УДК 004.56:61

д.т.н., проф. **Лукова-Чуйко Н.В.** (КНУ ім. Т. Шевченко)
д.т.н., с.н.с. **Лаптєв О.А.** (КНУ ім. Т. Шевченко)
д.т.н., проф.**Барабаш О.В.** (НТУ «КПІ ім. І. Сікорського»)
д.т.н., доц. **Мусієнко А.П.** (НТУ «КПІ ім. І. Сікорського»)
д.т.н., с.н.с. **Ахрамовіч В.М.** (ДУТ)

DOI: https://doi.org/10.17721/2519-481X/2022/76-05

МЕТОД РОЗРАХУНКУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ З УРАХУВАННЯМ КОМПЛЕКСУ СПЕЦИФІЧНИХ ПАРАМЕТРІВ СОЦІАЛЬНИХ МЕРЕЖ

В Україні право на захист особистих даних – це конституційна гарантія, а захист персональних даних – одна із сфер, у якій така гарантія має реалізовуватись. Предметом нашого дослідження будуть не об'єкти взагалі, а динамічні системи захисту інформації в соціальних мережах у математичному розумінні цього терміну. У дослідженні розроблено лінійну математичну модель і проведено дослідження моделі захисту персональних даних від комплексу специфічних параметрів мережі і інтенсивності передачі даних в соціальних мережах.

Розглянуто залежності: величини потоку інформації в соціальній мережі від складових захисту інформації, персональних даних, і швидкості потоку даних; захищеності системи від розмірів системи та від кількості персональних даних; загроз безпеці інформації від комплексу специфічних параметрів мережі.Отримано систему лінійних рівнянь, яка складається з рівняння: швидкості зміни потоку інформації від захищеності соціальної мережі і коефіцієнтів, які відображають вплив заходів захищеності, кількості персональних даних, швидкості витоку, зміни показника захисту інформації від комплексу специфічних параметрів мережі, її розмірів, захищеності персональних даних. В результаті розв'язання системи диференціальних рівнянь отримані математичні та графічні залежності показника захисту персональних даних в соціальній мережі від різних складових. Розглянувши три варіанти вирішення рівняння близько стаціонарного стану системи, можна прийти до висновку, що, виходячи з умов співвідношення дисипації, загасання частоти коливань до певного значення здійснюється періодично, із затухаючою амплітудою, або експоненціально за згасаючим законом. Виконано більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь до дискретної і промодельовано деякий інтервал існування системи.

Представлені математичні та графічні залежності частоти власних коливань системи, періоду коливань, коефіцієнта загасання.Проведено імітаційне моделювання для значень з відхиленням від стаціонарної позиції системи. В результаті імітаційного моделювання доведено, що система захисту соціальної мережі нелінійна.

Ключові слова: соціальна мережа, потік інформації, довіра, репутація, моделювання, коефіцієнт захисту, безпека, захист інформації.

Вступ та постановка задачі. Швидке поширення соціальних онлайн-сервісів і розвиток технології Big Data викликали інтерес до використання інформації з соціальних мереж у різних сферах. Обмін структурними та тематичними даними потенційно дозволяє використовувати соціальні мережі для вирішення широкого кола завдань захисту інформації та даних. Предметом даного дослідження будуть не об'єкти взагалі, а динамічні системи захисту інформації в соціальних мережах у математичному розумінні цього терміну.

Зважаючи на складність процесів в соціальних мережах, інтенсивний розвиток технологій несанкціонованого доступу до персональної інформації, забезпечення захисту є одним із актуальних завдань для спільноти в Україні та світі. Існуючі компоненти захисту особистої інформації, не забезпечують повного захисту персональних даних особи, що обумовлено низкою проблем. Відсутність методології побудови систем захисту в соціальних мережах являється стримуючим фактором подальшого розвитку соціальних мереж та інформаційних технологій в цілому. Якщо на сьогодні більш менш досліджені класичні загрози персональної інформації та розроблені методи їх захисту, то залишається до кінця не

вивченим вплив специфічних параметрів соціальних мереж на захист персональної інформації. До таких специфічних параметрів відносяться: конфіденційність персональних даних, репутація користувачів мережі, взаємовплив користувачів, довіра між користувачами, спільні думки користувачів мережі, сильні та слабкі зв'язки, авторитет користувача, швидкість поширення персональних даних в мережі, параметри розширення мережі, кількість співтовариств в мережі, канали поширення інформації, ідентифікація користувачів тощо.

Дослідження динамічної поведінки реального об'єкта захисту вимагає створення його математичної моделі. У багатьох випадках процедура розробки моделі полягає в складанні математичних системи рівнянь. В результаті координати стану системи і її параметри виявляються пов'язаними між собою, що дозволяє приступити до розв'язання диференціальних рівнянь при різних початкових умовах і параметрах.

Тому розробка нових та удосконалених методів підвищення рівня захищеності інформаційного простору соціальних мереж, які базуються на математичних моделях динамічних систем в залежності від специфічних параметрів соціальної мережі є актуальною.

Аналіз останніх досліджень. Більшість відомих підходів до моделювання, відрізняються тім, які параметри при моделюванні ними використовують в якості вхідної інформації та які характеристики модельованої системи розраховуються та надходять на вихід моделі. При цьому аналітичні моделі, що розглядаються з позиції теоретичної математики, не є тотожними реальній дійсності, зважаючи на обмежену точність результатів.

У роботі [1], вказується, що поведінка соціальної мережи змінюється з часом, тому вага користувача в соціальної мережи різна в кожному періоді часу. Таким чином, показник для оцінки ваги користувача в соціальні мережи залежить від точності метрики, яка використовується для визначення часового інтервалу. Нова метрика для визначення часових інтервалів базується на стандартному відхиленні та визначає, що вага користувача базується на простій експоненційній моделі згладжування. В роботі [2], досліджується всесвітня мережа, яка утворює великий орієнтований граф, вершинами якого є документи, а ребра – посилання, що вказують шлях від одного документа до іншого. Незважаючи на його очевидний випадковий характер, топологія цього графа має ряд універсальних характеристик. Представлена модель може описувати мережу без масштабування з певними процесами самоорганізації.

