МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені Тараса Шевченка

Кваліфікаційна наукова
праця на правах рукопису

ЛАПТЄВ СЕРГІЙ ОЛЕКСАНДРОВИЧ

УДК 004.056.53

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ З УРАХУВАННЯМ СПЕЦИФІКИ СОЦІАЛЬНИХ МЕРЕЖ

12 Інформаційні технології
125 Кібербезпека та захист інформації

Подається на здобуття наукового ступеня
доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ С.О. ЛАПТЄВ

Науковий керівник:
Толюпа Сергій Васильович,
доктор технічних наук, професор

Київ – 2025

АНОТАЦІЯ

Лаптєв С.О. Моделі та методи захисту персональних даних з урахуванням специфіки соціальних мереж. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 «Кібербезпека». – Київський національний університет імені Тараса Шевченка, Київ, 2025.

У сучасному світі усі розвинені країни Європи стурбовані проблемою інформаційної безпеки. Інформаційної безпеки не тільки Держави, а і інформаційної безпеки персональних даних своїх громадян. Широка інформатизація й оцифровка інформації набули широкого поширення у всіх країнах та сферах діяльності людини. Це привело не тільки до позитивних, а і до негативних наслідків. Об’єм інформації значно збільшився, що привело к додатковим проблемам захисту даних та інформації у цілому. Одним з головних напрямків захисту інформації та даних стає захист персональної інформації з урахуванням специфіки параметрів функціонування інформаційних мереж.

Інформаційні мережі є одним з основних методів комунікацій, пошуку зв'язків та обміну як загальнодоступною, так і конфіденційною інформацією. Соціальні мережі, як складова інформаційних систем, становлять постійно зростаючу частку серед загальних інформаційних мереж. Крім того, сама мережа набуває нових властивостей, діючи як самостійний фактор. Оскільки інформація в глобальній мережі існує завжди, 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 й економічні інтереси та можливості.

Захист персональних даних в умовах сучасного інформаційного життя являється чи не найважливішим аспектом у задоволенні безпечного використання усіх можливостей нинішніх технологій. Однак, разом зі зручністю та швидкістю обміну, пов'язані й питання безпеки. Кожен з нас прагне зберегти приватність та конфіденційність своїх даних, тому захист інформації є надзвичайно важливим аспектом в розробці програмних засобів комунікації. Десятки мільйонів людей по всьому світу щорічно стають жертвами крадіжок персональних даних. Користувачі мережі втрачають величезні гроші через шахраїв, які використовують їхні дані у незаконний спосіб, і жертвою цього може стати абсолютно будь-яка людина. Згідно з дослідженнями, в 2022 році викрадення даних завдало збитків у розмірі 16 мільярдів доларів 15,4 мільйонам споживачів у Сполучених Штатах. У тому ж році британська організація з запобігання шахрайства Cifas зафіксувала майже 173 тисячі випадків шахрайства, пов’язаних з особистими відомостям. Для нашої країни дуже масштабна кібератака була на мережу стільнікового звязку «Київстар», яку здіснила 12 грудня 2023 року російське хакерське угруповування Killnet. Це приклад найбільших випадків шахрайства за останні 13 років. Особливо це стосується інформаційних мереж, які частише за все використовують шахраї. Тому проблеми дослідження параметрів та специфіки параметрів функціонування інформаційних мереж для подальшого їх використання щодо вирішення задач захисту особистих та персональних даних є важливою та актуальною.

У дисертаційній роботі досліджено стратегічні напрямки захисту персональної інформації у окремих глобальних мережах. Проведено аналіз, властивостей інформації та особливості надання людиною персональної інформації з метою виявлення особливо важливих факторів для вирішення питання захисту персональної інформації. Представлено стратегічні пріоритети

розвитку системи захисту персональної інформації та припинення її витоку. На підставі проведеного аналізу факторів впливу на процеси передачі особистої інформації у глобальних мережах було визначено, що сучасні системи захисту персональної інформації не у повній мірі враховують параметри функціонування інформаційних мереж.

Доведено, що існуючі науково-методичні підходи, щодо проблеми захисту персональної інформації, мають певні недоліки. Загальним недоліком є те, що не використовується комплексний підхід, який би систематизував і узагальнив методи захисту персональної інформації. Не вирішується проблема аналізу параметрів поведінки системи захисту під час та після зовнішніх впливів на систему захисту персональних даних з урахуванням динаміки зміни параметрів впливу. Існуючі моделі не у повної мірі враховують запізнення реагування на атаку, параметр комплексної довіри, параметр розширення інформаційних мереж. При оцінювані безпеки персональних даних не проводиться об'єктивна оцінка балансу між загрозами безпеки інформації та специфічними параметрами функціонування інформаційної мережі, такі як параметр сильних та слабких зв’язків між користувачами та не оцінюються економічні витрати на захист персональної інформації з урахуванням специфіки функціонування мереж.

