соціальних мережах.

2. Розробити математичну модель оцінки стійкості системи захисту інформації у соціальних мережах.

3. Розробити методику підвищення рівня захищеності інформаційного простору соціальних мереж.

4. Удосконалити математичну модель захисту інформації в соціальній мережі на основі динамічних характеристик безпеки системи.

5. Удосконалити математичну модель захисту інформації в соціальній мережі за рахунок врахування специфічних параметрів соціальної мережі, таких як параметр розповсюдження інформації, розширення мережи та коефіцієнта кореляції.

6. Удосконалити математичну модель та методику підвищення рівня захищеності інформації за рахунок врахування впливу компонентів системи таких як: довіра, репутація, кореляції, коефіцієнта кластеризації, на систему захисту інформації.

7. Виконати експериментальну оцінку отриманих теоретичних результатів шляхом математичного моделювання.

Об’єктом дослідження є процеси інформаційної взаємодії користувачів у соціальних мережах.

Предметом дослідження є моделі забезпечення захисту інформації у соціальних мережах.

Методи дослідження. Для досягнення поставленої мети в дисертаційній роботі використано методи теорії графів, математичного моделювання, теорії множин, системного аналізу, матричного аналізу, математичної статистики, теорії ймовірностей, теорії інформації для розробки способу моделювання, математичних моделей безпеки даних в соціальній мережі. Дослідження основані на сучасних методах теорії графів, методів моделювання, множин, системного аналізу, матричного аналізу, теорії управління для удосконалення методики підвищення рівня захищеності інформаційного простору соціальних мереж, яка базується на аналізі параметрів поведінки системи захисту під час та після проведення комплексних атак на систему захисту даних зі зміною параметрів атак та системи захисту. Під час дослідження застосовано сучасні методи теорії графів, методів моделювання, множин, системного аналізу, матричного аналізу, математичної статистики, ймовірностей для розробки методики підвищення рівня захищеності інформаційного простору соціальних мереж, яка базується на аналізі впливу окремих компонентів системи та комплексному аналізі впливу всіх компонентів в сукупності на систему захисту даних та реакції системи захисту на зовнішні впливи.

Наукова новизна одержаних результатів полягає у такому:

1. Вперше розроблено концепцію комплексного забезпечення захисту інформації в соціальних мережах, яка поєднує теоретичні методи, методики, моделі та технологічні підходи до захисту інформації у соціальних мережах. Концепція базується на оцінці балансу між загрозами втрати інформації від специфічних параметрів соціальної мережі; на математичній моделі зворотного зв'язку з урахуванням розміру системи, кількості даних та достовірності; на методиці підвищення рівня захищеності інформації з урахуванням коефіцієнтів довіри, репутації, кореляції, кластеризації, розповсюдження інформації та розширення мереж. Реалізація запропонованої концепції дозволяє забезпечити перехід від організаційно-технічної до структурно-організаційної технології захисту інформації в соціальних мережах.

2. Вперше розроблено математичну модель оцінки стійкості системи захисту інформації у соціальних мережах, яка базується на аналізі параметрів поведінки системи захисту під час та після зовнішніх впливів на систему захисту даних з урахуванням динаміки зміни параметрів впливу. Модель дозволяє проводити дослідження параметрів захисту системи та вживати необхідні заходи для удосконалення системи захисту інформації з урахуванням нелінійної взаємодії елементів системи захисту та зовнішніх впливів.

3. Вперше розроблено методику підвищення рівня захищеності інформаційного простору соціальних мереж, яка базується на результатах аналізу побудованого фазового портрету та аналізу перехідних процесів системи захисту інформації. Методика дозволяє ефективно досліджувати перехідні процеси з можливістю візуалізації моделей (блок-схем) і результатів дослідження.

4. Удосконалено математичну модель захисту інформації в соціальній мережі на основі динамічних характеристик безпеки системи, яка, на відміну від існуючих моделей, має зворотний зв'язок за такими параметрами, як, розмір системи, кількість даних та їх достовірність. Реалізація удосконаленої моделі дозволяє динамічно змінювати параметри захисту користувачів мережі в залежності від інтенсивності атак та заданого рівня захищеності інформації.

5. Набула подальшого розвитку математична модель системи захисту інформації в соціальних мережах, яка на відміну від існуючих, враховує розширення мережі, параметр розповсюдження інформації й коефіцієнт кореляції та дозволяє провести об'єктивну оцінку балансу між загрозами безпеки інформації й специфічними параметрами соціальної мережі, що, в свою чергу, дає можливість змінювати рівень доступу до інформації користувача в залежності від репутації оточення.

6. Удосконалено математичну модель та методику підвищення рівня захищеності інформації, які, на відміну від існуючих, враховують вплив на

систему захисту інформації специфічних параметрів: довіри, репутації, кореляції та коефіцієнта кластеризації мережі. Застосування моделі та методики дозволяє проводити аналіз впливу на систему захисту інформації інших ситуативних параметрів (наявної кількості діад, тріад, спільнот).

Практичне значення отриманих результатів.

Реалізація запропонованих в дисертації розробки методологічних основ захисту інформації в соціальних мережах з урахуванням впливу на захист специфічних параметрів мережі дозволяє:

1) проводити математичне моделювання процесу захисту інформації з метою отримання необхідного рівня захищеності інформаційного простору соціальних мереж;

2) здійснювати оцінку захисту користувачів під час та після проведення комплексних атак на систему захисту інформації зі зміною параметрів атак та системи захисту;

3) здійснювати підвищення рівня захищеності інформаційного простору соціальних мереж за рахунок побудови фазового портрету та аналізу перехідних процесів системи захисту даних;

4) проводити оцінку рівня захищеності інформаційного простору соціальних мереж з використанням окремих компонентів системи: довіри, репутації, взаємовідносин, взаємовпливу, центральності, коефіцієнта кластеризації, розповсюдження інформації, розширення мереж, середнього шляху;

5) проводити аналіз захищеності інформації при нелінійній взаємодії компонентів захисту.

Впровадження запропонованих методологічних основ захисту інформації в соціальних мережах з урахуванням впливу на захист специфічних параметрів мережі, дозволить значно скоротити час на знешкодження впливів на мережу та дозволяє підвищити захищеність інформації на 10,5 – 12,5 % у комплексному показнику захисту інформації.

Результати досліджень прийняті до впровадження в ТОВ «Бліц-Інформ» (акт від 23.05.2020 р.), в Науково-методичному центрі кадрової політики Міністерства оборони України (акт від 19.11.2020 р.), в ТОВ «Укрінфосистеми» (акт від 27.12.2019 р), в ТОВ «Комплексна служба безпеки «СИСТЕМА»» (акт від 9.10.2020 р.), ПП «ІТ Центр» (акт від 15.09.2020 р.), в навчальному процесі кафедри систем інформаційного та кібернетичного захисту Державного університету телекомунікацій при викладанні дисципліни «Методи та засоби технічного захисту інформації» для студентів спеціальності 125 «Кібербезпека» денної форми навчання (акт від 16.09.2019 р.).

Особистий внесок здобувача. Всі положення, які виносяться на захист, належать особисто автору. В роботах, які опубліковано в співавторстві,

особисто здобувачу належать: в [1, 6] розроблено часткова модель захищеності інформації в соціальних мережах; в [2, 11] виконаний аналіз параметрів, які впливають на захист інформації в соціальних мережах. Визначені типи зовнішніх впливів на систему захисту інформації, які впливають на СМ та ймовірність її побудови; в [3-5, 19] визначена необхідність врахування зв'язків користувачів та розроблено модель захисту інформації з врахуванням зв'язків користувачів у соціальних мережах, приведені результати моделювання процесу захисту, які підтвердили адекватність розробленій моделі; в [9] удосконалено модель сильних і слабких зв'язків, кореляційних зв'язків в СМ; в [10, 21] проведено аналіз параметрів соціальних мереж (передача інформації іншим користувачам, щільність трафіку, ймовірність побудови мережі). Розроблено математична модель визначення захищеності персональних даних від довіри в соціальних мережах; в [13] розроблено модель підвищення ефективності криптографічного захисту інформації в СМ; в [6, 17, 20] удосконалено модель управління ризиками інформаційної безпеки та захистом інформації; в [14] розроблено часткову методику виявлення каналів поширення інформації в соціальних мережах; в [7] розроблено модель пошуку співтовариств в соціальній мережі та їх вплив на захист інформації в СМ; в [12, 15, 16] розроблено методику оцінки характеристик безпеки даних користувачів в залежності від параметрів зовнішніх впливів; в [17] розроблено методику управління ризиками інформаційної безпеки банку; в [22] розроблено аналіз впливу на захист інформації хмарних технологій; в [23] розроблено модель захисту інформації при врахуванні розширенні соціальних мереж, збільшення кількісті користувачів та ступеня їх репутаційних характеристик; в [24] розроблено модель пошуку співтовариств в соціальній мережі з метою визначення репутаційних параметрів для формування моделі захисту інформації; в [25] проведено моделювання і візуалізацію системі захисту соціальних мереж; в [26] розроблено модель захисту інформації при розширенні соціальних мереж; В [27, 28] розроблена математична модель на основі врахування таких параметрів соціальних мереж, як передача інформації іншим користувачам, щільність трафіку, ймовірність побудови захищених мережі. Розглянуто три варіанти вирішення рівняння близько стаціонарного стану системи, доведено, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненційним загасаючим законом.

Апробація результатів дисертації. Основні результати дисертаційних досліджень доповідалися й обговорювалися на конференціях і семінарах, а саме:

– 3rd International scientific and practical conference «Perspectives of world science and education». (Osaka, Japan, November 27 – 29, 2019);

– Регіональний семінар Міжнародного союзу електрозв'язку для країн Європи та СНД «Цифрове майбутнє на основі 4G/5G» «Digital Future Powered by 4G/5G» (м. Київ, 14–16 травня 2018);

– I International Scientific and Practical Conference «Science, society, education: topical issues and development prospects» (Kharkiv, Ukraine, December 16 – 17, 2019);

– IV International Scientific and Practical Conference «Scientific achievements of modern society» (Liverpool, United Kingdom, December 4 – 6, 2019).

– International scientific conference «Advances of science» (Karlovy Vary, Czech Republic – Kyiv, Ukraine, December 6, 2019);

– VIII міжнародна науково–практична конференція «Осінні наукові читання» (м. Київ, 31 жовтня 2019 р.);

– IV International Scientific and Practical Conference «Topical issues of the development of modern science» (Sofia, Bulgaria, December 11 – 13, 2019);

– Семінар-практикум Міжнародного союзу електрозв'язку для регіонів Європи та СНД. «Інфраструктура ІКТ як основа цифрової економіки» (Київ, 14 – 16 травня 2019 р.);

– II Міжнародної науково–практичної конференції. «Тенденції розвитку конвергентних мереж: рішення пост-NGN, 4G і 5G». (Київ, 17 – 18 листопада 2016 р.);

– II International Scientific and Practical Conference «Priority directions of science development» (Lviv, Ukraine, November 25-26, 2019).

Публікації. За результатами дисертаційних досліджень опубліковано 45 наукових праць. Основні наукові положення викладено у 29 наукових статтях [1 – 29], що опубліковані у фахових наукових виданнях України та закордонних періодичних виданнях. Із них 1 стаття [1] опублікована у науковому виданні, що входить до наукометричної бази SCOPUS. За матеріалами виступів на науково-технічних конференціях опубліковано 10 публікацій [30 – 39]. Додатково результати досліджень відображені в статтях [40 – 45].

Структура та обсяг дисертації. Структура та обсяг дисертації. Дисертація складається зі вступу, 5 розділів, висновків, списку використаних джерел з 229 найменувань на 21 сторінці. Повний обсяг дисертації 301 сторінка, з них 275 сторінок основного тексту.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У вступі обґрунтовано актуальність теми дисертації, сформульовано науково–прикладну проблему, мету, об’єкт, предмет, завдання дослідження, наукову новизну одержаних результатів, практичне значення результатів, зв'язок роботи з науковими програмами, планами, темами досліджень Державного університету телекомунікацій. Визначено особистий внесок здобувача, відомості про апробацію результатів роботи, публікації.

У першому розділі дисертації здійснено аналіз існуючих методів захисту інформації. Проведено аналіз вітчизняної та зарубіжної наукової літератури за темою дисертаційної роботи. Розглянуто існуючі загрози персональним даним в соціальних мережах. Проаналізовано сучасний стан проблеми захисту даних в соціальних мережах. Здійснено постановку проблеми дослідження.

Проводиться аналіз різних типів існуючих моделей впливів та атак на систему захисту інформації. Описується динаміка впливів на систему захисту. Інформації як система диференційних рівнянь:

$$\frac{d\,\ddot{x}(t)}{dt} = F(t)\,\ddot{x}(t) + B(t)\,\ddot{u}(t) + G(t)\,\ddot{\xi}(t), \qquad (1)$$

де: $\ddot{x}(t)$ – вектор стану впливу, $F(t)$ і $B(t)$ – матриці стану і управління, $\ddot{\xi}(t)$ – випадковий процес, $\ddot{u}(t)$ – вектор управління параметрами, $G(t)$ – матриця масштабування.

Стан загроз впливів: $\ddot{y}(t) = R(\ddot{x}(t), t)$, де: $R(\ddot{x}(t), t)$ – матриця спостереження.

Вказана система рівнянь – нелінійна, успіх розрахунків залежить від апріорних ймовірностей та ресурсів.