У роботі [3] проводиться виявлення підозрілої та незаконної поведінки в соціальних мережах, що є актуальним завданням під час аналізу соціальних мереж. Моделі взаємодії підозрілих користувачів значно відрізняються від їхніх товаришів і можуть бути ідентифіковані за допомогою методів виявлення аномалій. Зазначені методи можуть застосоввуватись для мереж із лише одним типом взаємодії між користувачами. У цій роботі досліджується проблема виявлення аномалій у багатошарових соціальних мережах шляхом об'єднання інформації, доступної на кількох мережевих рівнях.

У роботі [4] вказується, що швидка цифрова трансформація та технологічні зриви в сучасних організаціях вимагають розвитку робочих місць, орієнтованих на людей, за допомогою яких співробітники зможуть підвищити рівень усвідомлення безпеки та відповідальності за свої дії завдяки участі в соціальних мережах.

У роботах [5,7,18] наведено результати імітаційного моделювання експерименту для вирішення завдання щодо запобігання поширенню забороненої інформації в соціальній мережі. Представлені інструментальні засоби імітаційного моделювання та їх особливості, що сприяють успішному застосуванню для моделювання соціальних мереж. Автори наводять приклад імітаційної моделі для виявлення зловмисників у соціальній мережі.

У роботі [6] вказується можливість передбачення та аналізу поведінки людини в соціальній мережі за результатами аналізу дій користувача: теми, настрої, відповіді на повідомлення, тощо. Для вирішення цього завдання представлено метод моделювання інтерактивної поведінки в соціальної мережи мікроблогів з урахуванням настроїв користувачів. Використовується стохастичний підхід, заснований на кількох агентах. В якості

прикладу досліджується мережа Twitter Барака Обами як егоцентрична мережа, щоб представити результати експериментального моделювання.

У роботах [8,11,13-15] досліджено динамічні нелінійні системи захисту соціальних мереж, які враховують показники довіри, репутації, взаємодії користувачів, розповсюдження інформації та конструктивних особливостей соціальні мережи. Показані результати стійкості системи захисту з використанням фазової площини.

У роботах [9,10] представлені моделі випадкових графів та їх застосування. Описано неявний соціальний граф, який формується взаємодією користувачів із контактами та групами контактів, і який відрізняється від явних соціальних графів, у яких користувачі явно додають інших людей як своїх «друзів». Представлено метрику взаємодії для оцінки спорідненості користувача з його контактами та групами. Запропоновано новий алгоритм створення групи друзів, який використовує неявний соціальний граф користувача, враховуючи невеликий початковий набір контактів, яких користувач уже позначив як друзів. Показано експериментальні результати, що демонструють важливість як неявних групових стосунків, так і рейтингу спорідненості на основі взаємодії для пропонування друзів. Аналізуються два застосування алгоритму Friend Suggest, які були випущені як функції Gmail Labs.

В роботах [12, 21] розглядається застосування теорії динамічного хаосу до вивчення соціальних явищ. Звернення до витоків створення теорії динамічного хаосу в природознавстві виявило нелінійні динамічні системи в природному середовищі (турбулентні потоки атмосфери, біологічні популяції тощо). Застосування теорії хаосу можливе також на мікро- та макрорівнях соціальних досліджень.

В роботах [16, 17] досліджуються соціальні мережі як феномен організації суспільства: сутність та підходи до використання й моніторингу.

В роботі [19] проведено аналіз характеристик соціальних графів, побудованих за даними соціальної мережі Twitter за тиждень, що дозволяє використовувати вказані характеристики для генерації моделей випадкових графів. Таке використання є корисним на етапах експериментального аналізу під час оцінки ефективності математичного та програмного забезпечення. Пропонується удосконалена модель зростання соціальної мережі, заснована на опосередкованому зв'язуванні вузлів. Для цієї моделі представлені результати комп'ютерного моделювання. Продемонстровано наявність фаз щільної та розрідженої мережі, а також обумовленість властивостей мережі з її густиною.

Разом з тим у всіх зазначених джерелах математичне моделювання розглядається як застосування математичної моделі конкретних параметрів (деякі параметри мають імовірнісний характер). Питання взаємозв'язку та глибини взаємозв'язку вхідних параметрів під час моделювання процесів не розглядаються. Ці чинники взаємозв'язку і взаємовпливу можуть істотно спотворити результати моделювання і поставити під сумнів адекватність моделі. Тому розробка нових та удосконалених методів підвищення рівня захищеності інформаційного простору соціальних мереж, які базуються на математичних моделях динамічних систем в залежності від специфічних параметрів соціальної мережі є актуальною.

Метою роботи є удосконалення моделі захисту даних у соціальної мережи за рахунок врахування специфіки соціальних мереж. Для цього необхідно провести дослідження впливу комплексу специфічних параметрів соціальної мережі на параметри захисту інформації, а також на основі лінійної моделі параметрів соціальної мережи перевірити лінійність системи захисту інформації.

Виклад основного матеріалу. Теоретичне дослідження динамічної поведінки реального об’єкта вимагає створення його математичної моделі. У багатьох випадках процедура розробки моделі полягає в складанні математичних рівнянь на основі фізичних законів. Зазвичай ці закони формулюються сукупністю диференціальних рівнянь. В результаті координати стану системи та її параметри виявляються пов’язаними між собою, що дозволяє приступити до розв’язання диференціальних рівнянь при різних початкових умовах і параметрах.

Згідно класичного підходу до захисту персональних даних, розрізняють:

$$T_i = \left[D_j, D_n, D_m, D_k, P_{ij}, N_{ij}, r_i R, V_i, V_j, C(G), y_i, y_j, L_i, I_{a,b}, I_a, P_i, P_j \right], \quad (1)$$

де: T_i – множина загроз від специфічних параметрів соціальної мережі,

D_j – довіра до надання послуг (людина довіряє певній компанії щодо надання якісних послуг або ресурсів),

D_n – довіра делегування (delegation trust) описує довіру до користувача (представника), що діє і виносить рішення від імені компанії, якій довіряє,

D_m – довіра доступу (access trust) описує довіру зі сторони провайдера до користувача, якому надається доступ до ресурсів. Цей контроль доступу використовується в системах автентифікації,

D_k – контекстна довіра, визначає міру довіри учасника в необхідні системи та інституційні механізми, що підтримують транзакції і забезпечують безпеку мережі,

r_i – репутація *i*–того користувача,

R – колективна сумарна репутацію членів СМ,

P_{ij} – позитивний вплив між користувачами,

N_{ij} – негативний вплив між користувачами,

V_i – позитивна взаємодія між користувачами,

V_j – негативна взаємодія між користувачами,

$C(G)$ – середній коефіцієнт кластеризації всіх вузлів графа,

y_i – можлива передача інформації між користувачами,

y_j – неможлива передача інформації між користувачами,

L_i – довжина шляху між користувачами,

$I_{a,b}$ – ідентифікація користувачів в мережах а і в,

I_a – ідентифікація користувача в мережі,

P_i – ймовірність того, що зв'язок буде створений з даною вершиною при випадковому приєднанні,

P_j – ймовірність того, що зв'язок буде створений з даною вершиною при переважному приєднанні.