На підставі проведеного аналізу, результатів вивчення наукових публікацій за темою дослідження дисертацій, патентів, монографій та практичних розробок встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій існує об’єктивне протиріччя між існуючими методами захисту персональних даних та необхідністю ефективного та надійного захисту персональних даних з урахуванням специфіки соціальних мереж. Вирішенню цього наукового завдання і присвячена дисертаційна робота.

Наукова новизна одержаних результатів полягає в тому, що:

Вперше розроблено математичну модель захисту персональних даних у соціальних мережах, яка базується на моделі Лотки-Вольттери та враховує такі параметри функціонування мережі: запізнення реагування на атаку, параметр загальної довіри та параметр розширення соціальної мережі. Модель дозволяє провести об'єктивну оцінку балансу між загрозами безпеки інформації та специфічними параметрами мережі.

Удосконалено метод оцінки поведінки системи захисту персональних даних, який відрізняється від існуючих застосуванням запропонованої моделі та оцінювання стійкості системи за допомогою методу фазової площини. Метод дозволяє знайти характеристики особливих точок, ізольованих замкнутих траєкторій, що, в свою чергу, дозволяє оцінити динаміку досліджуваної нелінійної динамічної системи в широкому діапазоні можливих початкових умов без отримання остаточних рішень диференціальних рівнянь.

Набув подальшого розвитку метод деперсоналізації даних для захисту персональної інформації в мережах, який, на відміну від існуючих, базується на розробленій моделі захисту. Запропонований метод дозволяє забезпечити ефективний захист персональної інформації в системах обробки даних інформаційної мережі.

Практична реалізація одержаних в роботі результатів полягає в науково-методичному забезпеченні системи безпеки персональних даних з урахуванням специфіки соціальних мереж та дозволяє вирішувати задачі ліквідування наслідків загроз та їх дестабілізуючих факторів.

Наведені науково-обґрунтовані практичні рекомендації які дозволяють підвищити ефективність захисту цілісності, конфіденційності та доступності персональної інформації на 10-12% відсотків більше ніж ефективність захисту за існуючими методами. Реалізація зазначеного науково-методичного апарату

наддасть можливість підвищити ефективність захищеності персональних даних у мережах за рахунок врахування специфіки соціальних мереж таких як: запізнення реагування на атаку, загальної довіри, розширення інформативних мереж, урахування сильних та слабких зв’язків між користувачами.

Відсутність аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

Напрямками наступних досліджень є подальше удосконалення запропонованих методів виявлення зовнішніх впливів на середовища збереження персональних даних, що дозволить зменшити загальний вплив дестабілізуючих факторів різного роду під час експлуатації таких систем.

Ключові слова: агент, алгоритм, атака, безпека, верифікація, відмова, дані, дослідження, запізнення, захист інформації, збіжність, інформаційні технології, кібербезпека, кіберзагроза, кібер простір, конфіденційність, кріптоаналіз, метод, модель, надійність, нелінійна система, оптимізація, персональні дані, прогнозування, соціальна мережа, стійкість, фазовий портрет

ANOTATION

Laptiev S.O. The model and methods of protection of personal data, taking into account the specifics of the parameters of the functioning of information networks.

Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of Doctor of Philosophy in the field of knowledge 12 Information technologies in the specialty 125 "Cyber security". – Taras Shevchenko National University of Kyiv, 2024.

In today's world, all developed European countries are concerned about the problem of information security. Information security not only of the State, but also information security of personal data of its citizens. Wide informatization and digitization of information have become widespread in all countries and spheres of human activity. This led not only to positive, but also to negative consequences. The volume of information has increased significantly, which has led to additional problems of data protection and information in general. One of the main areas of information and data protection is the protection of personal information, taking into account the specific parameters of the functioning of information networks.

Information networks are one of the main methods of communication, finding connections and sharing both public and confidential information. Social networks, as a component of information systems, constitute a constantly growing share among general information networks. In addition, the network itself acquires new properties, acting as an independent factor. Since information in the global network always exists, the network itself becomes an active agent of human influence, keeping, first of all, publicly available large volumes of data. In recent years, the vision of the problem of cyber security has begun to change significantly. Because a person increasingly ceases

to be only a subject of cybercrimes. It becomes an object in itself, not only its financial and economic interests and its capabilities.