Загрози впливів визначається наступним чином:

$$\frac{d\,\vec{x}(t)}{dt} = \Phi[\vec{x}(t), \vec{y}(\vec{x}(t), t)]. \qquad (2)$$

Потік впливів визначається:

$$\varepsilon \frac{d\,\vec{y}(t)}{dt} = Q[\vec{x}(t), \vec{y}(\vec{x}(t), t)], \qquad (3)$$

де: ε – матриця, що характеризує ефективність впливів.

В роботі проаналізовано методологію синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу. Динаміку протікання інформаційного конфлікту, яка описується системою диференціальних рівнянь Колмогорова-Чепмена. Вплив представлений в

вигляді Орграфа. Під орграфом загрози захисту інформаційної системи розуміється зважений орієнтований граф. Вершинами якого є вразливості, що характеризуються («зважені») рівнем їх актуальності. Тобто значенням ймовірності того, що інформаційна система готова до безпечної експлуатації у відношенні цього впливу. Дуги графа визначають можливість використання зловмисником виявлених впливів, що утворюють загрозу.

З метою послідовної оцінки уразливості, в дисертаційній роботі, автор обґрунтовує та вибирає класифікацію оцінки уразливості системи захисту інформації (CommonVulnerabilityScoringSystem, CVSS). Дана система призначена для класифікації вразливості за шкалою критичності від 0 до 10:

- 0,0 - 3,9 – низький ступінь;
- 4,0 - 6,9 – середній ступінь;
- 7,0 - 9,9 – високий ступінь;
- 10 – критичний ступінь.

Оцінка (віднесення до рівня критичності) уразливості проводиться на основі набору показників, а саме: вектор доступу, складність доступу, аутентифікація, вплив на конфіденційність, вплив на цілісність, вплив на доступність.

У загальному вигляді, основні дослідження присвячені виявленню атак та методикам захисту. Проте, поза увагою науковців залишається вплив специфічних параметрів соціальних мереж: конфіденційність даних, репутація користувачів мережі, взаємовплив користувачів, довіра між користувачами, спільні думки користувачів мережі, сильні та слабкі зв’язки, сила користувача, або центральність вузлів, швидкість поширення даних в мережі, параметри розширення мережі, кількість співтовариств в мережі, канали поширення інформації, ідентифікація користувачів, на захист інформації у цілому. Більшість наукових досліджень мають описово-дослідницький характер, призначені для вирішення окремих завдань захисту інформації та баз даних і не можуть бути використані як методологічна основа для розробки системи забезпечення захисту інформації.

Існуючі методики та моделі захисту не складають єдину концепцію комплексного забезпечення захисту інформації в соціальних мережах, яка б поєднувала теоретичні методи, методики, моделі та технологічні підходи до захисту інформації у соціальних мережах.

Виходячи з проведеного аналізу, виникає науково-прикладна проблема щодо розробки методологічних основ захисту інформації в соціальних мережах з урахуванням впливу на захист специфічних параметрів мережі. Тому потрібно розробити концепцію захисту інформації у соціальних мережах.

Таким чином, при розробці нових або модернізації існуючих методів та методик захисту інформації в соціальних мережах потрібно застосовувати комплексний підхід до розробки алгоритму захисту інформації. Одночасно враховуючий визначення параметрів захисту, конфігурацію та довженну мережі та всі погрішності обробки сигналів зовнішніх впливів. Для досягнення поставленої мети в роботі використано методи дослідження на основі теорії

графів, множин і системного аналізу (для дослідження функціонування ІСМ, визначення потрібних параметрів СМ, в тому числі, центральності соціальних мереж), теорії когнітивної логіки, управління, ймовірностей, матричного аналізу та математичної статистики (для дослідження процесів взаємодії користувачів у ІСМ, їх взаємного впливу), теорії графів, когнітивної, булєвої алгебри (довіри, репутації, взаємовпливу користувачів), теорії розповсюдження епідемії, теорії графів, множин і системного аналізу (для дослідження поширення інформації в мережі), моделі конкурентного зростання, теорії графів, множин і системного аналізу (для дослідження розширення соціальних мереж), теорії степеневих соціальних мереж, графів, множин (для дослідження середнього шляху та коефіцієнта кластеризації), теорії інформації, синергетики (хаос і структури графів), множин, системного і математичного аналізу, систем моделювання (в основу закладено структурний, ресурсний, нормативний та динамічний принципи) (для дослідження впливів на систему захисту інформації, параметрів системи захисту, їх нелінійної взаємодії). Лінійна модель системи захисту містить параметри традиційних параметрів захисту інформації та специфічні параметри соціальної мережі. При розробці нелінійної математичної моделі системи захисту інформації, зроблено припущення, що не лінійність системи незначна. При розробці математичної моделі взаємодії системи захисту та впливу зроблено припущення, що взаємодія нелінійна та динамічна.

Математична модель стійкості системи захисту та перехідних процесів заснована на моделюванні взаємодії системи захисту та впливів. Модель впливів враховує комплекс параметрів нападу на систему захисту, основана на припущенні, що амплітуда впливу нелінійна в часі. Модель центральності мережі ґрунтується на аналізі параметрів щільності графа, кількості можливих зв’язків, діаметрі графа, валентність вершин відрізняється від розподілу Пуассона. При рішенні нелінійної схеми впливу користувачів прийнято припущення, що степінь впливу кожного користувача не залежить явним чином від об’єктів впливу та пропорційна його відносній репутації. Модель нелінійної взаємодії вершин мережі при приєднанні до них інших вершин заснована на принципі переважного приєднання та припущені, що чим вище валентність вершини, тим швидше вона збільшується. Модель довіри та репутації заснована на припущенні, що між ними існує прямо пропорційна залежність. Модель розширення мережі, ґрунтується на самоорганізації в критичний стан, яка відбувається у відкритих далеких від рівноваги нелінійних системах, та з опорою на початкову цілісність системи і в загальному випадку не вимагає ні не лінійності, ні взаємодії елементів системи між собою.

Таким чином, після рішення завдань розробки та удосконалення моделей та методик захисту інформації буде розроблено методологічні основи захисту інформації в соціальних мережах.

Другий розділ присвячений розробці концепції захисту інформації в соціальних мережах.

На сьогоднішній день не існує одній універсальний концепції захисту інформації в соціальних мережах. Відсутні універсальні методи та методики

захисту інформації в соціальних мережах, які б склали основу концепції. Тому у новій концепції передбачено розробка моделі оцінки стійкості системи захисту інформації, яка базується на аналізі параметрів поведінки системи захисту під час та після зовнішніх впливів на систему захисту даних з урахуванням динаміки зміни параметрів впливу. Розробка методики підвищення рівня захищеності інформаційного простору соціальних мереж, яка базується на результатах аналізу побудованого фазового портрету та аналізу перехідних процесів системи захисту інформації. Удосконалення математичної моделі захисту інформації в соціальній мережі за рахунок врахування динамічних характеристик безпеки системи. Потребує подальшого розвитку математична модель системи захисту інформації в соціальних мережах, яка б дозволила провести об'єктивну оцінку балансу між загрозами безпеки інформації та специфічними параметрами соціальної мережі. Удосконалення математичної моделі та методики підвищення рівня захищеності інформації, яка враховує вплив на систему захисту інформації довіри, репутації, кореляції та коефіцієнта кластеризації мережі.

В даному розділі наводиться пояснення терміну довіра. В вигляді, якому він застосовується в роботі.

Довіра – це складні ментальні відносини позиції довіра когнітивного користувача X (ментальний стан), що характеризують його мислення, по відношенню до обраної суті користувача Y з приводу очікуваної поведінки/дії α, що має значення для досягнення мети G (конкретний стан світу, необхідне і бажане X). Користувач X по суті делегує виконання α.

Визначаються види довіри: Довіра на надання послуг (provision trust) описує довіру. Людина довіряє стороні в наданні якісних послуг провайдером послуг або ресурсів (те, що ми розглядаємо). Довіра делегування (delegation trust) описує довіру в користувача (представника), що діє і виносить рішення від імені сторони, якій довіряє. Як окремий випадок provision trust. Довіра доступу (access trust) описує довіру, що довіряє зі сторони (провайдера) до агентів, яким надається доступ до ресурсів. Це – контроль доступу. Довіра до справжності описує переконання в заявлену справжність користувача. Використовується в системах автентифікації. Контекстна довіра визначає міру віри учасника в необхідні системи та інституційні механізми, що підтримують транзакції і забезпечують безпеку мережі, в тому випадку, якщо щось піде не так (страхування, правова система, правоохоронні органи – теж розглядаються як ситуаційний контекст довіри).

Для розробки концепції використовуються види довіри та їх класифікація. Наводиться класичний варіант моделі захисту інформації:

$$T_i = \left[D_j, D_n, D_m, D_k \right], \tag{4}$$

де T_i – множина загроз від втрати довіри між користувачами, D_j – довіра на надання послуг. Людина довіряє стороні в наданні якісних послуг провайдером послуг або ресурсів, D_n – довіра делегування (delegation trust), що описує довіру в користувача (представника), який діє і виносить рішення від імені

сторони, якій довіряє, D_m – довіра доступу (access trust) описує довіру довіряє зі сторони (провайдера) до користувача, яким надається доступ до ресурсів. Це – контроль доступу. Використовується в системах автентифікації, D_k – контекстна довіра визначає міру віри учасника в необхідні системи та інституційні механізми, що підтримують транзакції і забезпечують безпеку мережі.

Втрата такої якості, як довіра – процес, який має часовий інтервал. Враховуємо, що кількість інформації в системі – I. Потік інформації який витікає за межі інформаційної системи *dI*, швидкість зміни цього потоку – $\frac{dI}{dt}$. Тоді, якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає: $dI = 0; \frac{dI}{dt} = 0$.

Для розробки математичних моделей. Які є складовими концепції захисту інформації в соціальних мережах. Запропонована система рівнянь:

$$\begin{cases} \frac{dI}{dt} = Z_p Z + \varepsilon(C_v + C_K) I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1})\varepsilon \end{cases}, \quad (5)$$

де D_i – коефіцієнт, що відображає вплив загроз безпеки даних від втрати довіри між користувачами на захищеність інформаційної системи; C_{d2} – коефіцієнт, що відображає вплив розмірів системи на захищеність; C_{d1} – коефіцієнт, що відображає вплив захищеності на витік даних, Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації; *Cv* – коефіцієнт, що відображає вплив швидкості витоку даних; C_k – коефіцієнт, що відображає вплив кількості даних на їх витік.

Для вимог, відсутності витоку інформації ($dI = 0; \frac{dI}{dt} = 0$ – умови стаціонарності):

$$\begin{cases} Z_p \bar{Z} + \varepsilon(C_v + C_K)\bar{I} = 0 \\ D_i - I(C_{d2} + Cd_1)\varepsilon = 0 \end{cases}. \quad (6)$$

Кінцеве рівняння визначення захисту інформації при лінійній залежності параметрів довіри та кількості інформації приймають вигляд:

$$\bar{Z} = \frac{(C_v + C_K)D_i)}{(C_{d2} + C_{d1})Z_p}, \quad (7)$$

$$\begin{cases} \bar{I} = \dfrac{D_i}{C_{d2} + C_{d1}} \\ \bar{Z} = \dfrac{(C_v + C_K)D_i}{(C_{d2} + C_{d1})Z_p} \end{cases}. \tag{8}$$

Для нелінійної залежності система рівнянь приймає вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)I - L_2(I_0{}^2 \operatorname{Sin}^2 \omega t) - L_3(I_0{}^3 \operatorname{Sin}^3 \omega t) - ...L_k(I_0{}^k \operatorname{Sin}^k \omega t) \\ \dfrac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) - K_2(Z_0{}^2 \operatorname{Sin}^2 \omega t) - K_3(Z_0{}^3 \operatorname{Sin}^3 \omega t) - ...K_n(Z_0{}^n \operatorname{Sin}^n \omega t) \end{cases} \tag{9}$$

де $I = I_0 \operatorname{Sin} \omega t, Z = Z_0 \operatorname{Sin} \omega t$.

На базі рівнянь (2) та (6) у другому розділі розроблено математичну модель оцінки стійкості системи захисту інформації у соціальних мережах.

Рівняння цфєї моделі представлено у вигляді:

$$\begin{cases} \dfrac{dP}{dt} = \beta P - \gamma IiP - \beta_0 P^2 \\ \dfrac{dI}{dt} = \mu - \alpha Ii + bIiP - \eta\gamma IiP \end{cases} \tag{10}$$

де: $P(t)$ – щільність шкідливих об'єктів;

$Ii(t)$ – імунний статус системи;

β – коефіцієнт швидкості росту шкідливого об'єкта;

γ – коефіцієнт швидкості розпаду шкідливого об'єкта через його взаємодії з імунною системою мережі;

β_0 – коефіцієнт внутрішньовидової інтерференції шкідливих об'єктів;

μ – швидкість зростання імунної системи;

a – коефіцієнт природної швидкості її розпаду;

b – стимулююча швидкість росту імунної системи через її взаємодії з шкідливими об'єктами;

η – коефіцієнт швидкості її розпаду через взаємодію з шкідливим об'єктом;

α – коефіцієнт швидкості росту пошкодженого вузла через шкідливого об'єкта.

На базі цей моделі проведено моделювання визначення поведінки системи захисту під час та після зовнішніх впливів на систему захисту даних з урахуванням динаміки зміни параметрів впливу. Отримані результати приведені на графіках рис.1 – 4.