Зміна такої якості, як специфічні параметри соціальних мереж, є процесом, що має часовий інтервал. Позначимо кількість інформації в системі – *I*. Потік інформації за межі інформаційної системи позначимо через *dI*, швидкість зміни цього потоку – $\frac{dI}{dt}$. Логічно, що, якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає:

$$dI = 0; \quad \frac{dI}{dt} = 0. \quad (2)$$

Витік інформації залежить від захищеності системи – вжитих заходів з нейтралізації загроз безпеки персональних даних. Z – показник захищеності інформаційної системи. Складемо рівняння:

$$\frac{dI}{dt} = Z_p Z + (C_v + C_k) I, \quad (3)$$

де Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації;

C_v – коефіцієнт, що відображає вплив швидкості витоку персональних даних;

C_k – коефіцієнт, що відображає вплив кількості персональних даних на їх витік.

Інтерпретувати дане рівняння можна наступним чином. Витік інформації залежить від:

–розміру інформаційної системи (так і від кількості персональних даних);

–швидкості витоку персональних даних;

–витоку інформації блокується захищенністю системи (заходами щодо нейтралізації загроз безпеки інформації).

Далі розглянемо, від чого залежить захищеність системи Z. Визначимо захищеність системи як здатність системи протистояти несанкціонованому доступу до конфіденційнихперсональних даних. Отже, захищеність системи буде залежати від:

–розмірів системи (так і від кількості персональних даних);

–загроз безпеки інформації від втрати довіри між користувачами;

–загроз безпеки інформації від взаємоємовпливу між користувачами;

–загроз безпеки інформації від взаємовідносин між користувачами;

–загроз безпеки інформації від приєднання між користувачами;

–загроз безпеки інформації від коефіцієнта кластеризації;

–швидкості витоку персональних даних; витік інформації купіюється захищенністю системи (заходами щодо нейтралізації загроз безпеки інформації);

–загроз безпеки інформації від поширення інформації між користувачами;

–загроз безпеки інформації від неідентифікації користувачів.

Складемо рівняння:

$$\frac{dZ}{dt} = D_i + DR + \frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i} + (\bar{P}_{ij} - \bar{N}_{ij})/(\bar{P}_{ij} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i + \frac{\sum_{v \in V} C_{v1}}{N} + \\ + t\ (r+1)^{-f} + EXP(-\sum_{v \in V} \Phi(y_v, x_v) + \sum_{v \in u} \Psi(y_v, x_u)) - I(C_{d2} + C_{d1}), \quad (4)$$

де D – довіра між користувачами,

R – загальна репутація користувачів мережі,

n_i – загальне число вершин графа в момент часу t,

x_i – кількість зв’язків які має вершина графа в момент часу t,

P_{ij}^m та N_{ij}^m – число позитивних і негативних шляхів довжини m, що йдуть від фактора x_i до фактору x_j, відповідно;

параметр 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,

N – загальне число вершин графа в момент часу t,

$\sum_{v \in V} C_v$ – сумарне число зв’язків вершин графа в момент часу t, $f>0$,

r – кількість користувачів з якими може поділитися даний користувач інформацією,

t – користувач мережі, який знаходиться на визначеному вузлі, унарна енергії Φ і бінарна енергія ψ.

Ці дві енергетичні функції є дійсними і невід’ємними. Унарна енергія відповідає за схожість профілю в графі А і його проекції в В з точки зору полів профілів, а бінарна енергія відповідає за близькість між проекціями вершин v та u в графі B.

Об'єднаємо рівняння (3) і (4) в систему рівнянь:

$$\begin{cases} \dfrac{dZ}{dt} = D_i + DR + \dfrac{1}{n_i} + \dfrac{x_1}{\sum\limits_{i=1}^{n} x_i} + (\bar{P}_{ij} - \bar{N}_{ij})/(\bar{P}_{ij} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i + \\ + \dfrac{\sum\limits_{v \in V} C_{v1}}{N} + t\ (r+1)^{-f} + EXP(-\sum\limits_{v \in V} \Phi(y_v, x_v) + \sum\limits_{v \in u} \Psi(y_v, x_u)) - I(C_{d2} + C_{d1}); \\ \dfrac{dI}{dt} = Z_p Z + (C_v + C_K)I. \end{cases} \quad (5)$$

Знайдемо стаціонарну позицію системи, що описується рівняннями (5). Умови стаціонарності $dI = 0; \dfrac{dI}{dt} = 0$. Отже:

$$\begin{cases} D_i + DR + \dfrac{1}{n_i} + \dfrac{x_1}{\sum\limits_{i=1}^{n} x_i} + (\bar{P}_{ij} - \bar{N}_{ij})/(\bar{P}_{ij} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i + \\ + \dfrac{\sum\limits_{v \in V} C_{v1}}{N} + t\ (r+1)^{-f} + EXP(-\sum\limits_{v \in V} \Phi(y_v, x_v) + \sum\limits_{v \in u} \Psi(y_v, x_u)) - I(C_{d2} + C_{d1}); \\ Z_p \bar{Z} + (C_v + C_K)\bar{I} = 0. \end{cases} \quad (6)$$

З другого рівняння системи слідує:

$$\bar{I} = \frac{D_i + DR + \dfrac{1}{n_i} + \dfrac{x_1}{\sum\limits_{i=1}^{n} x_i} + (\bar{P}_{ij} - \bar{N}_{ij})/(\bar{P}_{ij} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V}{(C_{d2} + C_{d1})} + \frac{\dfrac{\sum\limits_{v \in V} C_{v1}}{N} + t\ (r+1)^{-f} + EXP(-\sum\limits_{v \in V} \Phi(y_v, x_v) + \sum\limits_{v \in u} \Psi(y_v, x_u)}{(C_{d2} + C_{d1})}. \quad (7)$$