The protection of personal data in the conditions of modern information life is perhaps the most important aspect in satisfying the safe use of all the possibilities of current technologies. However, along with the convenience and speed of exchange, there are security issues. Each of us strives to preserve the privacy and confidentiality of our data, therefore information protection is an extremely important aspect in the development of communication software. Tens of millions of people around the world become victims of personal data theft every year. Netizens lose huge amounts of money due to fraudsters who use their data in an illegal way, and absolutely anyone can become a victim of this. According to research, data theft will cost 15.4 million consumers in the United States $16 billion in 2022. In the same year, the British fraud prevention organization Cifas recorded almost 173,000 cases of identity fraud in the UK. For our country, there was a very large-scale cyber attack on the Kyivstar cellular communication network, which was carried out on December 12, 2023 by the Russian hacker group Killnet. This is an example of the largest cases of fraud in the last 13 years. This especially applies to information networks, which are most often used by fraudsters. Therefore, the problems of researching the parameters and the specifics of the parameters of the functioning of information networks for their further use in solving the problems of personal and personal data protection are important and relevant.

The dissertation examines the strategic directions of personal information protection in separate global networks. An analysis of the properties of information and the peculiarities of the provision of personal information by a person was carried out in order to identify particularly important factors for solving the issue of personal information protection. The strategic priorities for the development of the personal

information protection system and stopping its leakage are presented. Based on the analysis of factors influencing the processes of transferring personal information in global networks, it was determined that modern personal information protection systems do not fully take into account the parameters of the functioning of information networks.

It has been proven that the existing scientific and methodical approaches to the problem of personal information protection have certain shortcomings. A general drawback is that no comprehensive approach is used that would systematize and generalize the methods of personal information protection. The problem of analyzing the parameters of the behavior of the protection system during and after external influences on the personal data protection system, taking into account the dynamics of changes in the parameters of the influence, is not solved. Existing models do not fully take into account the delay in responding to an attack, the parameter of complex trust, the parameter of the expansion of information networks. When assessing the security of personal data, there is no objective assessment of the balance between information security threats and specific parameters of the functioning of the information network, such as the parameter of strong and weak ties between users, and the economic costs of protecting personal information are not assessed taking into account the specifics of the functioning of networks.

On the basis of the conducted analysis, the results of the study of scientific publications on the topic of research, theses, patents, monographs and practical developments, it was established that at the current stage of the development of progressive information technologies there is an objective contradiction between the existing methods of personal data protection and the need for effective and reliable protection of personal data taking into account the specificity of the parameters of the

functioning of information networks. The dissertation work is dedicated to the solution of this scientific task.

The scientific novelty of the obtained results is that:

For the first time, a mathematical model of protection of personal information in an information network was developed, which, unlike existing models, takes into account the following parameters of network functioning: the delay of response to an attack, the parameter of complex trust and the parameter of the expansion of the information network. The model makes it possible to conduct an objective assessment of the balance between information security threats and specific network parameters, to estimate the economic costs of protecting personal information in the information network.

The method of assessing the behavior of the personal information protection system has been improved, which differs from the existing ones by applying the proposed model and assessing the stability of the system using the phase plane method. The method allows you to find the characteristics of special points, isolated closed trajectories, which, in turn, allows you to evaluate the dynamics of the investigated nonlinear dynamic system in a wide range of possible initial conditions without obtaining final solutions of differential equations.

The method of data depersonalization for the protection of personal information in networks has been further developed, which, unlike the existing ones, takes into account specific parameters of network functioning: the delay of response to an attack, the parameter of complex trust and the parameter of information network expansion. The proposed method allows for effective protection of personal information in information network data processing systems.

The practical implementation of the results obtained in the work consists in the scientific and methodical provision of the security system of personal data taking into

account the specifics of the network functioning parameters and allows solving the problems of countering the consequences of threats and destabilizing factors.

Scientifically based practical recommendations are presented that allow to increase the effectiveness of protecting the integrity, confidentiality and availability of personal information by 10% more than the effectiveness of protection by existing methods.

The implementation of the specified scientific and methodological apparatus will provide an opportunity to increase the effectiveness of personal data protection in networks by taking into account the specifics of network functioning parameters such as: delayed response to an attack, complex trust, expansion of informational networks, taking into account strong and weak ties between users and estimating economic costs on the protection of personal information in information networks.

The lack of similar solutions in our country and abroad makes research results a priority.

The directions of further research are the further improvement of the proposed methods of detecting external influences on the personal data storage environment, which will allow to reduce the overall impact of destabilizing factors of various kinds during the operation of such systems.

Keywords: agent, algorithm, attack, security, verification, denial, data, research, delay, information protection, convergence, information technology, cybersecurity, cyber threat, cyberspace, privacy, cryptanalysis, method, model, reliability, nonlinear system, optimization, personal data, forecasting, social network, resilience, phase portrait.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Лаптєв С. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. *Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка*. 2022. Том 4, №16. С. 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562

2. Лаптєв С., Собчук В., Собчук А., Лаптєва Т. Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. *Кібербезпека: освіта, наука, техніка.* 2021. Том 4, № 12. С.19 – 28. https://doi.org/10.28925/2663-4023.2021.12.1928, ISSN 2663-4023

3. Laptiev S., Tolupa S. The methodology for evaluating the functional stability of the protection system of special networks. *Наукоємні технології.* Vol. 55, № 3. 2022. P.178 – 183. https://doi.org/10.18372/2310-5461.55.16900

4. Корольков Р., Лаптєв С. Натурне моделювання атаки «war driving» на бездротову мережу. *Кібербезпека: освіта, наука, техніка.* Том 2, №18. 2022. С. 99-107. https://doi.org/10.28925/2663-4023.2022. 18.99107, ISSN 2663-4023.