Графіки параметрів системи захисту при мінімальних значеннях зовнішніх впливів

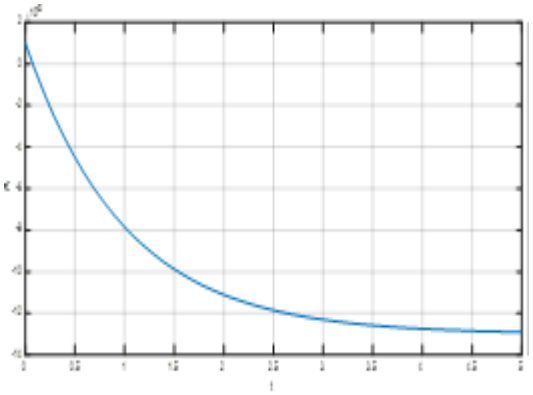

Рис.1. Мінімальне значення амплітуди впливу від часу проведення впливу–всі параметри системи захисту дорівнюють 0,1

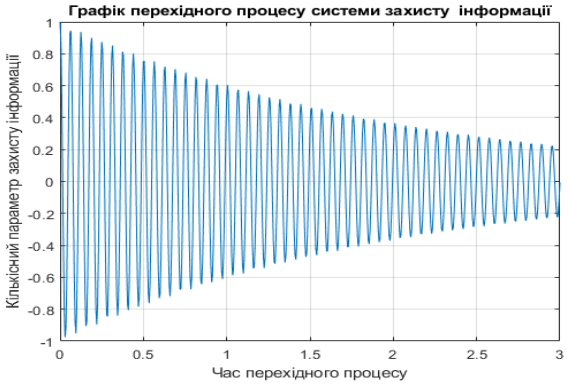

Рис. 2. Перехідний процес системи захисту при відсутності впливів та значенні параметрів системи захисту 0.1.в.о.

Графіки параметрів системи захисту при максимальних значеннях зовнішніх впливів

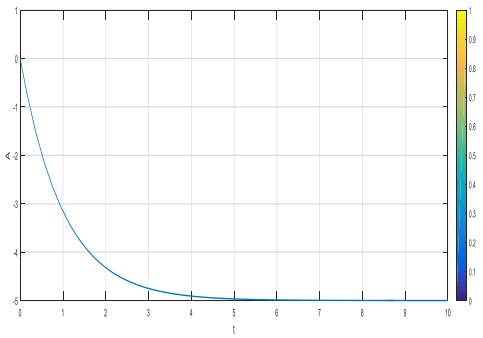

Рис. 3. Максимальне значення амплітуди впливу від часу проведення впливу – всі параметри системи захисту інформації дорівнюють 1 в.о

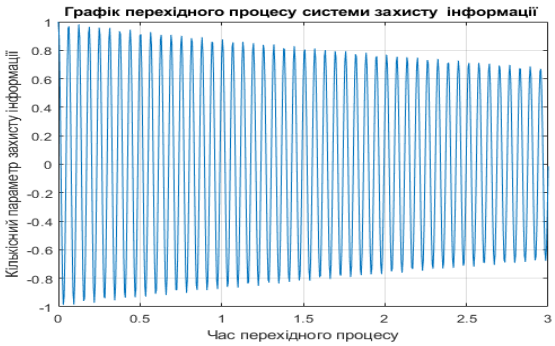

Рис. 4. Перехідний процес системи захисту при мах значенні впливу та значенні параметрів системи захисту інформації 1.в.о.

Розроблена модель дозволяє проводити дослідження параметрів захисту системи від зовнішніх впливів та вживати необхідні заходи для поліпшення системи захисту інформації з урахуванням нелінійної взаємодії елементів системи захисту та зовнішніх впливів.

Удосконалена математична моделі підвищення рівня захищеності інформації, яка отримана у даному розділі базується на врахуванні додаткових параметрів захисту, таких як: щільність інформації, привабливість, взаємодія суб'єктів та ін.

Ще однією особливістю є те, що розрахунок показника захищеності інформації – *Z*, ведеться не за коефіцієнтом витоку інформації, а за швидкістю зміни потоку інформації з урахуванням впливу інших компонентів мережі: наявної кількості діад та тріад, спільнот, і т.п.

Система рівнянь, яка описує захист інформації, після рішення та проведення перетворень, має вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + \varepsilon(C_v + C_K)I \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho)V - I(C_{d2} + C_{d1})\varepsilon \end{cases}, \quad (11)$$

де V_i – коефіцієнт, що відображає вплив загроз безпеки персональних даних, від взаємодії між користувачами, на захищеність інформаційної системи; α – описує схильність суб'єкта до встановлення взаємодії; параметр β – описує привабливість або популярність; θ – щільність графа (оцінка – число ребер L); ρ – характеристика тенденцій моделі до симетричності діад.

Остаточне рівняння моделі з урахуванням впливу додаткових параметрів має вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)I + L_2(I^2) + L_3(I^3) + \ldots + L_k(I^k) \\ \dfrac{dZ}{dt} = (\alpha + \beta + \theta + \rho)V - I(C_{d2} + C_{d1}) + K_2(Z^2) + \ldots + K_n(Z^n) \end{cases}. \quad (12)$$

З метою підтвердження теоретичних результатів, було проведено моделювання процесів, отримані результати представлені на рис. 5.

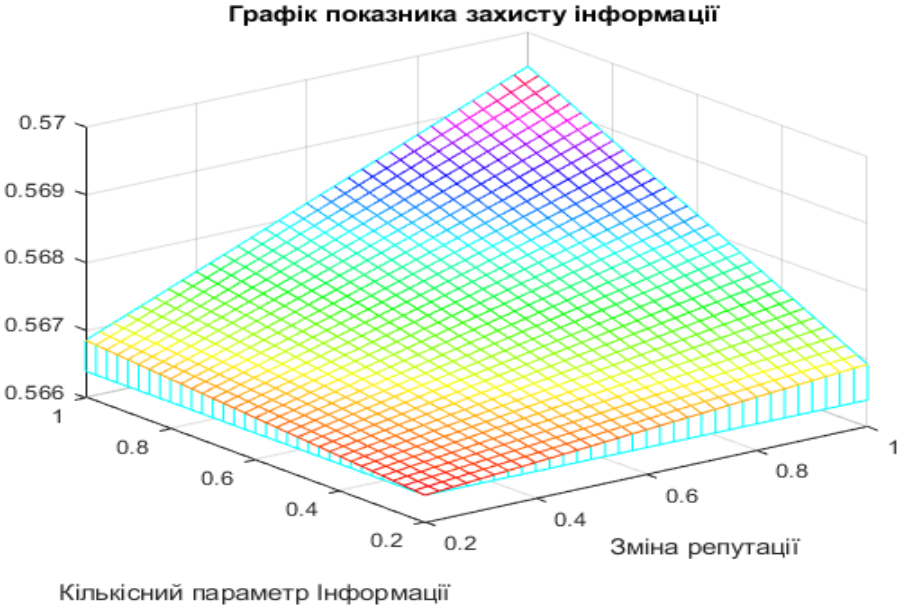

Рис.5. Графік залежності показника захисту інформації, від впливу на систему ситуативних параметрів

Отримані результати підтверджують запропоновані теоретичні розрахунки.

Таким чином удосконалено математичну модель та методику підвищення рівня захищеності інформації, які, на відміну від існуючих, враховують вплив на систему захисту інформації специфічних параметрів: довіри, репутації, кореляції та коефіцієнта кластеризації мережі. Застосування моделі та методики

дозволяє проводити аналіз впливу на систему захисту інформації інших ситуативних параметрів (наявної кількості діад, тріад, спільнот).

Третій розділ присвячено розробці методів та методик підвищення рівня захищеності інформаційного простору соціальних мереж та удосконаленню математичної моделі системи захисту інформації в соціальних мережах.

При розробки цих наукових положень використовується поняття репутації. Можливість впливу одних членів соціальної мережі (СМ) на інших членів суттєво залежить від репутації перших. Репутація – створена загальна думка про переваги та недоліки кого небудь, чого небудь, суспільна оцінка. Репутацію можна розглядати, по-перше, як очікувану іншими користувачами норму діяльності іншого користувача, яку чекають від нього інші; по-друге, вага думки користувача, яка визначається виправданістю його суджень, або ефективністю діяльності.

При розробки моделі були прийняти припущення, що зовнішній вплив на систему захисту має обмеження за амплітудою та часом.

Базове рівняння з урахуванням додаткових параметрів приймає вигляд:

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \tag{13}$$

де $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = \left(\dfrac{\sum\limits_{v \in V} C_{v1}}{N^2}\right)$, $\sum\limits_{v \in V} C_{v1}$ – загальна кількість з’єднань в мережі, N – кількість вершин в мережі.

Рівняння моделі з урахування загальної кількості з’єднань в мережі має вигляд:

$$\frac{d^2 Z}{dt^2} - \beta_1 \frac{dZ}{dt} - \alpha\beta_2 Z = -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \gamma + \\ + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t - \beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \tag{14}$$

де $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = \left(\dfrac{\sum\limits_{v \in V} C_{v1}}{N^2}\right)$

Для оцінки достовірності отриманих результатів. Проведено моделювання процесу визначення стійкості системи захисту від зовнішніх впливів. З цей метою визначено фазовий портрет та проаналізовано перехідний процес системи захисту інформації. На рис. 6. Представлена схема машинного моделювання запропонованої моделі.

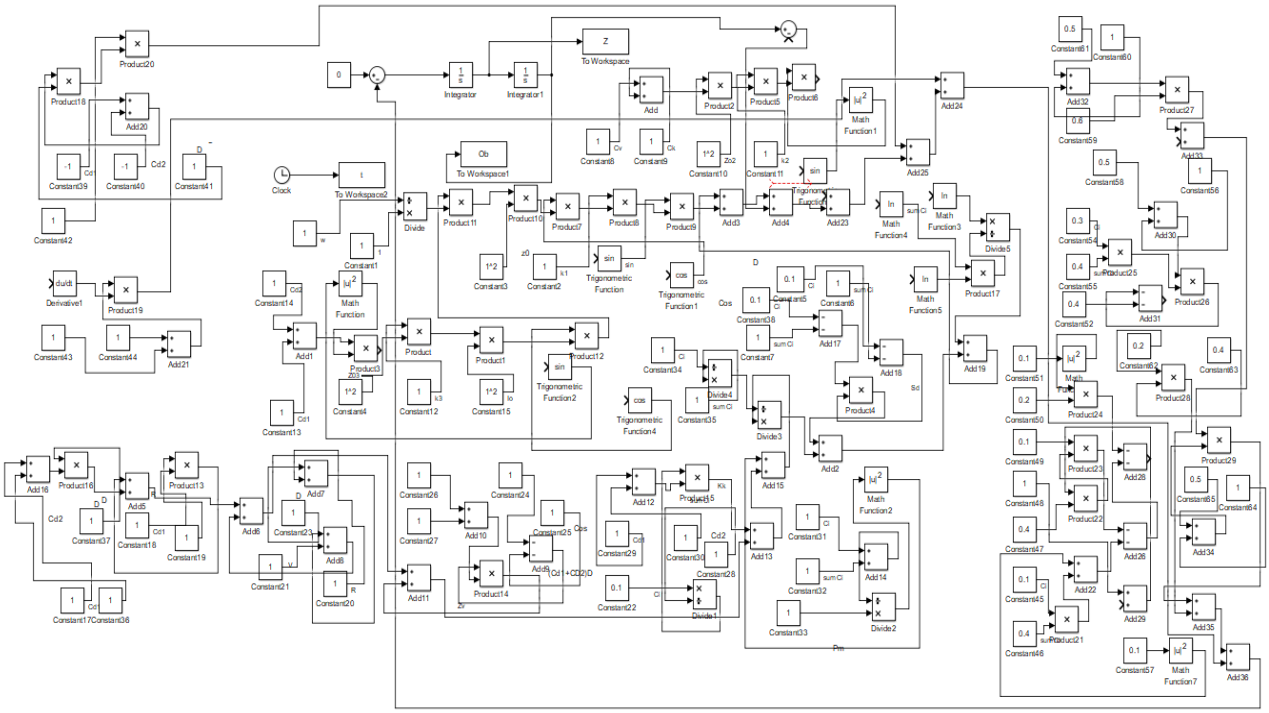

Рис.6. Блок схема моделювання впливу на систему захисту інформації з метою отримання фазового портрету

Результати моделювання представлені на рис. 7 – 10.

Графіки фазових портретів системи захисту інформації в соціальних мережах

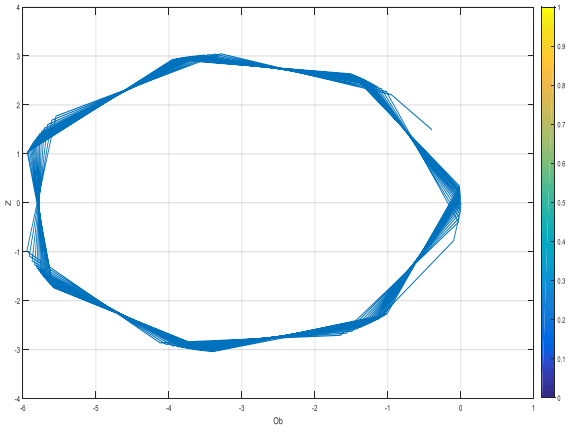

Рис. 7. Фазовий портрет системи захисту при мах значенні впливу та значенні довіри 0.1, репутації 0.01, без взаємодії та кореляції

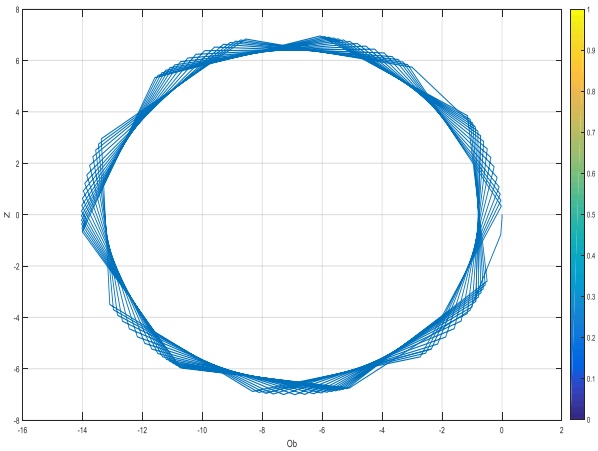

Рис. 8. Фазовий портрет системи захисту інформації при мах значенні впливу та значенні довіри 0.1, репутації 0.01, взаємодії та взаємовпливу – 0.1

Графіки перехідних процесів системи захисту інформації при зовнішніх впливах.