Далі з першого рівняння системи рівнянь (6) знаходимо $\bar{Z}$.

$$Z_p \bar{Z} - \frac{D_i + DR + \dfrac{1}{n_i} + \dfrac{x_1}{\sum\limits_{i=1}^{n} x_i} + (\bar{P}_{ij} - \bar{N}_{ij})/(\bar{P}_{ij} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V}{(C_{d2} + C_{d1})} + \frac{\dfrac{\sum\limits_{v \in V} C_{v1}}{N} + t\ (r+1)^{-f} + EXP(-\sum\limits_{v \in V} \Phi(y_v, x_v) + \sum\limits_{v \in u} \Psi(y_v, x_u)(C_v + C_k)}{(C_{d2} + C_{d1})} = 0. \quad (8)$$

$$\bar{Z} = \frac{D_i + DR + \frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i} + (\bar{P}_{ij} - \bar{N}_{ij}) / (\bar{P}_{ij} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i}{(C_{d2} + C_{d1})Z_p} + \frac{\frac{\sum_{v \in V} C_{v1}}{N} + t\ (r+1)^{-f} + EXP(-\sum_{v \in V} \Phi(y_v, x_v) + \sum_{v \in u} \Psi(y_v, x_u)(C_v + C_k)}{(C_{d2} + C_{d1})Z_p}. \quad (9)$$

Отже, умови позиції стаціонарності системи: рівняння (7), (9).

Результати моделювання системи (7), (9) відображено на рис. 1.

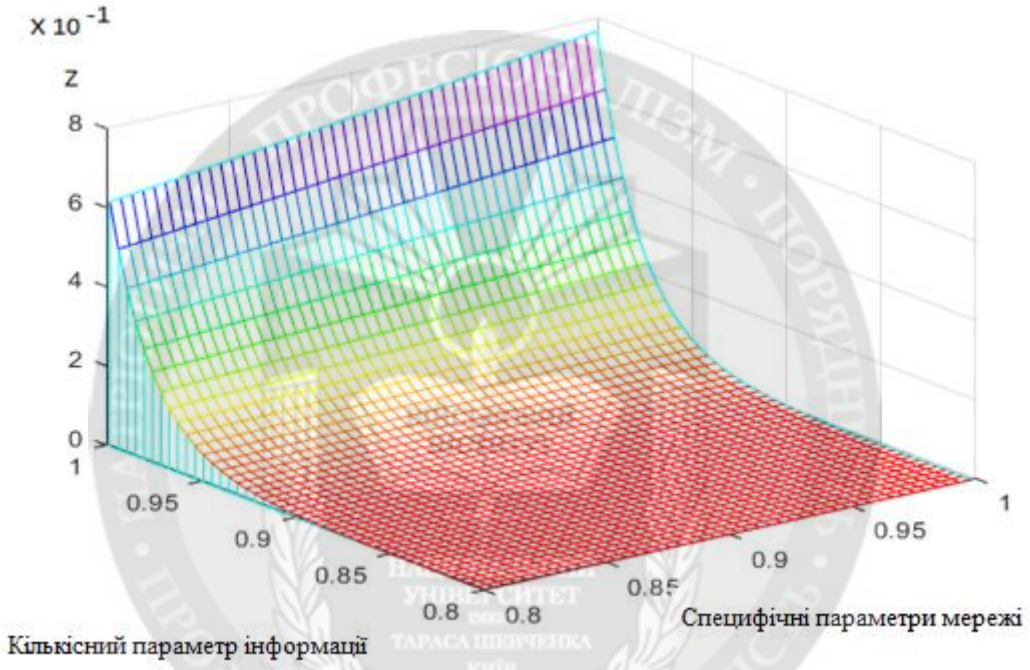

Рисунок 1 - Залежність захисту персональних даних від складових для рівняння (7), (9)

Вирішимо систему рівнянь (5) методом «малих відхилень»

$I = \bar{I} + I; Z = \bar{Z} + Z$. Отже, система рівнянь прийме вигляд:

$$\begin{cases} \dfrac{dZ}{dt} = R + DR + D_i + ((x_v + y_v) - e^{x_u + y_v}) + \dfrac{1}{n_i} + \dfrac{x_1}{\sum\limits_{i=1}^{n} x_i} + (C_v + C_k)_i \cdot (C_v + C_k) + \\ +(\bar{P}_{ij} - \dfrac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \dfrac{\sum C_{v1}}{N^2} + \dfrac{ft\ (r+1)^{-f}}{r-1} - (\bar{I} + I)(C_{d2} + C_{d1}); \\ \dfrac{dI}{dt} = Z_p\,(\bar{Z} + Z) + (C_v + C_K)(\bar{I} + I). \end{cases} \quad (10)$$

$$\begin{cases} \dfrac{dI}{dt} = (C_{d1} + C_{d2})Z - (C_v + C_K)I; \\ \dfrac{dZ}{dt} = -I(C_{d2} + C_k) + R + DR + D_i + ((x_v + y_v) - e^{x_u + y_v}) + \dfrac{1}{n_i} + \dfrac{x_1}{\sum\limits_{i=1}^{n} x_i} + (C_v + C_k)_i \cdot (C_v + C_k) + \\ +(\bar{P}_{ij} - \dfrac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \dfrac{\sum C_{v1}}{N^2} + + \dfrac{ft\ (r+1)^{-f}}{r-1} - \\ -(\bar{I} + I)(C_{d2} + C_{d1})(C_v + C_k)_i(C_v + C_k). \end{cases} \quad (11)$$