5. Толюпа С., Лаптєв С. Удосконалення математичної моделі захищеності особистих даних за рахунок врахування довіри та кількісті інформації в соціальних мережах. *Безпека інформації*. 2022.Том 28, № 3. С.143–148. https://doi.org/10.18372/2225-5036.28.17371

6. Замрій І.В., Собчук А.В., Лаптєв С.О., Лаптєва Т.О., Копитко С.Б. Алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем. *Телекомунікаційні та інформаційні технології*. 2022.№ 1 (74). С.4 - 15. https://doi.org/10.31673/2412-4338.2022.010414

7. Sobchuk V., Laptiev S., Laptieva T., Barabash O., Drobyk O., Sobchuk A. A modified method of spectral analysis of radio signals using the operator approach for the fourier transform. 2024. IT, Automation, Measurements in Economy and

Environmental Protection. Vol. 14, No 2, P.56–61. https://doi.org/10.35784/iapgos.5783 **Scopus**

8. Лаптєв С. Розробка моделі захисту особистих даних у соціальних мережах. *Захист інформації*. Том 26, №1. 2024. С.43-50 https://jrnl.nau.edu.ua/index.php/ZI/article/view/18824

Наукові праці, які засвідчують апробацію матеріалів дисертації:

9. Лаптєв С.О. Удосконалення моделі виявлення загроз несанкціонованого витоку персональних даних з соціальних мереж. Науково-технічна конференція молодих вчених *«Актуальні проблеми інформаційних технологій» (APJT-2021)*19-20 жовтня 2021р. Київ. С.58 –60.

10. Laptiev S., Laptieva T. An improved method of detecting signals of unauthorized information leakage. *VIII Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем»* 11 – 12 листопада 2021р. Львів, Україна. С.115–117.

11. Лаптєв С.О., Лаптєва Т.О. Удосконалення методу захисту інформації за рахунок топологічної ідентифікації загроз. *VIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень»* 17-19 листопада 2021 р. Київ. Україна. С.92–95.

12. Savchenko V., Akhramovych V., Dzyuba T., ...Lukova-Chuiko N., LaptievA T. Methodology for calculating information protection from parameters of its distribution in social networks. *2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 – Proceedings*. 2021. С. 99 – 105. **Scopus**

13. Лаптєв С.О., Толюпа С.В., Барабаш О.В. Модель виявлення витоку інформації за допомогою топологічної ідентифікації загроз. *Математика. Інформаційні технології. Освіта.* 2022 рік: збірка тез допов. учасник. XI Міжнар.

наук.–практ. конф., 3–5 червня 2022 р. Луцьк–Світязь: СНУ імені Лесі Українки, 2022. С. 96 – 101.

14. Sobchuk V., Zamrii I., Laptiev S. Ensuring Functional Stability of Technological Processes as Cyber-physical Systems Using Neural Networks. *At the international conference on smart technologies in urban engineeringheld in Kharkiv*, Ukraine, 9-11 June 2022. Springer. https://link.springer.com/chapter/10.1007/978-3-031-20141-7_53

15. Лаптєв С., Толюпа С., Опірський І. Дослідження моделей захисту інформації у кіберфізичних системах. *V Міжнародна науково-практична конференція. «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS)* 27-28 жовтня 2022 р. Київ, Україна. Збірник матеріалів доповідей та тез. С 11-12.

16. Лаптєв С.О. Моделі та методи захисту персональних даних з урахуванням специфіки соціальних мереж. *X Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених. «Об'єднані наукою: перспективи міждисциплінарних досліджень».* 23–24 листопада 2023 р. Київ. Збірник праць конференції. С.129-130.

17. Лаптєв С. Модель захисту персональних даних з урахуванням специфіки функціонування інформаційних мереж. *1st international scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2024)",* March 6, 2024. Kyiv. C. 350-352.