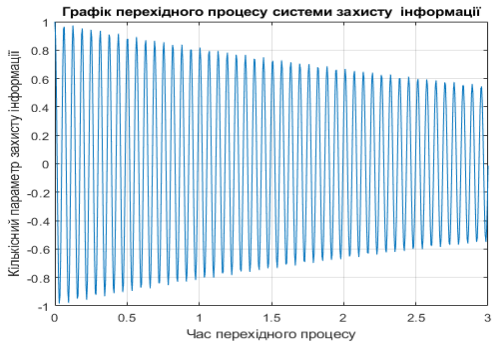

Рис. 9. Перехідний процес системи захисту при мах значенні впливу та значенні довіри 0.1, репутації 0.01, без взаємодії та кореляції

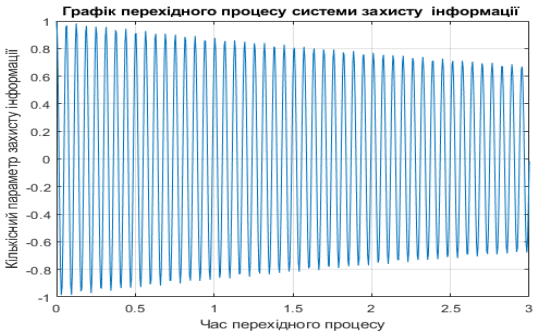

Рис. 10. Перехідний процес системи захисту при мах значенні впливу та значенні довіри 0.1, репутації 0.01, кореляції 0,1

Наступною моделлю цього розділу є модель захисту інформації для лінійних параметрів та нелінійних параметрів зовнішніх впливів на систему захисту інформації.

Для побудови моделі використовуємо наступні вираз:

$$C_D(i) = \sum_{j=1}^{n} a(i, j), \tag{15}$$

де CD (i) – степінь центральності вузла і; $a(i,j)$ – зв'язок між вершинами i та j, n – число вершин в мережі.

Нормована характеристика визначається наступним чином:

$$C_D(i) = \frac{C_D(i)}{n-1}. \tag{16}$$

Нормована степінь центральності вузла і є аналогом індексу соціометричного статусу члена групи (C_i), а нормована ступінь вихідної центральності вузла є аналогом індексу емоційної експансивності члена групи.

Для порівняння різних структур і визначення, яка з них забезпечує найкращу централізацію, будемо знаходити степінь центральності за формулою Фрімана:

$$C_D = \frac{\sum_{i=1}^{n} (C_D'(i) - C_D(i))}{(n-1)(n-2)}. \tag{17}$$

Центральність в цьому випадку розглядається, як контроль зв'язків між певними позиціями, і визначається числом індивідуумів, які повинні будуть пройти через цей вузол.

При створені моделі нами було застосовано припущення: система інформаційного сховища має границі.

Система рівнянь з урахуванням додаткових параметрів для лінійної системи приймає вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I - L_2(I^2) - ... - L_k(I^k) \\ \dfrac{dZ}{dt} = DR - I(C_{d2} + C_{d1}) - K_2(Z^2) - ... - K_n(Z^n) \end{cases} \quad (18)$$

$$I = I_1 + I_2 + ... + I_k;\ Z = Z_1 + Z_2 + ... + Z_n$$

де Cv – коефіцієнт, що відображає вплив репутації системи на захищеність інформації;

C_k– коефіцієнт, що відображає вплив довіри на витік інформації;

C_{d1} – коефіцієнт, що відображає вплив розмірів системи на захищеність;

C_{d2} – коефіцієнт, що відображає вплив захищеності на витік персональних даних;

$L_2, L_3 \cdots L_n$ та $K_2, K_3 \cdots K_n$ – лінійні оператори;

D – коефіцієнт, що відображає вплив репутації системи на захищеність інформації;

R– коефіцієнт, що відображає вплив довіри на витік інформації.

Система рівнянь з урахуванням додаткових параметрів для нелінійної системи приймає вигляд:

$$\begin{cases} \dfrac{dI}{dt} = Z_p Z + (C_v + C_K) I - L_2(I_0^2 \operatorname{Sin}^2 \omega t) - ... - L_k(I_0^k \operatorname{Sin}^k \omega t) \\ \dfrac{dZ}{dt} = DR - I(C_{d2} + C_{d1}) - K_2(Z_0^2 \operatorname{Sin}^2 \omega t) - ... - K_n(Z_0^n \operatorname{Sin}^n \omega t) \end{cases} \quad (19)$$

$$I = I_0 \operatorname{Sin} \omega t, Z = Z_0 \operatorname{Sin} \omega t$$

Рівняння моделі з урахуванням впливу додаткових параметрів (репутації):

$$\frac{d^2 Z}{dt^2} = \beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t - \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \gamma + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \quad (20)$$

де $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = DR$.

Для розробки моделі захисту інформації в залежності від параметра зростання мережи будемо використовувати наступні вирази, визначення та обмеження.

Ймовірність утворення зв'язку з даною вершиною приймається пропорційною x^z, оскільки немає підстав вважати наявність будь-яких характерних масштабів для даного процесу, що означає можливість використання тільки однорідних функцій x.

При випадковому приєднані ймовірність того, що зв'язок буде створений з даної вершиною, не залежить від її характеристик і дорівнює $\frac{1}{n(t)}$, де $n(t)$ – загальне число вершин графа в момент часу t. При переважному приєднані ймовірність утворення зв'язку з вершиною i, яка вже має x_i зв'язків дає відношення $x_i/S(t)$ де сумарна валентність $S(t)=\sum_{i=1}^{n(t)} x_i(t)$.

Середня швидкість росту валентності вершини i описується рівнянням:

$$\frac{dx_i}{dt}=\frac{p_0+s_0}{n(t)}+\frac{x_i(p_1+s_1)}{S(t)}. \tag{21}$$

Підсумовуючи рівняння за всіма наявними, а також тими вершинами, що приєднуються, отримаємо рівняння для зростання сумарної валентності:

$$\frac{dS}{dt}=(2p_0+s_0)+(2p_1+s_1). \tag{22}$$

З урахуванням отриманих формул закон зростання вершин може бути переписаний у вигляді системи рівнянь:

$$\frac{dx_i}{dt}=f(x_i,t)=\frac{g(x_i)}{2(p+s)}x, \tag{23}$$

де

$$g(x)=\frac{p_0+s_0}{p}+\frac{p_1+s_1}{2(p+s)}x, \tag{24}$$

Використовуючи вище зазначені вирази та припущення, отримуємо остаточне рівняння.

Рівняння з урахуванням кількості зв’язків вершин у визначений момент часу:

$$\begin{aligned}\frac{d^2Z}{dt^2}=\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\\ -\beta_1\gamma\vartheta+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t,\end{aligned} \tag{25}$$

де $\vartheta=\frac{1}{n_i}+\frac{x_1}{\sum_{i=1}^{n}x_i}$, n – кількість вершин в мережі в момент часу t, x_i – кількість зв’язків які має вершина мережі в момент часу t.

Графічні матеріали моделювання математичної моделі системи захисту інформації в соціальних мережах представлені на рис. 11 та рис. 12.

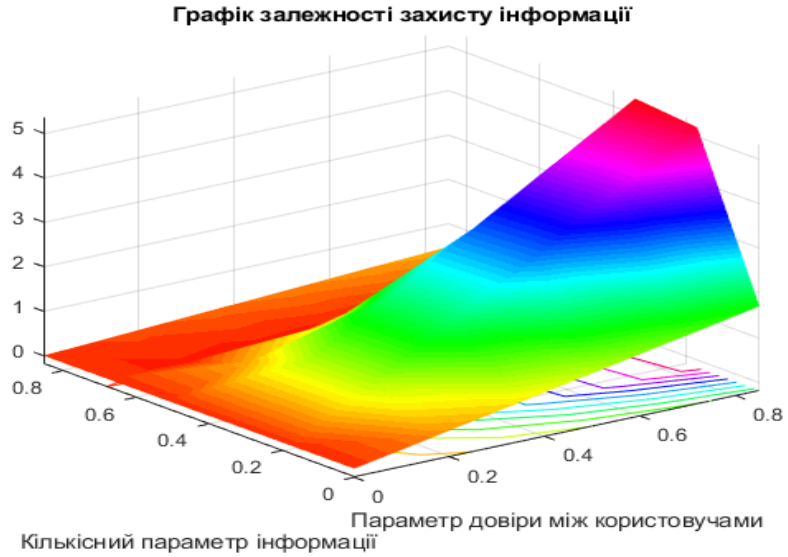

Рис. 11. Залежність показника захисту інформації від параметрів комплексних показників мережі та величини потоку інформації

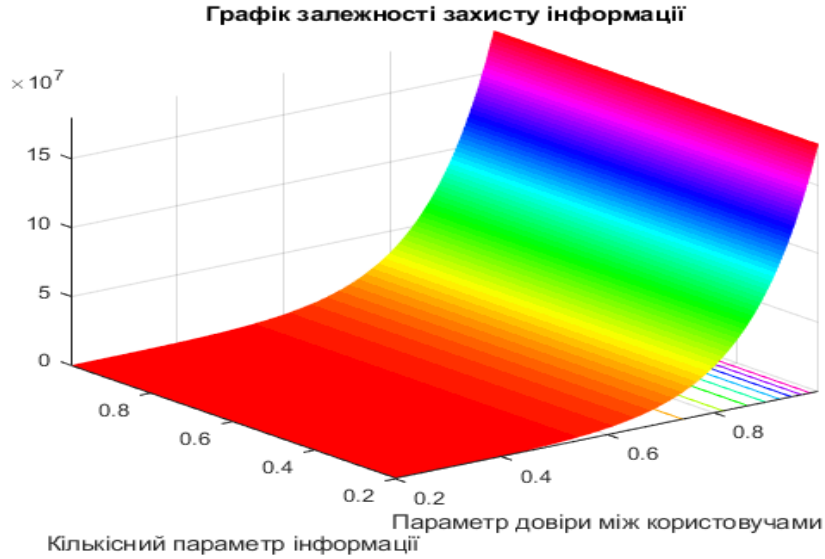

Рис. 12. Залежність показника захисту інформації від параметрів: розширення мережи та коефіцієнта кореляції

Таким чином отримані результати підтвердили теоретичні викладки застосування математичної моделі системи захисту інформації в соціальних мережах, яка на відміну від існуючих, враховує розширення мережі, параметр розповсюдження інформації й коефіцієнт кореляції та дозволяє провести об'єктивну оцінку балансу між загрозами безпеки інформації й специфічними параметрами соціальної мережі, що, в свою чергу, дає можливість змінювати рівень доступу до інформації користувача в залежності від репутації оточення.

Четвертий розділ присвячено розробці математичної моделі та методики захисту в соціальних мережах з урахуванням параметрів центральності та динамічних характеристик системи захисту.

Міра центральності описує випуклість конкретного вузла в порівнянні з іншими вузлами. Середня міра центральності – це централізована оцінка, яка вказує, наскільки щільний граф по відношенню до кожного вузла.

Формально ступінь центральності вузла можна представити в наступному вигляді:

$$C_D(i) = \sum_{j=1}^{n} a(i, j), \tag{26}$$

де CD (i) – степінь центральності вузла i; $a(i,j)$ – зв'язок між вершинами i та j, n – число вершин в мережі; $a(i,j)$ =1 тоді коли вершини з'єднані ребром.

Щоб можна було порівнювати степінь центральності вузла не тільки всередині одного графа, але і між графами різної структури, необхідно розрахувати нормовану центральність вузла

$$C_D^{/}(i) = \frac{C_D(i)}{n-1}, \tag{27}$$

де $C'D(i)$ – нормована степінь центральності вузла i; $CD(i)$ – степінь центральності вузла i; n – число вершин в мережі. Величина $C'D(i)$ змінюється в інтервалі від 0 до 1 і говорить про те, наскільки добре вершина i безпосередньо пов'язана з усіма іншими вершинами мережі. Нормована степінь центральності вузла i є аналогом індексу соціометричного статусу члена групи (C_i), а нормована ступінь вихідної центральності вузла є аналогом індексу емоційної експансивності члена групи.

Щоб мати можливість порівняти різні структури і визначити, яка з них забезпечує найкращу централізацію вузлів, знаходять степінь центральності всього графа за формулою:

$$C_D = \frac{\sum_{i=1}^{n} (C_D^{'}(i) - C_D(i))}{(n-1)(n-2)}, \tag{28}$$

де C_D – степінь центральності всього графа; $C_D^{'}(i)$ – максимальний ступінь центральності вузла в мережі; $C_D(i)$ – степінь центральності вузла i; n – число вершин в мережі.