Диференціюючи перше рівняння системи (11) отримуємо:

$$\frac{d^2I}{dt^2} = -I(C_{d1} + C_{d2})(Z_p + R + DR + D_i + ((x_v + y_v) - e^{x_u + y_v}) + \frac{1}{n_i} + \frac{x_1}{\sum\limits_{i=1}^{n} x_i} +$$

$$+(C_v + C_k)_i \cdot (C_v + C_k) + (\bar{P}_{ij} - \frac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \frac{\sum C_{v1}}{N^2} + \frac{ft\ (r+1)^{-f}}{r-1} - \quad (12)$$

$$-(\bar{I} + I)(C_{d2} + C_{d1})(C_v + C_k)) - (C_v + C_K)\frac{dI}{dt}.$$

$$\frac{d^2I}{dt^2} + (C_v + C_K)\frac{dI}{dt} + (C_{d1} + C_{d2})(Z_p + R + DR + D_i + ((x_v + y_v) - e^{x_u + y_v}) + \frac{1}{n_i} + \frac{x_1}{\sum\limits_{i=1}^{n} x_i} +$$

$$+(C_v + C_k)_i \cdot (C_v + C_k) + (\bar{P}_{ij} - \frac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \frac{\sum C_{v1}}{N^2} + + \frac{ft\ (r+1)^{-f}}{r-1} - \quad (13)$$

$$-(\bar{I} + I)(C_{d2} + C_{d1})(C_v + C_k))I = 0.$$

Рівняння (13) є рівнянням гармонічного осцилятора з затухаючою амплітудою, де:

$$\omega_0 = \left(\begin{array}{l} (C_{d1} + C_{d2})(Z_p + R + DR + D_i + ((x_v + y_v) - e^{x_u + y_v}) + \frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i} + \\ \\ +(\bar{P}_{ij} - \frac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \frac{\sum_{v \in V} C_{v1}}{N^2} + \frac{ft\ (r+1)^{-f}}{r-1}) - I(C_{d2} + C_{d1}) \end{array} \right)^{\frac{1}{2}} .(14)$$

$$\omega = \left(\begin{array}{l} (C_{d1} + C_{d2})(Z_p + R + DR + D_i + ((x_v + y_v) - e^{x_u + y_v}) + \frac{1}{n_i} + \frac{x_1}{\sum_{i=1}^{n} x_i} + (C_v + C_k)_i \cdot (C_v + C_k) + \\ \\ +(\bar{P}_{ij} - \frac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \frac{\sum_{v \in V} C_{v1}}{N^2} + + \frac{ft\ (r+1)^{-f}}{r-1}) - (\bar{I} + I)(C_{d2} + C_{d1}) - \frac{(C_v + C_K)^2}{4} \end{array} \right)^{\frac{1}{2}} . \quad (15)$$

$$T = \frac{2\pi}{\omega}. \quad (16)$$

$$\beta = \frac{(C_v + C_K)}{2}. \quad (17)$$

Розв'язання рівняння гармонічного осцилятора розпадається на три випадки.

1. $\beta \prec \omega_0$: $I = A_0 \exp(-\frac{(C_v + C_K)}{2} \cos(\omega t + \varphi_0). \quad (18)$

2. $\beta = \omega_0$: $I = (A_0 + B_0 t \exp(-\frac{(C_v + C_K}{2} t)$. (19)

3. $\beta \succ \omega_0 : I = A_0 \exp(-y_1 t) + B_0 \exp(-y_2 t)$, (20)

де

$$y_{12} = \beta \pm \left(\begin{array}{l} \frac{(C_v + C_K)^2}{4} - (C_{d1} + C_{d2} + Z_p + R + DR + D_i + ((x_v + y_v) - e^{x_u + y_v}) + \frac{1}{n_i} + \\ + \frac{x_1}{\sum_{i=1}^{n} x_i} + (C_v + C_k)_i \cdot (C_v + C_k) + (\bar{P}_{ij} - \frac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \frac{\sum_{v \in V} C_{v1}}{N^2} + \\ + \frac{ft\ (r+1)^{-f}}{r-1} - (\bar{I} + I)(C_{d2} + C_{d1})(C_v + C_k) \end{array} \right)^{\frac{1}{2}} .$$

На рис. 2, 3, 4 наведено залежності показниказахищеності інформаційної системи з урахуванням умов (18), (19), (20).

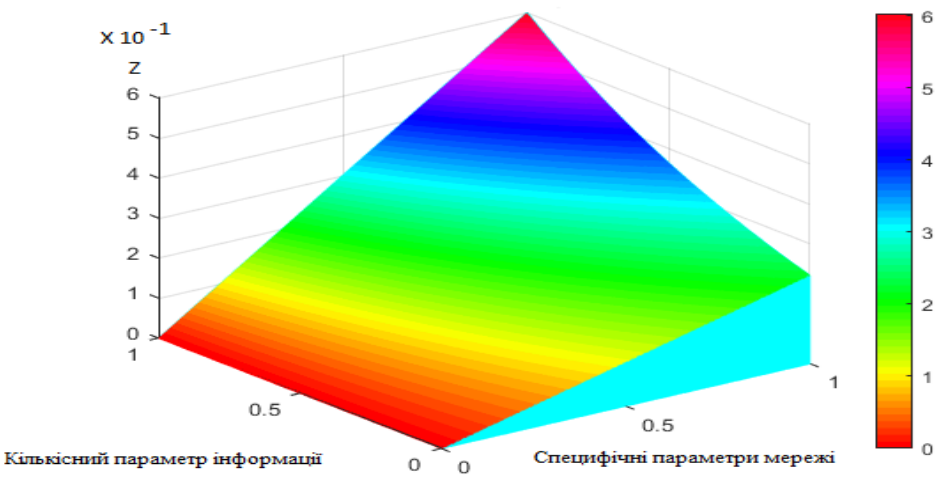

Рисунок 2 - Залежність захисту персональних даних за умови (18)

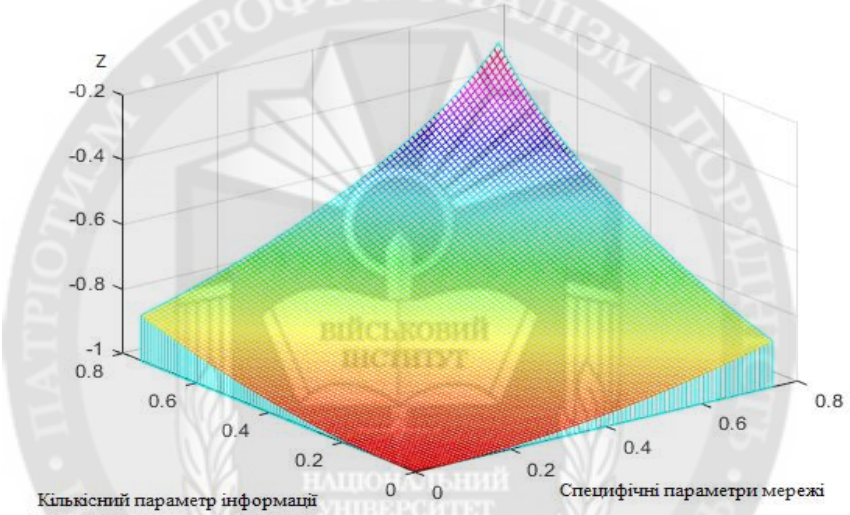

Рисунок 3 - Залежність захисту персональних даних за умови (19)