LIST OF BUILDER PUBLICATIONS

Scientific papers, in which the main scientific results of the dissertation are published:

1. Laptiev S. An improved method of protecting personal data from attacks using social engineering algorithms. Electronic professional scientific publication "*Cybersecurity: education, science, technology*". 2022. 4(16), P. 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562

2. Laptiev S., Sobchuk V., Sobchuk A., Laptieva T. An improved model for estimating economic costs for the information protection system in social networks. *Cybersecurity: education, science, technology*. 2021. Vol. 4, No. 12. P.19 – 28. https://doi.org/10.28925/2663-4023.2021.12.1928, ISSN 2663-4023

3. Laptiev S., Tolupa S. The methodology for evaluating the functional stability of the protection system of special networks. *Scientific technologies*. 2022. Vol. 55, No 3, P.178 – 183. https://doi.org/10.18372/2310-5461.55.16900

4. Korolkov R., Laptiev S. Realistic simulation of a "war driving" attack on a wireless network. *Cybersecurity: education, science, technology.* 2022. No 2 (18), P. 99-107. https://doi.org/10.28925/2663-4023.2022. 18.99107, ISSN 2663-4023.

5. Tolyupa S., Laptev S. Improvement of the mathematical model of personal data security by taking into account trust and quantitative information in social networks. *Information security*. 2022. Vol. 28, No 3. P.143-148. https://doi.org/10.18372/2225-5036.28.17371

6. Zamrii I.V., Sobchuk A.V., Laptiev S.O., Laptieva T.O., Kopytko S.B. Algorithm of control and prediction of functional stability of complex information and technical systems. *Telecommunications and information technologies*. 2022. No 1. P.4 - 15. https://doi.org/10.31673/2412-4338.2022.010414

7. Sobchuk V., Laptiev S., Laptieva T., Barabash O., Drobyk O., Sobchuk A. A modified method of spectral analysis of radio signals using the operator approach for the fourier transform. 2024. IT, Automation, Measurements in Economy and Environmental Protection. Vol. 14, No 2, P.56–61. https://doi.org/10.35784/iapgos.5783 **Scopus**

8. Laptiev S. Development of a model for the protection of personal data in social networks 2024. Vol. 26 No. 1*: Ukrainian Information Security Research Journal.* P.43 – 50 https://doi.org/10.18372/2410-7840.26.18824

Scientific papers certifying the testing of the materials of the dissertation:

9. Laptiev S.O. Improvement of the threat detection model of unauthorized leakage of personal data from social networks. *Scientific and technical conference of young scientists "Actual problems of information technologies"* (ARJT-2021) October 19-20, 2021. Kyiv. P.58-60.

10. Laptiev S., Laptieva T. An improved method of detecting signals of unauthorized information leakage. *VIII International Scientific and Technical Conference "Information Protection and Security of Information Systems"* November 11-12, 2021. Lviv, Ukraine. P.115–117.

11. Laptiev S.O., Laptieva T.O. Improvement of the method of information protection due to topological identification of threats. *VIII All-Ukrainian scientific and practical conference of students, postgraduates and young scientists "United by science: perspectives of interdisciplinary research"* November 17-19, 2021, Kyiv. Ukraine. P.92–95

12. Savchenko V., Akhramovych V., Dzyuba T., ...Lukova-Chuiko N., Laptiev S. Methodology for calculating information protection from parameters of its distribution in social networks. *2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021.* Proceedings, 2021, P. 99 – 105. Scopus

13. Laptiev S.O., Tolyupa S.V., Barabash O.V. A model of information leakage detection using topological threat identification. *Math. Information Technology. Education. 2022: a collection of theses add. member. XI International science and practice conference*, June 3–5, 2022. Lutsk–Svityaz: Lesya Ukrainka State University, 2022. P. 96 – 101.

14. Sobchuk V., Zamrii I., Laptiev S. Ensuring Functional Stability of Technological Processes as Cyber-physical Systems Using Neural Networks. *At the international conference on smart technologies in urban engineeringheld in Kharkiv*, Ukraine, 9-11 June 2022. Springer. https://link.springer.com/chapter/10.1007/978-3-031-20141-7_53

15. Laptiev S., Tolyupa S., Opirskyi I. Study of information protection models in cyber-physical systems. V International Scientific and Practical Conference. *"Problems of cyber security of information and telecommunication systems" (PCSITS)* October 27-28, 2022, Kyiv, Ukraine. A collection of reports and abstracts. P. 11-12.

16. Laptiev S.O. Models and methods of personal data protection taking into account the specifics of social networks. *X All-Ukrainian scientific and practical conference of students, postgraduates and young scientists. "United by science: perspectives of interdisciplinary research"*. November 23–24, 2023. Kyiv. Proceedings of the conference. P.129-130.