Центральність як посередництво (betweenness). Центральність вузла в цьому випадку розглядається, як контроль зв'язків між певними позиціями. Вона визначається числом індивідуумів, які повинні будуть пройти через цей вузол, щоб досягти іншої позиції та описується виразом:

$$C_B(i) = \sum_{j-k} \frac{g_{jk}(i)}{g_{jk}}, \tag{29}$$

де $C_B(i)$ – центральність як посередництво вузла i; $g_{jk}(i)$ – число найкоротших шляхів, що з'єднують j і k та проходять через вершину i; g_{jk} – загальна кількість коротких ребер, що з'єднують j і k.

Для розробки моделі використовується вхідна система рівнянь:

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \tag{30}$$

де $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = \dfrac{\sum\limits_{i=1}^{n} (C_D{}'(i) - C_D(i))}{(n-1)(n-2)}$.

Після перетворення та розв'язання цих рівнянь, остаточні рівняння математичної моделі з урахуванням впливу додаткових параметрів:

$$Z(t) = \int N(t) e^{\frac{-\beta_1 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t} \frac{e^{\frac{\beta_1 + \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}} dt - \int N(t) - \frac{e^{\frac{\beta_2 - \sqrt{\beta_1^2 + 4\alpha\beta_2}}{2} t}}{\sqrt{\beta_1^2 + 4\alpha\beta_2}}. \tag{31}$$

Для розробки моделі захисту інформації від подовження мережі додатково використовуються вираз для середньої довжини шляху інформації з моделі Барабаша–Альберта (БА). Середня довжина шляху збільшується в середньому, як логарифм розміру мережі. Точна форма має подвійну логарифмічну поправку і виглядає, як: $l \sim \dfrac{\ln N}{\ln \ln N}$.

Базова система рівнянь прийме вигляд:

$$\begin{cases} \dfrac{dI}{dt} = \alpha Z + \beta_1 I - \sum\limits_{k=2}^{\infty} L_k I_0^k \sin^k \omega t, \\ \dfrac{dZ}{dt} = \beta_2 I + \gamma\theta - \sum\limits_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t, \end{cases} \tag{32}$$

де $\alpha = Z_p$, $\beta_1 = C_v + C_K$, $\beta_2 = -\left(C_{d2} + C_{d1}\right)$, $\gamma = \dfrac{\sum\limits_{i=1}^{n} (C_D{}'(i) - C_D(i))}{(n-1)(n-2)}$, $\theta = \left(\dfrac{\ln \ln n - n}{n(\ln \ln n)^2}\right)$.

Після перетворення та розв'язання цих рівнянь, остаточне рівняння моделі з урахуванням впливу додаткових параметрів набуло вигляд:

$$\begin{aligned} N(t) = -\frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) - \beta_1 \gamma\theta + \beta_1 \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t - \\ - \beta_2 \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t. \end{aligned} \tag{33}$$

Для підтвердження коректного використання математичного апарату та обґрунтування теоретичних положень. В дисертації проведено моделювання з використанням розробленої моделі з метою збіжності теоретичних результатів з результатами моделювання процесу захисту інформації в соціальних мережах.

Результати моделювання для різних складових параметрів захисту та зовнішніх впливів представлені на рис. 13 – 16.

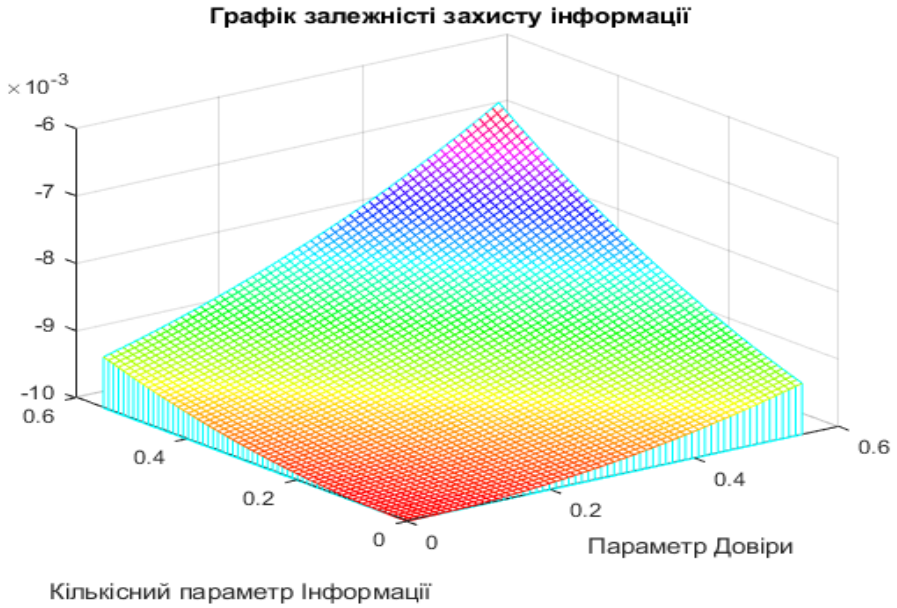

Рис. 13. Залежність показника коефіцієнту захисту від параметра довіри та величини потоку інформації

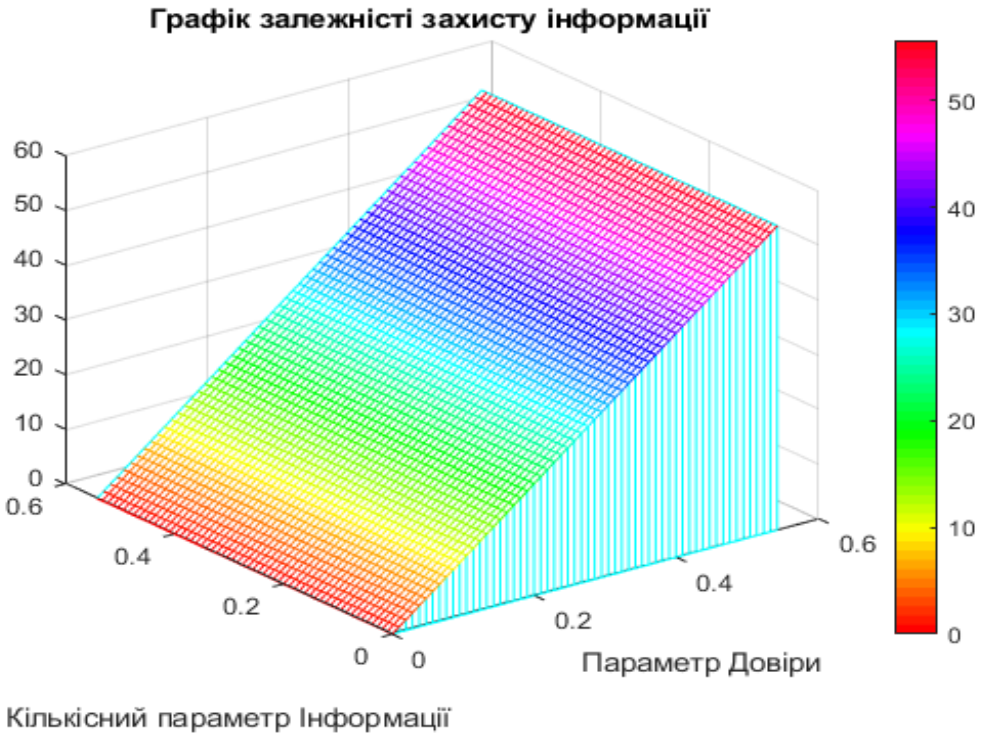

Рис.14. Залежність показника коефіцієнту захисту від середньої довжини шляху між користувачами та величини потоку інформації

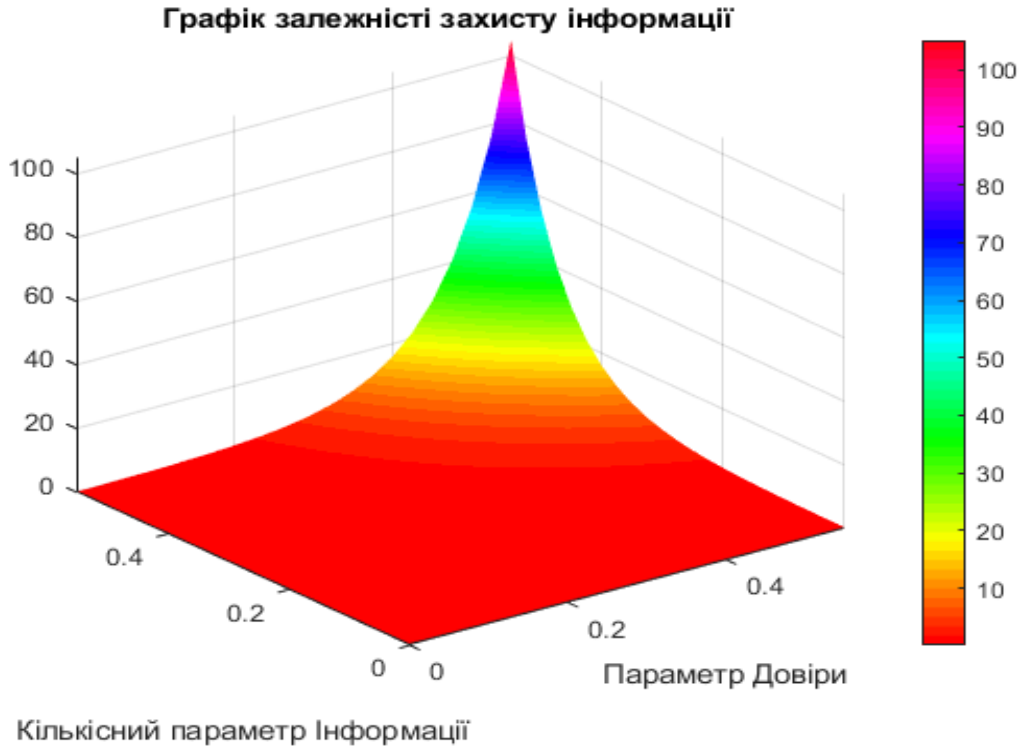

Рис. 15. Залежність показника коефіцієнту захисту інформації від параметра репутації та величини потоку інформації

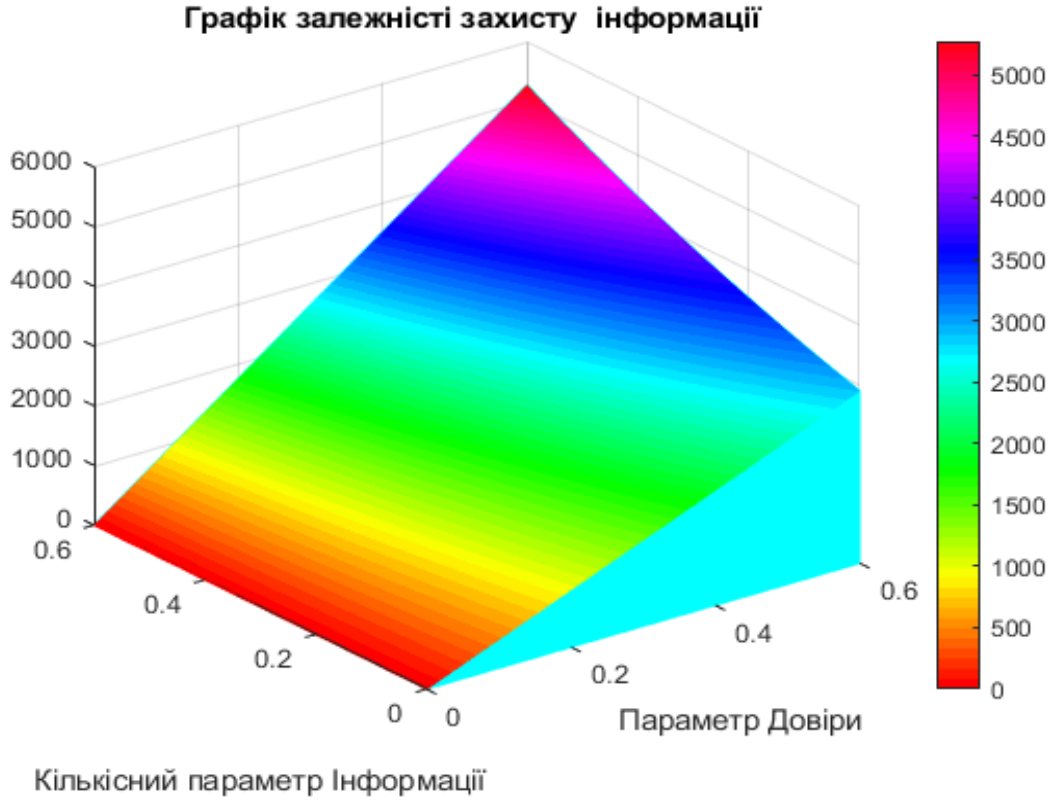

Рис.16. Залежність показника коефіцієнта захисту інформації від середньої довжини шляху між користувачами та величини потоку інформації

Таким чином удосконалено удосконалено математичну модель захисту інформації в соціальній мережі на основі динамічних характеристик безпеки

системи, яка, на відміну від існуючих моделей, має зворотний зв'язок за такими параметрами, як, розмір системи, кількість даних та їх достовірність. Реалізація удосконаленої моделі дозволяє динамічно змінювати параметри захисту користувачів мережі в залежності від інтенсивності атак та заданого рівня захищеності інформації. Отримані результати моделювання підтвердили адекватність отриманих теоретических результатів.