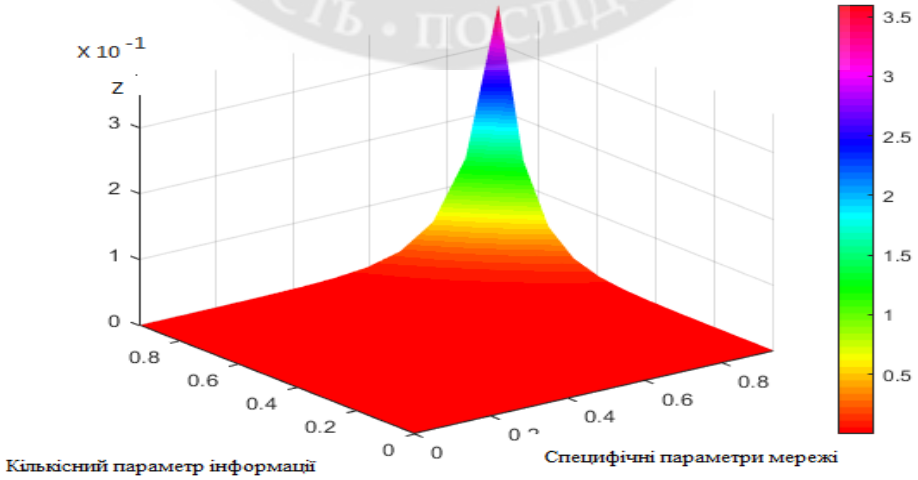

Рисунок 4 - Залежність захисту персональних даних за умови (20)

Розглянувши три варіанти розв'язання рівняння близько стаціонарного стану системи, можна прийти до висновку, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненціальним згасаючим законом. Виконаємо більш наочний аналіз поведінки системи, перейшовши від диференціальної форми рівнянь (5, 6) до дискретної і промоделювавши деякий інтервал існування системи. А саме:

$$\begin{cases} \frac{I_{n+1}-I_n}{\Delta t} = (C_{d1}+C_{d2})Z_n - (C_v + C_K)I_n); \\ \frac{Z_{n+1}-Z_n}{\Delta t} = Z_p - (C_{d2}+C_{d1})I_n - (Z_p + R + DR + D_i + ((x_v + y_v) - e^{x_u+y_v}) + \frac{1}{n_i} + \\ + \frac{x_1}{\sum_{i=1}^{n} x_i} + (C_v + C_k)_i \cdot (C_v + C_k) + (\bar{P}_{ij} - \frac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \frac{\sum_{v \in V} C_{v1}}{N^2} + \\ + \frac{ft\ (r+1)^{-f}}{r-1} - (\bar{I} + I)(C_{d2} + C_{d1})(C_v + C_k)(C_v + C_k)I_n). \end{cases} \quad (21)$$

$$\begin{cases} I_{n+1} = I_n + (C_{d1}+C_{d2})Z_n - (C_v + C_K)I_n)\Delta t; \\ Z_{n+1} = Z_n + (Z_n - I_n(C_{d2} + C_{d1} + Z_p + (R + DR + D_i + ((x_v + y_v) - e^{x_u+y_v}) + \frac{1}{n_i} + \\ + \frac{x_1}{\sum_{i=1}^{n} x_i} + (C_v + C_k)_i \cdot (C_v + C_k) + (\bar{P}_{ij} - \frac{N_{ij}}{P_{ij}} + \bar{N}_{ij}) + (\alpha + \beta + \theta + \rho)V_i - \frac{\sum_{v \in V} C_{v1}}{N^2} + \\ + \frac{ft\ (r+1)^{-f}}{r-1} - (\bar{I} + I)(C_{d2} + C_{d1}))(C_v + C_k)(C_v + C_k))\Delta t. \end{cases} \quad (22)$$

Виходячиіз умови стаціонарної позиції системи, *I*та*Z* будуть дорівнювати 0.5 та 0.5. Крок моделювання приймемо за 0.1 для всіх ітерацій моделювання. Величини I_{sp}, Z_{sp} відображають стаціонарні значення параметрів, якщо такі були досягнуті за кінцеве число ітерацій. Далі проведемо імітаційне моделювання для значень $\beta \prec \omega_0, \beta = \omega_0, \beta \succ \omega_0$ з відхиленням від стаціонарної позиції системи (табл. 1).

Таблиця 1

Параметри моделювання

№	Z_p	I	Z	C_v	C_{d1}	C_{d2}	C_K	D	R	Параметри
1	1	0,5	1	2	3	3	1	1	1	$\beta \prec \omega_0$
2	1	0,5	1	0,6	1	1	0,6	1	1	$\beta = \omega_0$
3	1	0,5	1	6	1	1	6	0,5	1	$\beta \succ \omega_0$
№	x_v	y_v I	y_u Z	n_i	V_i	x_i	P_{ij}	N_{ij}	α	Параметри
1	1	0,5	1	1000000	0,1	0,5	1	1	0,8	$\beta \prec \omega_0$
2	1	0,5	1	1000000	0,1	1	1	1	0,8	$\beta = \omega_0$

3	1	0,5	1	1000000	0,1	1	6	0,5	0,8	$\beta \succ \omega_0$
№	β	θ_I	ρ	n	C_{v1}	N	f	t	r	Параметри
1	0,5	0,2	0,5	1000000	1	0,5	1	1	1	$\beta \prec \omega_0$
2	0,5	0,2	0,5	1000000	1	0,5	1	1	1	$\beta = \omega_0$
3	0,5	0,2	0,5	1000000	1	1	6	0,5	1	$\beta \succ \omega_0$

Візуалізація результатів (рис. 5-7).