17. Laptev S. The model of personal data protection taking into account the specifics of the functioning of information networks. *1st international scientific and practical conference «Information Systems and Technology: Results and Prospects»* (IST 2024)", March 6, 2024. Kyiv. P. 350-352.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БА	–	граф Барабаші-Альберт;
ВСМ	–	віртуальні соціальні мережі;
ІС	–	інформаційна система;
ЗІ	–	захист інформації;
ЗІСМ	–	захист інформації в соціальних мережах;
НППЗ	–	нелінійне правило переважного зв'язування;
ОСМ	–	облікова соціальна мережа;
СМ	–	соціальна мережа;
СПП	–	сервіс посилання повідомлень;
СЗПД	–	система захисту персональних даних;
ТОСІ	–	теорія обробки соціальної інформації;
CVSS	–	CommonVulnerability Scoring System – загальна система оцінки вразливості системи захисту інформації;
ID	–	Identity document – унікальна ознака об'єкта, що дозволяє відрізняти його від інших об'єктів, тобто ідентифікувати;
LLC	–	Logical link control – Підрівень керування логічним зв’язком.
MAC	–	Media Access Control – Унікальний ідентифікатор мережевого інтерфейсу;
NAS	–	Network Attached Storage – сервер зберегання даних на файловому рівні;

ВСТУП

Обґрунтування вибору теми дослідження. Цифровізація економіки обумовила проникнення інформаційних технологій у всі сфери суспільства і людства загалом, призвела до вразливості інформації про особистість, яка збирається в цілодобовому режимі, а суб'єктом персональних даних найчастіше не усвідомлюється не лише її збирання та обробка, а й мета таких дій. Цифрові інформаційні потоки та комунікаційні технології необхідні для ефективної роботи вузлів і частин мережевого суспільства. Термін «мережеве суспільство» стає все більш популярним у міру прискорення інформаційної революції. Створення та експоненційне зростання використання Інтернету, його інтеграція з радіомережами та телебаченням, економічні наслідки мережевої діяльності спровокували наукові та філософські дискусії щодо значення мереж для сучасного суспільства.

Все більш широке використання мережевих комунікацій може призвести до появи якісно іншої соціальної та політичної системи. Особливим результатом телекомунікаційної революції стала заміна однолінійного зв'язку між відправником і одержувачем інформації багатофункціональним і діалоговим спілкуванням, що створює нові можливості для участі в обміні інформацією. Наслідками стрімкого розвитку інформаційних технологій у світі та в Україні є значне прискорення інформатизації суспільної діяльності, посилення процесів глобалізації, інтернаціоналізації. Активізація інформаційних процесів торкнулася й системи стратегічних комунікацій суспільства, в якій провідна роль відводиться комунікативній складовій. Завдяки постійному вдосконаленню інформаційного середовища соціальні мережі перетворилися на домінуючий канал поширення інформації та спілкування громадян у віртуальному кіберпросторі. Інтернет та соціальні мережі стали дієвим та ефективним інструментом формування громадянського суспільства. Завдяки наявності засобів створення контенту в мережі Інтернет, його збереження та використання з метою задоволення інформаційних інтересів і потреб громадян, соціальні

мережі є невід’ємною частиною національного інформаційного простору. З огляду на останні події інформаційні мережі перетворилися на джерело загроз безпеці персональних даних особи.

Особиста контактна інформація описує, ким є користувач, надаючи не лише основну інформацію, таку як ім’я користувача, стать, дату народження, та сімейний стан, але й додаткові дані, такі як інформація про членство в соціальній мережі, контактна інформація, така як адреси електронної пошти, номери телефонів, ідентифікатори обміну миттєвими повідомленнями та особисті веб-сайти. Крім того, вони описують порядок денний користувача та можуть передавати особисті, політичні чи релігійні інтереси та вподобання. Користувачі часто можуть включити короткий опис про себе, описуючи свої професійні якості, погляди та думки, навички, якими вони можуть користуватися, і короткий опис того, що вони шукають.Зв'язок описує "кого знає користувач", надаючи список контактів користувача. Зокрема, Інтернет соціальні мережі - платформи з більш приватними поглядами часто просять користувача надати інформацію про стан відносин, а отже, ім'я та профіль їх контактів. Інтереси користувача описують, що його цікавить. Інформація про особисти дані користувача може бути розкрита через заяви сторонніх осіб про користувача, зроблені на форумах груп інтересів, або у вигляді анотацій чи коментарів інших користувачів.

Внаслідок поширення конфіденційної інформації користувачів у поєднанні з технологіями інформаційно-психологічного впливу на індивідуальну, колективну та масову свідомість у суспільстві можуть виникати прояви національної та релігійної ворожнечі: шантаж, знущання, крадіжки, залякування; вплив на репутацію та довіру, думку користувачів, вплив на кар'єрний ріст, сімейні стосунки тощо.

Тому, зважаючи на комплексний характер загроз безпеці персональних даних, розробка методів та моделі захисту персональних даних з урахуванням специфіки функціонування інформацйних мереж є актуальним науковим завданням, що має теоретичне та практичне значення.