П'ятий розділ присвячений оцінці та визначенню ефективності захисту даних з урахуванням одночасно дії багатьох параметрів мережі. Крім того, в розділі розроблено рекомендацій щодо застосування отриманих наукових положень та результатів. Визначено переваги розробленої методології та проведено оцінку достовірності запропонованих наукових результатів.

Методологічні основи захисту інформації в соціальних мережах являють собою сукупність концептуальних, теоретичних та технологічних основ. Концептуальні основи складаються з концептуальних положень та визначень. Теоретичні основи складаються з математичних моделей, методів та методик. Технологічні основи складаються з практичних рекомендацій та практичного використання методик та технологій.

Структура метологічних основ забеспечення защисту інформації у соціальних мережах представлена на рис. 17:

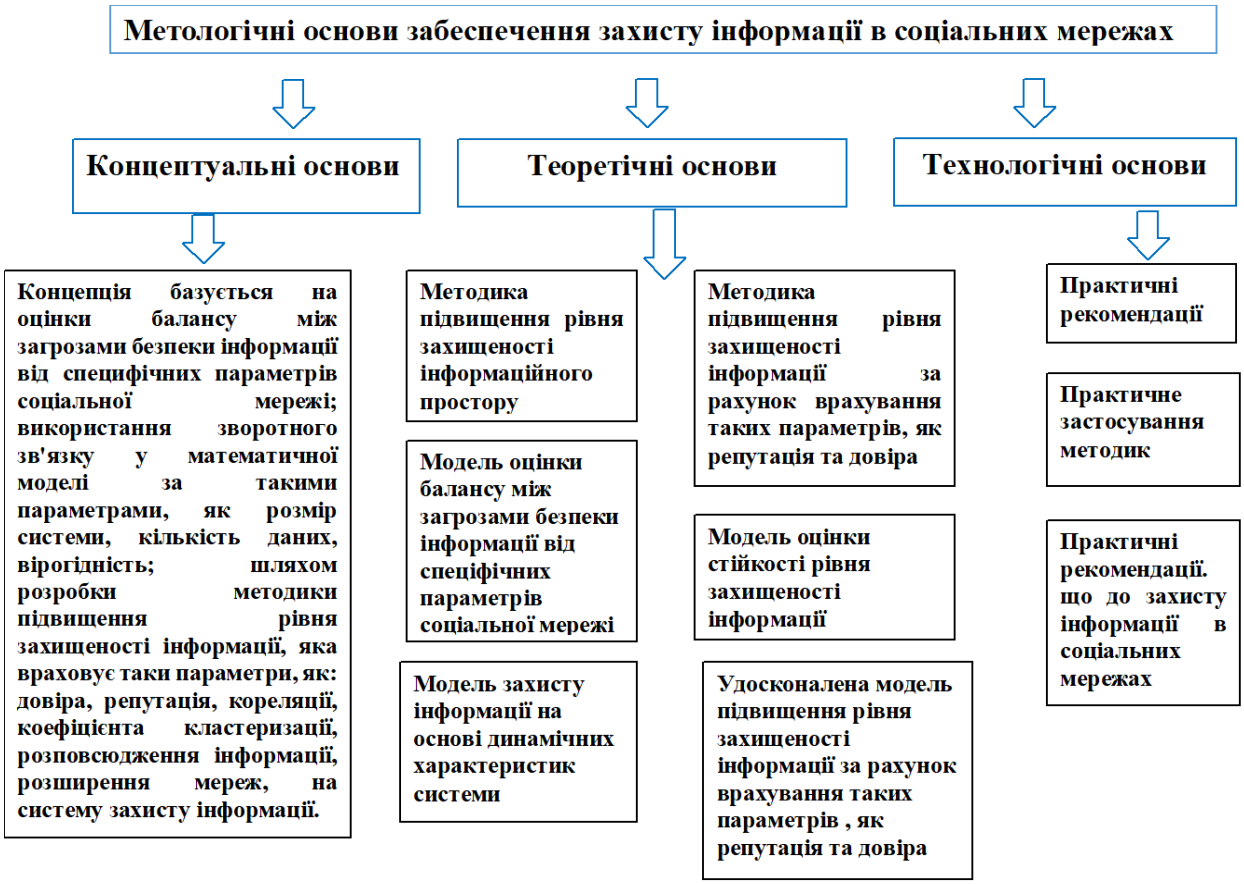

Рис. 17. Методологічні основи захисту інформації в соціальних мережах

Концептуальні положення визначають стратегічні шляхи удосконалення та розробки метологічних основ. Вони заклали основні напрямки розвитку

методології захисту інформації в соціальних мережах. Основні переваги розроблених метологічних основ захисту інформації на шляху стратегічних напрямків розвитку систем захисту інформації мають теоретичні основи, які складаються з методів, математичних моделей та методик захисту інформації в соціальних мережах.

На основі методів та методик, які запропоновані у другому третьому та четвертому розділах, здійснено розрахунки параметрів захисту інформації в соціальних мережах. За результатами моделювання побудовані графіки, гістограма ймовірностей захисту інформації в соціальних мережах.

Для перевірки достовірності запропонованих наукових результатів використаємо, виведене у роботі, остаточне рівняння оцінки захисту інформації в соціальних мережах, яке задається наступним чином:

$$K_z = \frac{\sum_{i=1}^{n}(C_D^{'}(i) - C_D(i))}{(n-1)(n-2)} + D + DR + (t*(r+1)\wedge(-f)) - (\frac{\sum_{v\in V} C_{v1}}{n^2}) + \\ + (P-N)*(P+N) + ((\alpha+\beta+\theta+\rho)V) + \\ + (\frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i}) + (\log(n)/Log(n)*\log(n)), \quad (34)$$

де D_i – коефіцієнт, що відображає вплив загроз безпеки даних від втрати довіри між користувачами на захищеність інформаційної системи; DR – коефіцієнт, що відображає вплив загроз безпеки даних від втрати репутації між користувачами на захищеність інформаційної системи; $(t*(r+1)\wedge(-f))$ – коефіцієнт, що відображає вплив загроз безпеки даних від розповсюдження інформації між користувачами на захищеність інформаційної системи; $(\frac{\sum_{v\in V} C_{v1}}{n^2})$ – коефіцієнт, що відображає вплив загроз безпеки даних від коефіцієнта кластеризації мережі на захищеність інформаційної системи; $(P-N)*(P+N)-$коефіцієнт, що відображає вплив загроз безпеки даних від взаємовпливу користувачів на захищеність інформаційної системи; $(\alpha+\beta+\theta+\rho)V-$коефіцієнт, що відображає вплив загроз безпеки даних від взаємодії користувачів на захищеність інформаційної системи; $(\frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i})-$ коефіцієнт, що відображає вплив загроз безпеки даних від розширення мережі на захищеність інформаційної системи; $\ln(n)/ln\ln(n)-$ коефіцієнт, що відображає вплив загроз безпеки даних від довжини шляху між користувачами на захищеність інформаційної системи.

Моделювання проведемо в програмному серидовищі MatLab/Multisim. Отримані результати представлено на рис. 18 – 21.

Графіки перехідного процесу та фазового портрету системи захисту інформації без зовнішніх впливів.

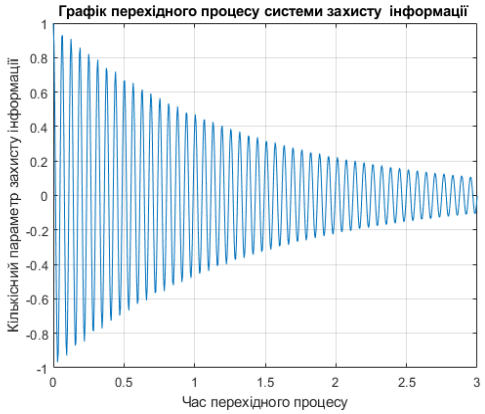

Рис. 18. Гармонійні коливання системи захисту інформації від часу $Z=f(t)$, без впливу на нею

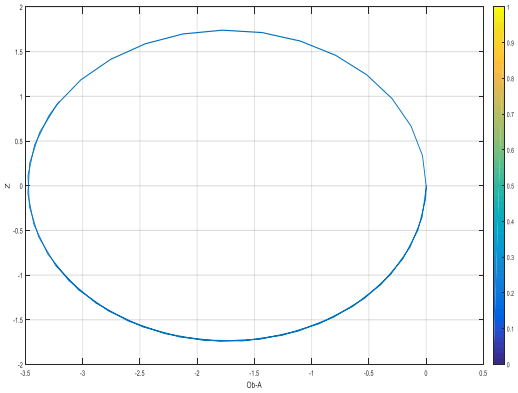

Рис. 19. Фазовий портрет системи захисту інформації без зовнішніх впливів на неї

Як випливає з аналізу отриманих графічних результатів перехідний процес та фазовий портрет доводять, що система захисту інформації стійка.

Графіки перехідного процесу та фазового портрету системи захисту інформації при наявності зовнішніх впливів.

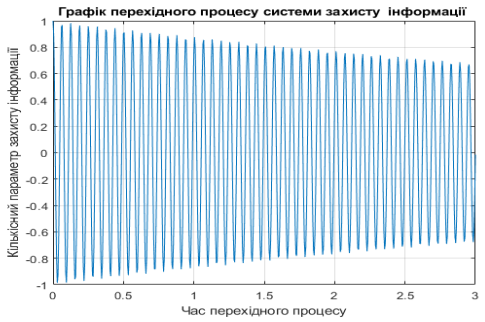

Рис. 20. Перехідний процес системи захисту при наявності зовнішнього впливу на систему захисту інформації

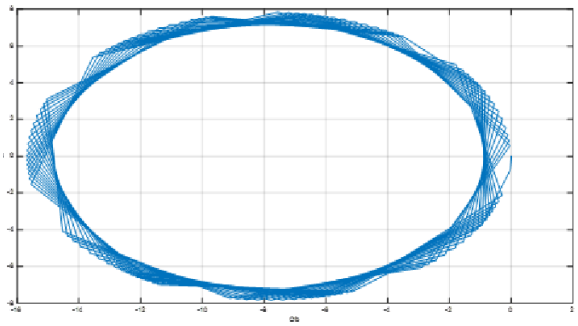

Рис. 21. Фазовий портрет системи захисту інформації при наявності зовнішнього впливу на систему захисту інформації

З аналізу отриманих графічних результатів перехідний процес має затухаючій характер, фазовий портрет представлений в вигляді еліпса, що вказує на стійкість системи захисту даних до зовнішніх впливів.

На основі методів та методик, які запропоновані у другому, третьому та четвертому розділах, здійснено моделювання. За результатами моделювання побудовані графіки та гістограма ймовірностей противодії впливу на систему захисту репутаційних параметрів побудовану за існуючим та розробленим методом наведена на рис. 22.

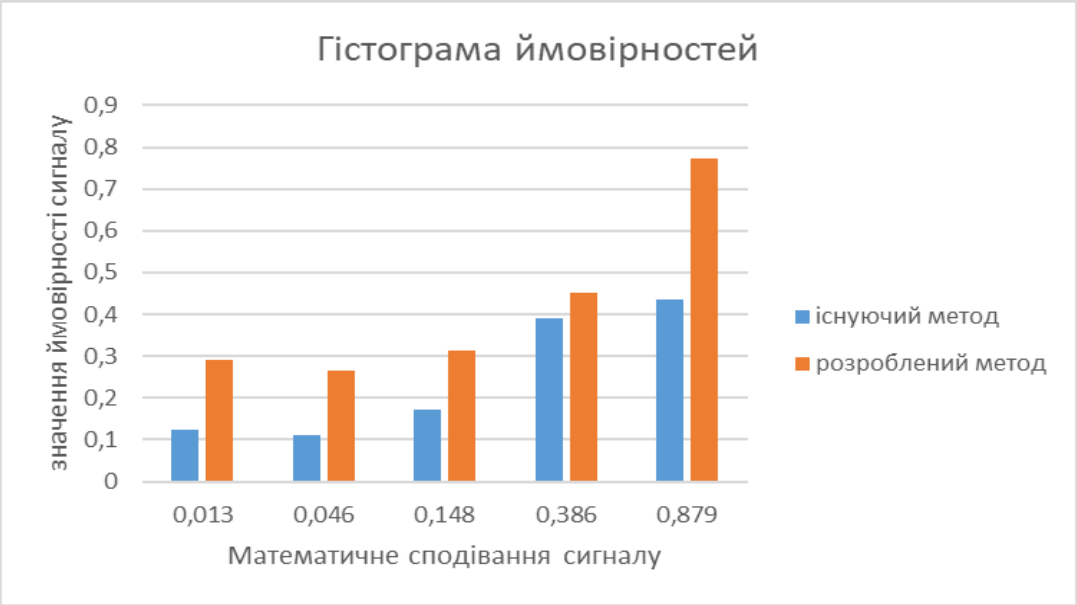

Рис.22. Гістограма ймовірностей протиодії впливу на систему захисту, побудовану за існуючим та розробленим методом

З аналізу рис. 22 бачимо, що перевага нової методики над існуючою, за параметром впливу на захист інформації репутаційних параметрів, близько 40 %. Реалізація розроблених методологічних основ захисту інформації в соціальних мережах дозволяє підвищити ймовірність протиодії впливу на систему захисту побудовану за існуючим та розробленим методом.

Для оцінки ймовірності захисту інформації в соціальних мережах, будемо використовувати нормальний закон розподілу, якій характеризується ймовірністю вигляду:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp[-\frac{(x - m_x)^2}{2\sigma^2}]. \qquad (35)$$

де σ – середньоквадратичне відхилення випадкової величини; m_x – математичне очікування випадкової величини.