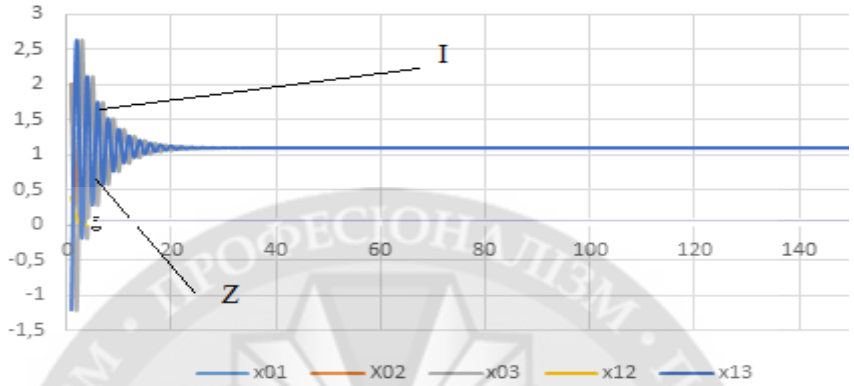

Рисунок 5 - Залежність інтенсивності та захисту даних від кількості ітерацій, дані складових взято з табл. 1: $\beta \prec \omega_0$, через і позначено кількість ітерацій

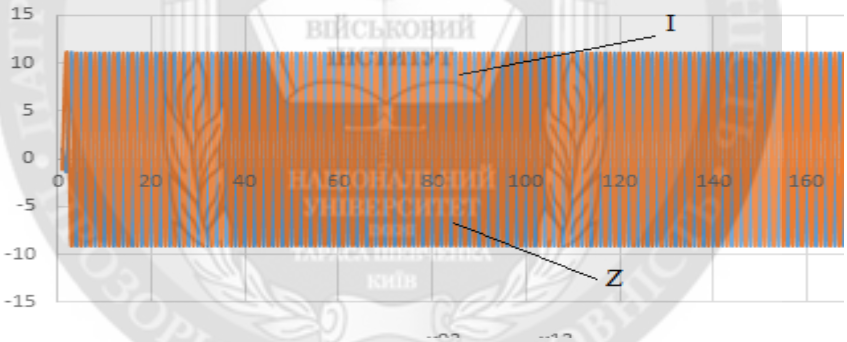

Рисунок 6 - Залежність інтенсивності та захисту даних від кількості ітерацій: $\beta = \omega_0$, Di=0,5

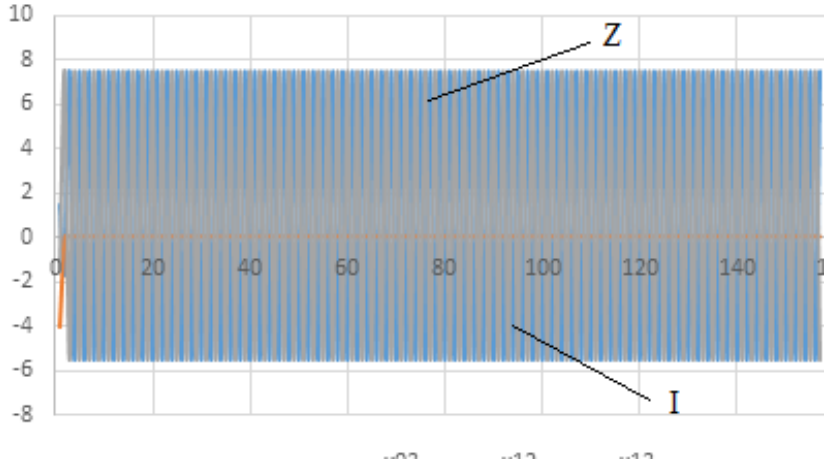

Рисунок 7 - Залежність інтенсивності та захисту даних від кількості ітерацій: $\beta \succ \omega_0$, Di=0,1

Аналіз графічних залежностей лінійної системи рис. 8 вказує на нелінійність системи. Як бачимо з аналізу графіків, коефіцієнт захисту соціальної мережі не приймає нульові значення, що цілком відповідає реальності. Не може бути захист інформації при відсутності довіри до інформації, інформація у такому випадку просто існує та не потрібує захисту бо користувачу інформація не потрібна. Бачимо, що коефіцієнти, які залежать від репутації на багато менш впливають на коефіцієнт захисту ніж коефіцієнти, які залежать від довіри. Це теж цілком відповідає логічному мисленню, бо параметр репутації обумовлює необхідну умову, але не достатню. Достатня умова залежить від параметру довіри.

Таким чином результати моделювання остаточно довели, що головним параметром який впливає на захист інформації є параметр довіри. Інші специфічні параметри соціальної мережі впливають на коефіцієнт захисту значно менше.

Висновки. Удосконалено математичну модель захисту інформації в соціальної мережі в залежності від її специфічних параметрів.

Проведено імітаційне моделювання удосконаленої моделі захисту інформації у соціальної мережі в залежності від її специфічних параметрів. Отримані графічні результати, які відображають актуальну картину захисту інформації соціальної мережі від зовнішніх впливів. Результати моделювання показали, що коефіцієнти, які залежать від репутації на багато менш впливають на коефіцієнт захисту ніж коефіцієнти, які залежать від довіри. Це доводить, що параметр репутації лежить в основі необхідної умови, але не достатньої. В основі достатньої умови лежить довіра.Отримані результати підтверджують адекватність розробленої математичної моделі захисту інформації у соціальної мережі.

Подальший розвиток запропонованої моделі полягає у більш детальному розгляді специфіки соціальної мережи та параметрів інформаційного захисту.