Захист персональних даних в умовах сучасного інформаційного життя є чи не найважливішим аспектом у забезпеченні безпечного використання всіх можливостей сучасних технологій. Тому наукове завдання дослідження параметрів функціонування інформаційних мереж для подальшого їх використання щодо вирішення задач захисту інформації та персональних даних є важливою та актуальною. Наразі дослідженню проблем, пов'язаних із забезпеченням захисту даних у інформаційній мережі, присвячується значна частина публікацій вітчизняних і зарубіжних вчених як індивідуально, так і в складі наукових колективів. В області дослідження захисту інформації у соціальних мережах відомі роботи науковців: Горбуліна Г.Г., Хорошка В.О., Грищука Р.В., Савченка В.А., Лаптєва О.А., Молодецької К.В., Євсеєва С.П., Ланде Д.В., Гірвана М., Леонсіо Антоніо Кутільо, Міхаєля Дюрру і інших.

Проте, більшість наукових досліджень мають обмежений характер і спрямовані на вдосконалення нормативно-правового регулювання інформаційного простору, призначені для вирішення окремих часткових завдань захисту інформації, не враховують особливості процесів соціальної комунікації користувачів у віртуальних спільнотах й функціонування інформаційних мереж та не можуть бути використані як методологічна основа для розроблення системи забезпечення захисту персональних даних користувачів. Зокрема невирішеними залишаються питання, пов'язані з оперативним виявленням загроз безпеці персональних даних користувачів та розробленням дієвого комплексу заходів з протидії ним.

Таким чином, на підставі проведеного аналізу, результатів вивчення наукових публікацій за темою досліджень, дисертацій, патентів, монографій та практичних розробок встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій існує об'єктивне протиріччя між існуючими методами захисту персональних даних та необхідністю ефективного та надійного їх захисту з урахуванням специфіки соціальних мереж.

Отже, *розробка науково-методичного апарату захисту персональних даних з урахуванням специфіки соціальних мереж* є **актуальним науковим завданням**, що має теоретичне і практичне значення. Вирішенню цього наукового завдання і присвячена дисертаційна робота.

Зв'язок роботи з науковими програмами, планами, темами.

Обраний напрям досліджень відповідає Доктрині інформаційної безпеки України від 25 лютого 2017 року №47/2017 та Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, № 2163-VIII., Закону України №2297–VI «Про захист персональних даних» від 1 січня 2011 року. Постанові Верховної Ради України від 3 липня 2014 року № 1565-VII «Законодавче забезпечення розвитку інформаційного суспільства в Україні», Постанові Верховної Ради України від 31 березня 2016 року № 1073-VIII «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», тематиці науково-дослідної роботи «Методи та моделі захисту персональних даних з урахуванням специфіки соціальних мереж» (Київський національний університет імені Тараса Шевченка, 2021-2025 р.), номер державної реєстрації 0121U113248, У цій роботі особисто автором запропоновано методику ефективного захисту персональних даних з урахуванням специфіки інформаційних мереж. Ця методика на відміну від існуючих, дозволяє провести об'єктивну оцінку балансу між загрозами безпеки персональної інформації та специфічними параметрами мережі. Метод базується на моделі та алгоритмі деперсоналізації. Алгоритм деперсоналізації застосовано для рішення задач із забезпечення інформаційної безпеки персональних даних у системах де вони обробляються. Цей метод на відміну від існуючих, додатково враховує розповсюдження таргетованої інформації в інформаційній мережі.

Мета і завдання дослідження.

Метою дисертаційної роботи є підвищення ефективності захищеності персональних даних у інформаційних мережах за рахунок врахування специфіки соціальних мереж: запізнення реагування на атаку; показника загальної довіри;

параметра розширення інформаційних мереж; урахування сильних та слабких зв'язків між користувачами та оцінки економічних витрат на захист персональної інформації в інформаційних мережах.

Для досягнення поставленої мети в дисертації вирішені такі наукові завдання:

1) здійснено порівняльний аналіз існуючих моделей та методів щодо оцінювання ефективності захисту персональних даних;
2) розроблено математичну модель захисту персональної інформації в соціальних мережах;
3) удосконалено метод оцінки поведінки системи захисту персональної інформації;
4) здійснено подальший розвиток методу деперсоналізації даних для захисту персональної інформації в мережах;
5) проведено математичне моделювання з метою підтвердження достовірності методу оцінки стійкості системи захисту персональних даних.

Об'єкт дослідження – процес забезпечення захисту персональних даних користувачів з урахуванням специфіки соціальних мереж.

Предмет дослідження – моделі та методи захисту персональних даних з урахуванням специфіки соціальних мереж.