Тобто в теорії ймовірностей нормальний закон (закон Гаусса), є граничним законом, до якого наближаються (за певних умов) інші закони розподілу.

У зв’язку з цим для оцінки ймовірності захисту інформації в соціальних мережах, будемо припускати, що процес пошуку підпорядковується нормальному закону розподілу випадкової величини.

Дані припущення отримали повне підтвердження в дослідженнях відомих вчених, в роботах яких був розроблений програмний комплекс для визначення закону розподілення зовнішніх впливів на систему захисту інформації.

Для наглядного представлення отриманих результатів побудуємо графіки для значеннн захисту даних.

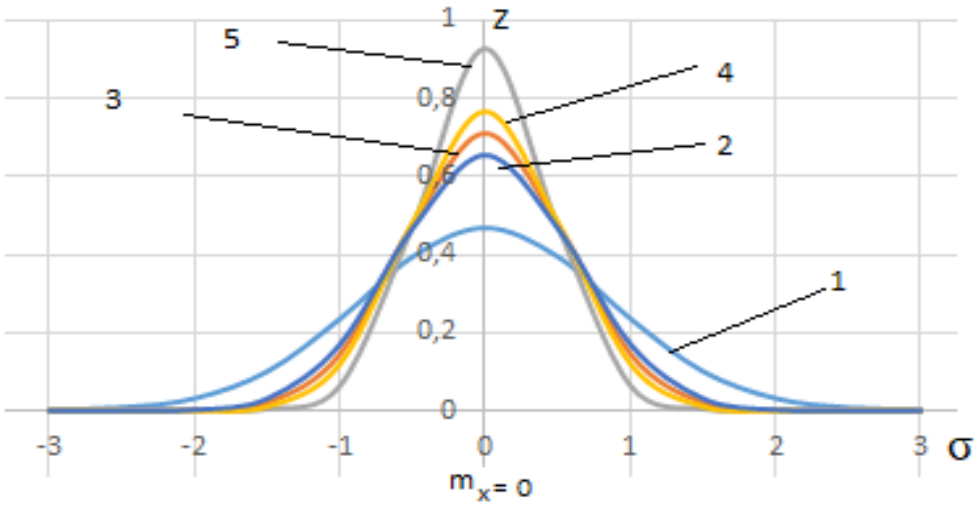

Рис. 23. Графік щільності розподілу ймовірної величини захисту інформації при різних значеннях σ: 1 – веб-додатків та робочих станції співробітників; 2 – даних; 3 – ключових серверів; 4 – в мережі; 5– за розробленою методикою

Відповідно до отриманих графіків щільності розподілу ймовірної величини захисту інформації бачимо, що максимальна ймовірність захисту інформації за існуючої методикою відносно захисту ключових серверів – 76 %, за розробленою – 90 %, тобто різниця складає 14 %; відносно порушення працездатності мережі відповідно 71 % та 90 %, різниця 19%; відносно даних – 65 % та 90 %, різниця 25 %; відносно порушення роботи веб-додатків та робочих станцій співробітників – 44 % та 90 %, різниця 46 %.

З наведених графіків, можна зробити висновок, що середнє значення захисту інформації за допомогою розробленої методики збільшений на 10,5 – 12 %.

Як показано раніше, забезпечення захисту інформації в соціальних мережах виконується «класичними методами» з використанням, маршрутизаторів, брандмауерів, антивірусного програмного забезпечення, підмереж захисту, методів доступу і т.п. При цьому не враховують вплив специфічних параметрів СМ (конфіденційність даних, репутація користувачів мережі, взаємовплив користувачів, довіра між користувачами, спільні думки користувачів мережі, сильні та слабкі зв’язки, сила користувача, або центральність вузлів, швидкість поширення даних в мережі, параметри розширення мережі, кількість співтовариств в мережі, канали поширення інформації, ідентифікація користувачів і т.п.). Крім того, оцінка стійкості системи захисту, перехідних процесів проводиться емпіричним шляхом або акцент робиться на загальних аспектах і методах виявлення загроз та захисту даних користувачів. Більшість наукових досліджень мають дескриптивний

характер, що розглядають окремо із різних математичних та технічних напрямків.

На думку соціологів «нема довіри між користувачами СМ немає й захисту даних», якщо перекласти на мову математики. Якщо довіра між користувачами дорівнює нулю, то й захист інформації дорівнює нулю. Тобто СМ не працездатна. У випадку коли репутація деяких користувачів дуже низька, то ігноруючи їх інші користувачі таким чином виключають їх з соціальних процесів в СМ і т.п.

Проведені дослідження, які розкриті в попередніх розділах наочно доводять переваги врахування при розробці систем захисту даних в СМ специфічних параметрів СМ, користувачів, врахування атак на систему захисту, визначення параметрів стійкості та перехідних процесів.

Визначення впливу кожного окремого параметра СМ на систему захисту та комплексного впливу всіх параметрів з урахуванням можливих атак дозволяють прогнозувати та розраховувати вказані параметри СМ, що важливо при створені нових СМ та модернізації існуючих.

Розробнику СМ достатньо застосувати вказану методологію, щоб отримати потрібні результати, які добре зрозумілі, не потребують застосування складного обладнання та програмного забезпечення для процесу обчислень.

Таким чином, розроблені методологічні основи захисту інформації в соціальних мережах з урахуванням впливу на захист специфічних параметрів мережі в рамках розробленої концепції перевершують існуючі методи та методики, які використовуються у сучасних соціальних мережах та наукових дослідженнях.

ВИСНОВКИ

В результаті дисертаційних досліджень вирішена актуальна науково–прикладна проблема, що полягає у створенні методологічних основ захисту інформації в соціальних мережах на основі запропонованих математичних моделей захисту інформації в соціальній мережі, визначення стійкості системи захисту даних (на основі фазових портретів), та стійкості системи до можливих атак, на підставі яких може бути проведена об’єктивна оцінка балансу між загрозами безпеки інформації та специфічними параметрами соціальної мережі з врахуванням їх нелінійної взаємодії, атаками та заходами щодо захисту і обсягом даних, що захищається. Застосування розроблених методологічних засад побудови системи забезпечення безпеки даних користувачів у соціальних мережах дозволить по новому поглянути на вже існуючі соціальні мережі (модернізація їх структури, параметрів, взаємодії користувачів) та створювати нові соціальні мережі, які забезпечать більш надійний захист інформації даних

користувачів при збережені параметрів використання. Відсутність аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

В дисертації одержані такі основні наукові результати:

1. На підставі проведеного аналізу існуючих методів захисту даних виявлено, що при аналізі та синтезі системи захисту не враховуються специфічні параметри соціальних мереж. Тому, на даний час в практиці і теорії побудови та використання соціальних мереж існує об’єктивне протиріччя між необхідністю підвищення рівня захищеності інформації та недосконалістю системи захисту інформації і можливостями існуючих методів які використовуються системою захисту інформації в соціальних мережах. Відтак, актуальною є науково–прикладна проблема щодо щодо розробки методологічних основ забезпечення захисту інформації в соціальних мережах.

2. Вперше розроблено концепцію комплексного забезпечення захисту інформації в соціальних мережах, яка поєднує теоретичні методи, методики, моделі та технологічні підходи до захисту інформації у соціальних мережах. Концепція базується на: оцінці балансу між загрозами безпеки інформації від специфічних параметрів соціальної мережі; математичній моделі зворотного зв'язку з урахуванням розміру системи, кількості даних та достовірності; методиці підвищення рівня захищеності інформації з урахуванням коефіцієнтів довіри, репутації, кореляції, кластеризації, розповсюдження інформації та розширення мереж. Реалізація запропонованої концепції дозволяє забезпечити перехід від організаційно-технічної до структурно-організаційної технології захисту інформації в соціальних мережах.

3. Вперше розроблено математичну модель оцінки стійкості системи захисту інформації у соціальних мережах, яка базується на аналізі параметрів поведінки системи захисту під час та після зовнішніх впливів на систему захисту даних з урахуванням динаміки зміни параметрів впливу. Модель дозволяє проводити дослідження параметрів захисту системи та вживати необхідні заходи для поліпшення системи захисту інформації з урахуванням нелінійної взаємодії елементів системи захисту та зовнішніх впливів.

4. Вперше розроблено методику підвищення рівня захищеності інформаційного простору соціальних мереж, яка базується на результатах аналізу побудованого фазового портрету та аналізу перехідних процесів системи захисту інформації. Методика дозволяє ефективно досліджувати перехідні процеси з можливістю візуалізації моделей (блок – схем) і результатів дослідження.

5. Удосконалено математичну модель захисту інформації в соціальній мережі на основі динамічних характеристик безпеки системи, яка, на відміну

від існуючих моделей має зворотний зв'язок за такими параметрами, як, розмір системи, кількість даних та їх достовірність. Реалізація удосконаленої моделі дозволяє динамічно змінювати параметри захисту користувачів мережі у залежності від інтенсивності атак та заданого рівня захищеності інформації.

6. Набула подальшого розвитку математична модель системи захисту інформації в соціальних мережах, яка на відміну від існуючих, дозволяє провести об'єктивну оцінку балансу між загрозами безпеки інформації та специфічними параметрами соціальної мережі, такі як параметр розповсюдження інформації, розширення мережі та коефіцієнт кореляції, що дає можливість змінювати рівень доступу до інформації користувача у залежності від репутації оточення.

7. Удосконалено математичну модель та методику підвищення рівня захищеності інформації, яка на відміну від існуючих враховує вплив на систему захисту інформації довіри, репутації, кореляції та коефіцієнта кластеризації мережі. Застосування моделі та методики дозволяє проводити аналіз впливу на систему захисту інформації інших ситуативних параметрів (наявної кількості діад, тріад, спільнот і т.п.).

8. Реалізація запропонованих в дисертації методологічних основ забезпечення захисту інформації та даних в соціальних мережах дозволяє:

проводити математичне моделювання захисту даних в соціальних мережах з метою отримання необхідного рівня захищеності інформаційного простору соціальних мереж;

здійснювати оцінку захисту користувачів під час та після проведення комплексних атак на систему захисту даних зі зміною параметрів атак та системи захисту;

забезпечити підвищення рівня захищеності інформаційного простору соціальних мереж за рахунок побудові фазового портрету та перехідних процесів системи захисту даних;

здійснювати оцінку рівня захищеності інформаційного простору соціальних мереж з використанням окремих компонентів системи: довіри, репутації, взаємовідносин, взаємовпливу, центральності, коефіцієнта кластеризації, розповсюдження інформації, розширення мереж, середнього шляху;

проводити оцінку захищеності даних при нелінійній взаємодії компонентів захисту.

9. Мета досліджень, яка полягає у підвищенні рівня захищеності інформації у соціальних мережах за рахунок врахування специфічних параметрів соціальних мереж: довіри, репутації користувачів та нелінійної взаємодії параметрів системи захисту інформації досягнута, всі часткові

завдання вирішено повністю. Наукові положення та результати дисертаційного дослідження є внеском у розвиток теорії моделювання процесів нападу на інформацію та її захисту в частині, що стосується забезпечення розробки методологічних основ захисту інформації користувачів в соціальних мережах.

10. Результати досліджень реалізовані у практичній діяльності ПрАТ “Бліц-Інформ” (Акт від 23.05.2020), Науково-методичному центрі кадрової політики Міністерства оборони України (Акт від 19.11.2020), ТОВ “Комплексна служба безпеки “Система”” (Акт від 09.10.2020), ТОВ “УКРІНФОСИСТЕМИ” (Акт від 27.12.2019), ПП “ІТ Центр” (Акт від 15.09.2020) та в освітньому процесі Державного університету телекомунікацій (Акт від 17.09.2020).

11. Перспективними шляхами подальших досліджень у зазначеному напрямку може бути широке коло питань щодо розробки нових та удосконалення існуючих методів і методик виявлення загроз несанкціонованого доступу до інформації або даних, на фоні зростання завантаженості інформаційного простору соціальних мереж

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Shchypanskyi P., Savchenko V., Akhramovych V., Muzshanova T., Lehominova S., Chegrenets V. The Model of Secure Social Networks Activity Based on Graph Theory. International Journal of Innovative Technology and Exploring Engineering (IJITEE). ISSN: 2278–3075, Vol. 9. Issue 4, February 2020, pp. 1803 – 1810. (**Scopus**) https://www.ijitee.org/download/volume–9–issue–4.

2. Savchenko V., Akhramovych V., Tushych A., Sribna I., Vlasov I. Analysis of Social Network Parameters and the Likelihood of its Construction. International Journal of Emerging Trends in Engineering Research (IJETER). ISSN: 2347 – 3983, Vol. 8. No. 2, February 2020. pp. 271 – 276.

http://www.warse.org/IJETER/static/pdf/file/ijeter05822020.pdf

3. Ахрамович В.М. Зв’язок та вплив користувачів в соціальних мережах. Colloquium-journal. Warszawa, Polska. 2020. № 3 (55). pp. 21 – 25.

http://www.colloquium-journal.org.

4. Ахрамович В.М. Степеневі соціальні мережі. Colloquium-journal. Warszawa, Polska. 2020. № 5 (57). pp. 27 – 29. http://www.colloquium-journal.org.

5. Ахрамович В.М. Стефурак О.Г. Центральність соціальних мереж. Colloquium-journal. Warszawa, Polska. 2020. № 6 (58). pp. 20 – 22.

http://www.colloquium–journal.org.