REFERENCES:

1. Akhramovich V.M. Limit probabilities of data security and user interaction in the social network. Magyar Tudományos Journal. Budapest, Hungary. 2020. № 41, pp. 25–31. www.magyar–journal.com.
2. Amin Mahmoudi, Mohd Ridzwan Yaakub, Azuraliza Abu Bakar. The Relationship between Online Social Network Ties and User Attributes. ACM Transactions on Knowledge Discovery from DataVolume 13, Issue 3, July 2019, Article No. 26, pp. 1–15 https://doi.org/10.1145/3314204
3. Barabasi L. A., Albert R., Jeong H. Scale-free characteristics of random networks: the topology of the world-wide web. Physica A. 2000. V. 281, pp. 69–77.
4. Bindu P.V., Thilagam P.S., Ahuja D. Discovering suspicious behavior in multilayer social networks. Computers in Human Behavior, Vol. 73, 2017, pp. 568–582.
5. Dang-Pham D., Pittayachawan S., V. B. Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. Computers & Security, Vol. 68, July 2017, pp. 1–15.
6. Davydenko V.A., Romashkina G.F., Chukanov S.N. Modelirovanie sotsial'nkh setei [Modeling social networks]. Vestnik Tyumenskogo gosudarstvennogo universiteta – Vesntik TSU, No. 1, 2005, pp. 68–79.
7. Gatti M. Large-Scale Multi-agent-Based Modeling and Simulation of Microblogging-Based Online Social Network. Multi-Agent-Based Simulation XIV. MABS. 2014, pp. 17−33.
8. Gubanov D., Chkhartishvili A. A conceptual approach to the analysis of online social networks. Upravlenie bol'shimi sistemami – Large-Scale Systems Control, No. 45, 2013, pp. 222−236.
9. Akhramovich V.M. Communication and influence of users in social networks. Colloquium–journal. Warszawa, Polska. 2020. №3 (55), pp. 21–25.
10. Oleg Barabash, Oleksandr Laptiev, Oksana Kovtun, Olga Leshchenko, Kseniia Dukhnovska, Anatoliy Biehun. The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 9, September 2020, pp. 5713–5718. DOI:10.30534/ijeter/2020/130892020
11. Barabash Oleg, Laptiev Oleksandr, Tkachev Volodymyr, Maystrov Oleksii, Krasikov Oleksandr, Polovinkin Igor. The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 8, August 2020, pp. 4133 – 4139. DOI:10.30534/ijeter/2020/17882020

12.Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksandr Laptiev, Svitlana Lehominova, Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 5, May 2020, pp. 2019 – 2025. DOI:10.30534/ijeter/2020/90852020

13.Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksandr Laptiev, Ivanna Salanda The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER), Volume 8. No. 5, May 2020, pp. 1920 – 1925. DOI:10.30534/ijeter/2020/73852020

14.Laptiev Oleksandr, ShuklinGerman, Savchenko Vitalii, Barabash Oleg, MusienkoAndrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Volume 8, No. 6. November - December 2019, pp. 2840 – 2846. DOI: 10.30534/ijatcse/2019/26862019

15.Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants. The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). Conference Proceedings Kyiv, Ukraine, November 25-27, pp. 176 –181.

16.Valentyn Sobchuk, Volodymyr Pichkur, Oleg Barabash, Oleksandr Laptiev, Kovalchuk Igor, Amina Zidan. Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). Conference Proceedings Kyiv, Ukraine, November 25-27, pp. 206 –211.

17.Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, Ukraine, November 25-27, pp. 246 –251.

18.Oleg Barabash, Andrii Musienko, Spartak Hohoniants, Oleksandr Laptiev, Oleg Salash, Yevgen Rudenko, Alla Klochko. Comprehensive Methods of Evaluation of Efficiency of Distance Learning System Functioning. International Journal of Computer Network and Information Security(IJCNIS), IJCNIS. Vol. 13, No. 1, Feb. 2021, pp. 16–28. DOI: 10.5815/ijcnis.2021.01.02

19.Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering», pp. 24–31. DOI:10.21303/2461-4262.2021.001615

20.Laptiev O., Savchenko V., Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021, pp. 15–21.

21.Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevskyi, Oleksandr Kolos, Viktor Hudyma. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021, pp. 48–54.

22.Oleg Barabash, Oleksandr Laptiev, Valentyn Sobchuk, Ivanna Salanda, Yulia Melnychuk, Valerii Lishchyna. Comprehensive Methods of Evaluation of Distance Learning System Functioning. International Journal of Computer Network and Information Security (IJCNIS). Vol. 13, No. 3, Jun. 2021, pp.62–71. DOI: 10.5815/ijcnis.2021.03.06

23.Bataeva I.P. Information protection and information security. NiKa. 2012. URL: https://cyberleninka.ru/article/n/zaschita-informatsii-i-informatsionnaya (10.06.2019).

24.Vynnyk V. D. Social networks as a phenomenon of the organization of society: the essence and approaches to the use and monitoring. Philosophy of Science. 2012. №4 (55), pp. 110–126.

Doctor of Technical Sciences Lukova-Chuiko N.V.,
Doctor of Technical Science Laptev O.A.,
Doctor of Technical Science Barabash O.V.,
Doctor of Technical Science Musienko A.P.,
Doctor of Technical Sciences Akhramovich V.M.

THE METHOD OF CALCULATION OF PERSONAL DATA PROTECTION ON THE BASIS OF A SET OF SPECIFIC PARAMETERS OF SOCIAL NETWORKS

In Ukraine, the right to protection of personal data is a constitutional guarantee, and the protection of personal data is one of the areas in which such a guarantee should be implemented. The subject of our research will not be objects in general, but dynamic systems of information protection in social networks in the mathematical sense of the term. The study developed a linear mathematical model and conducted a survey of the model of protection of personal data from a set of specific network parameters and the intensity of data transmission in social networks.

Dependencies are considered: the amount of information flow in the social network from the components of information protection, personal data, and data flow rate; security of the system from the size of the system and from the amount of personal data; information security threats from a set of specific network parameters.A system of linear equations is obtained, which consists of the equation: rate of change of information flow from social network security and coefficients that reflect the impact of security measures, amount of personal data, leakage rate, changes in information protection from a set of specific network parameters, its size, personal data protection As a result of solving the system of differential equations, mathematical and graphical dependences of the indicator of personal data protection in the social network on various components are obtained. Considering three options for solving the equation near the steady-state of the system, we can conclude that, based on the conditions of the ratio of dissipation and natural frequency, the attenuation of the latter to a specific value is carried out periodically, with attenuation: amplitude, or exponentially fading law. A more visual analysis of the system behavior is performed, moving from the differential form of equations to the discrete one and modeling some interval of the system's existence.

Mathematical and graphical dependences of the frequency of natural oscillations of the system, the period of oscillations, and the attenuation coefficient are presented. Simulation modeling for values with deviation from the stationary position of the system is performed. As a result of the simulation, it is proved that the social network protection system is nonlinear.

Keywords: social network, information flow, trust, reputation, modeling, protection factor, security, information protection.