6. Ахрамович В.М., Гончаренко Н.А. Дослідження конфіденційності приватної особи в соціальних мережах. Sciences of Europe. Praha, Czech Republic. 2020. № 48. pp. 6 – 10. www.european–science.org.

7. Ахрамович В.М., Гончаренко Н.А. Структурні властивості співтовариств в соціальних мережах. Colloquium-journal. Warszawa, Polska. 2020. № 4 (56). pp. 14 – 16. http://www.colloquium–journal.org.

8. Ахрамович В.М. Модель ідентифікації користувачів в інтернет соціальних мережах. Magyar Tudományos Journal. Budapest, Hungary. 2019. № 35. pp 55 – 57. www.magyar–journal.com.

9. Ахрамович В.М. Модель сильних та слабких зв'язків користувачів в соціальних мережах. Зв'язок. К. ДУТ, 2019. № 3. С. 8 – 12.

10. Ахрамович В.М. Проблеми відтворення атак на дані приватної особи та методи захисту в Інтернет–соціальних мережах. Sciences of Europe. Praha, Czech Republic. 2019. № 44. pp. 31 – 38. www.european–science.org.

11. Ахрамович В.М. Створення структури розподіленої соціальної мережі Friendsbook. Sciences of Europe. Praha, Czech Republic. 2019. № 47. pp. 35–42. www.european–science.org

12. Ахрамович В.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.

13. Ахрамович В.М., Сіренко О.О. Підвищення ефективності криптографічного захисту інформації у локальній мережі об'єкта інформаційної діяльності. Сучасний захист інформації. К. ДУТ, 2019. № 1. С. 12 – 16.

14. 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. www.magyar–journal.com.

15. Ахрамович В.М., Чегренець В.М. Дослідження безпеки даних користувачів в Інтернет-соціальних мережах. Magyar Tudományos Journal. Budapest, Hungary. 2019. № 36. pp 58–61. www.magyar–journal.com.

16. 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. www.european-science.org

17. Ахрамович В.М., Чегренець В.М. Управління ризиками інформаційної безпеки комерційного банку. Сучасний захист інформації. К. ДУТ, 2019. № 2. С. 54 – 59.

18. Ахрамович В.М. Моделі довіри та репутації користувачів в соціальних мережах. Сучасний захист інформації. К. ДУТ, 2019. № 4. С. 45 – 51.

19. Ахрамович В.М. Модель взаємовідносин користувачів в соціальних мережах. Сучасний захист інформації. К. ДУТ, 2019. № 3. С. 42 – 50.

20. Ахрамович В.М. Адміністративний рівень інформаційної безпеки. Сучасний захист інформації. К. ДУТ, 2017. № 1. С. 10 – 14.

21. Ахрамович В.М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. К. ДУТ. 2016. № 4. С. 47 – 51.

22. Чегренец В.М., Ахрамович В.М., Руденко Н.В. Хмарні технології та можливості використання в комп'ютерних телекомунікаційних системах. Наукові записки. Українського науково–дослідного інституту зв'язку. К. ДУТ, 2016. № 2 (42). С. 121 – 129.

23. Ахрамович В.М., Чегренець В.М. Тенденції розвитку захисту даних в соціальних мережах. Телекомунікаційні та інформаційні технології. Науковий журнал. К. ДУТ, 2020. № 1. С. 23 – 27.

24. Ахрамович В., Лазаренко С., Мартинюк Г., Баланюк Ю. Модель пошуку співтовариств в соціальній мережі. Безпека інформації. К. НАУ, 2020. № 1. С. 35 – 41.

25. Ахрамович В.М. Моделювання і візуалізація соціальних мереж. Зв'язок. К. ДУТ, 2020. № 1. С. 13 – 18.

26. Ахрамович В.М., Головач А.В. Модель розширення соціальних мереж. Colloquium-journal. Warszawa, Polska. 2020. № 7 (59). pp. 5 – 7. http://www.colloquium–journal.org.

27. Ахрамович В.М. Концепція безпечної архітектури соціальної мережі, що захищає конфіденційність. Sciences of Europe. Praha, Czech Republic. 2020. № 49. pp. 10 – 17. www.european–science.org.

28. Ахрамович В.М., Амелькін С.В. Система захисту інформації підприємства. Організація служби захисту. Сучасний захист інформації. К. ДУТ, 2019. № 1. С. 17 – 23.

29. Ахрамович В.М. Граничні ймовірності станів безпеки даних та взаємодії користувачів в соціальній мережі. Magyar Tudományos Journal. Budapest, Hungary. 2020. № 41. pp 25 – 31. www.magyar-journal.com.

30. Akhramovych V.M., Chegrenec V.M. The problem of the protection methods differences of the centralized and decentralized distributed social networks. Abstracts of the 3rd International scientific and practical conference «Perspectives of world science and education» (November 27 – 29, 2019). CPN Publishing Group. Osaka, Japan. pp. 217 – 225.

31. Ахрамович В.Н., Котенко А.Н., Степаненко В.И. Анализ безопасности сетей сотовой связи 4G /5 G. Тези доповідей Регіонального семінару Міжнародного союзу електрозв'язку для країн Європи та СНД «Цифрове

майбутнє на основі 4G/5G» “Digital Future Powered by 4G/5G”. 14–16 травня 2018 р. Київ. С. 12 – 14.

32. Ахрамович В.М., Чегренець В.М., Зідан А.М. Деякі аспекти безпеки особистих даних в соціальних мережах. Abstracts of I International Scientific and Practical Conference «Science, society, education: topical issues and development prospects» (December 16 – 17, 2019) SPC “Sci-conf.com.ua”, Kharkiv, Ukraine. 2019. С. 175 – 179.

33. Ахрамович В.М., Чегренець В.М., Зідан А.М. Диференціація соціальних мереж та їх основні функції. Abstracts of IV International Scientific and Practical Conference «Scientific achievements of modern society» (December 4 – 6, 2019). Liverpool, United Kingdom. pp 646 – 654.

34. Ахрамович В.М., Чегренець В.М. Дослідження характеристик особистої інформації користувача в інтернет-соціальних мережах. Proceedings of articles the international scientific conference «Advances of science» (Kyiv, December 6, 2019). Karlovy Vary, Czech Republic – Kyiv, Ukraine. pp 101 – 110.

35. Ахрамович В.М., Чегренець В.М. Постановка проблем захисту від загроз особистій інформації приватній особі в інтернет-соціальних мережах через дослідження їх функцій. Тези доповідей VIII міжнародної науково–практичної конференції «Осінні наукові читання» (м. Київ, 31 жовтня 2019 р.). К. Центр наукових публікацій, 2019. С. 51 – 59.

36. Ахрамович В.М., Чегренець В.М. Соціальні мережі та можливі ризики безпеки. Тези доповідей. Abstracts of IV International Scientific and Practical Conference «Topical issues of the development of modern science» (December 11 – 13, 2019) Publishing House “ACCENT”, Sofia, Bulgaria. 2019. pp. 583 – 568.

37. Ахрамович В.М., Білоцерківець О.В. Методика підвищення ефективності застосування засобів забезпечення інформаційної безпеки користувачів послуг Інтернет. Тези доповідей. Семінар-практикум Міжнародного союзу електрозв’язку для регіонів Європи та СНД «Інфраструктура ІКТ як основа цифрової економіки». 14 – 16 травня 2019 р. Київ. С. 12 – 13.

38. Ахрамович В.М., Чегренець В.М. Уразливості та способи захисту бездротових мереж. Тези доповідей ІІ Міжнародної науково–практичної конференції «Тенденції розвитку конвергентних мереж: рішення пост-NGN, 4G і 5G». 17 – 18 листопада 2016 р. Київ. С. 163 – 166.

39. Чегренець В.М., Ахрамович В.М., Інформаційна безпека особистості в соціальних мережах. Abstracts of II International Scientific and Practical Conference «Priority directions of science development» (November 25-26, 2019) SPC “Sciconf.com.ua”, Lviv, Ukraine. 2019. С. 250 – 255.

40. Ахрамович В.М. Захист інформації під час застосування операційної системи Windows XP. Науковий Вісник Національної академії статистики, обліку та аудиту. К. НАСОА, 2007. № 2. С. 92 – 105.

41. Ахрамович В.М. Захист інформації під час застосування операційної системи Windows 7. Науковий Вісник Національної академії статистики, обліку та аудиту. К. НАСОА, 2012. № 4. С. 96 – 116.

42. Ахрамович В.М. Захист інформації під час застосування особистої системи мережевого захисту McAfee Personal Firewall Plus. Науковий Вісник Національної академії статистики, обліку та аудиту. К. ДАСОА, 2006. № 2. С. 87 – 96.

43. Ахрамович В.М. Програми захисту інформації приховуванням її та шифруванням. Науковий Вісник Національної академії статистики, обліку та аудиту. К. НАСОА, 2008. № 4. С. 100 – 109.

44. Васильчук М.П., Ахрамович В.М. Концепція захисту інформації у комп'ютерних лабораторіях Національної академії статистики, обліку та аудиту. Науковий Вісник Державної академії статистики, обліку та аудиту. К. ДАСОА. 2004. № 2. С. 11 – 19.

45. Савченко В.А., Ахрамович В.М., Акулінічева М.В. Оцінювання параметрів безпеки даних у степеневих соціальних мережах на основі їх топології. Сучасний захист інформації. К. ДУТ, 2020. № 3. С. 6 – 13.

АНОТАЦІЯ

Ахрамович В.М. Методологічні основи захисту інформації в соціальних мережах. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Державний університет телекомунікацій, Київ, 2021.

Розроблено концепцію забезпечення захисту інформації в соціальних мережах, яка базується на математичних моделях захисту даних з урахуванням впливу специфічних параметрів соціальної мережі, впливів, що здійснюються на мережу, з урахуванням нелінійних зв’язків параметрів з системою захисту та параметрів зовнішніх впливів індивідуальних характеристик користувачів, характеру зв’язків між ними, соціальних та технічних параметрів мереж. Застосування концепції дозволяє розробити відповідний комплекс моделей та методів оцінювання взаємного впливу окремих складових на захищеність даних, визначати необхідні вхідні характеристики та умови функціонування

моделей для досягнення необхідного стану захищеності інформації в соціальних мережах.

Математичні моделі дозволяють визначати залежності показників захисту даних від складових системи захисту, стійкість системи захисту (фазові портрети), перехідні процеси в системі захисту, реакція системи захисту на зовнішні впливи.

Ключові слова: математичні моделі, соціальні мережі, дані, захист, безпека, фазові портрети, перехідні процеси, користувач, моделі, вплив, взаємодія, репутація, довіра, загрози.

АННОТАЦИЯ

Ахрамович В.М. Методологические основы защиты информации в социальных сетях. – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по спецальности 05.13.21 «Системы защиты информации». – Государственный университет телекомуникаций, Киев, 2021.

Разработана концепция обеспечения защиты информации в социальных сетях, основанная на математических моделях защиты данных с учетом влияния специфических параметров социальной сети, воздействий, совершаемых на сеть, с учетом нелинейных связей параметров с системой защиты и параметров атак влияния индивидуальных характеристик пользователей и характера связей между ними, социальных и технических параметров сетей. Применение концепции позволяет разработать соответствующий комплекс моделей и методов оценки взаимного влияния отдельных составляющих на защищенность данных, определять необходимые входные характеристики и условия функционирования моделей для достижения необходимого состояния защищенности информации в социальных сетях.

Математические модели позволяют определять зависимости показателей защиты данных от составляющих системы защиты, устойчивость системы защиты (фазовые портреты), переходные процессы в системе защиты, реакция системы защиты на внешние воздействия.

Ключевые слова: математические модели, социальные сети, персональные данные, защита, безопасность, фазовые портреты, переходные процессы, пользователь, модели, влияние, взаимодействие, репутация, доверие, угрозы.

ABSTRACT

Akhramovich V.M. Methodological bases of information protection in social networks. – The manuscript.

The dissertation for the degree of Doctor of Technical Sciences in the specialty 21.05.01 “Information Security of the State”. – State University of Telecommunications, Kiev, 2021.

A modeling method is proposed, on the basis of which an objective assessment of the balance between threats to information security, from specific parameters of a social network, attacks on the network and protection measures and the volume of protected data, analysis of the parameters of the behavior of the protection system during and after carrying out complex attacks against data protection system with changing parameters of attacks and protection systems.

A concept has been developed to ensure the security of personal data of an individual in social networks, based on mathematical models of personal data protection, taking into account the influence of specific parameters of a social network made on the network of attacks, taking into account the nonlinear relationships of parameters with the protection system and attack parameters, the influence of individual characteristics of users and the nature of connections between them, social and technical parameters of networks. Application of the concept makes it possible to develop an appropriate set of models and methods for assessing the mutual influence of individual components on the security of personal data, to determine the necessary input characteristics and conditions for the functioning of models to achieve a state of protection of personal data of an individual in social networks.

Mathematical models make it possible to determine the dependence of personal data protection indicators on the components of the protection system, the stability of the protection system (phase portraits), transient processes in the protection system, the response of the protection system to attacks.

A method for increasing the level of security of the information space of social networks has been developed, based on a comprehensive analysis of the impact of all components in aggregate on the data protection system and the response of the protection system to attacks. The technique is based on the use of the MatLab / Multisim program, and allows you to effectively investigate phase portraits and transients with visualization of models (block diagrams) and research results. Application of the technique allows analyzing the stability of the protection system and data security.

Keywords: mathematical models, social networks, personal data, protection, security, phase portraits, transient processes, user, models, influence, interaction, reputation, trust, threats.