Методи дослідження. Для досягнення поставлених в дисертаційній роботі задач використано: сучасні методи теорії графів, системного аналізу (для дослідження особливостей функціонування соціальних), теорії конгнітивної логіки, управління, ймовірностей та математичної статистики (для дослідження процесів взаємодії користувачів у соціальні мережі, їх взаємного впливу та динаміки думок), теорії графів, множин, комп'ютерної лінгвістики (для методики виявлення каналів поширення інформації в соціальних мережах, пошуку співтовариств), конгнітивної, булєвої алгебри (модель сильних та слабких зв'язків користувачів).

Наукова новизна отриманих результатів дисертаційної роботи полягає у наступному:

Вперше розроблено математичну модель захисту персональної інформації в соціальних мережах, яка базується на моделі Лотки-Вольттери та враховує такі параметри функціонування мережи: запізнення реагування на атаку, параметр загальної довіри та параметр розширення соціальних мереж. Модель дозволяє провести об'єктивну оцінку балансу між загрозами безпеки інформації та специфічними параметрами мережі.

Удосконалено метод оцінки поведінки системи захисту персональної інформації, який відрізняється від існуючих застосуванням запропонованої моделі та оцінювання стійкості системи за допомогою методу фазової площини. Метод дозволяє знайти характеристики особливих точок, ізольованих замкнутих траєкторій, що, в свою чергу, дозволяє оцінити динаміку досліджуваної нелінійної динамічної системи в широкому діапазоні можливих початкових умов без отримання остаточних рішень диференціальних рівнянь.

Набув подальший розвиток метод деперсоналізації даних для захисту персональної інформації в мережах, який, на відміну від існуючих, враховує специфіку соціальної мережі: запізнення реагування на атаку, параметр комплексної довіри та параметр розширення соціальної мережі. Запропонований метод дозволяє забезпечити ефективний захист персональної інформації у системах обробки даних та соціальних мереж.

Практичне значення одержани результатів.

Запропоновані в дисертаційній роботі наукові результати можуть бути використані для підвищення ефективності захисту персональних даних в соціальних мережах від несанкціонованого доступу та інших видів зовнішніх впливів. Реалізація розробленого науково-методичного апарату надасть можливість:

- виконувати математичне моделювання процесу захисту інформації з метою отримання необхідного рівня захисту персональної інформації в соціальних мережах;

- оцінювати стан захисту персональної інформації користувачів під час та після комплексних атак на систему захисту даних зі зміною параметрів впливу на систему захисту;

– забезпечити підвищення рівня стабільності та безпеки інформаційного простору соціальних мереж за рахунок аналізу перехідних процесів системи захисту інформації.

- здійснювати загальну оцінку рівня захисту персональних даних в соціальних мережах за допомогою окремих компонентів системи: затримка реагування на атаку; комплексної довіри, враховуючи параметр розширення соціальних мереж та сильні і слабкі зв'язки користувачів в соціальних мережах.

У роботі запропоновано рекомендації щодо удосконалення моделі захисту персональних даних користувачів у соціальних мережах з урахуванням специфіки їх функціонування, що наддасть можливість підприємствам різних форм власності, які функціонують в умовах інформаційного протиборства та в умовах війни з росією, на 10-12% підвищити ефективність захисту персональних даних співробітників та користувачів соціальної мережі у порівнянні з існуючими методиками.

Результати досліджень прийняті до впровадження в Інституті програмних систем НАН України (акт від 07.02.2023 року); Науково методичному центрі кадрової політики МО України (акт від 19.10.2023 року).

Особистий внесок здобувача. Дисертаційне дослідження є самостійно виконаною роботою, в якій відображено особистий авторський підхід та особисто отримані теоретичні і прикладні результати, які стосуються розв'язання наукового завдання щодо розробки науково-методичного апарату захисту персональних даних з урахуванням специфіки соціальних мереж. Основні положення і результати дисертаційної роботи здобуто автором самостійно та

опубліковано в профільних періодичних виданнях. У наукових роботах, що опубліковані у співавторстві, в дисертаційній роботі використані лише ті результати, які становлять індивідуальний внесок автора. У статях зазначених у списку публікацій здобувача, опублікованих у співавторстві, автору належить: [2] розроблена модель системи захисту інформації в соціальних мережах, яка у подальшому удосконаліна за рахунок економічних параметрів; [3] оцінка функціональної стійкості складних інформаційно-технічних систем на основі фазових портретов; [4] моделювання атаки на бездротову мережу з метою оцінки стійкості бездротовоі мережи до можливості перехоплення прав адміністратора; [5] удосконалення моделі захисту інформації у інформаційному просторі, а саме у соціальних мережах, за рахунок врахування довіри та кількісті інформації в соціальних мережах; [6] алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем; [7] метод аналізу параметрів стійкості системи захисту інформації з використанням операторного підходу.

Наукові положення, що виносяться на захист, висновки і рекомендації дисертації належать автору.

Апробація результатів дисертації. Основні теоретичні та практичні результати дисертаційної роботи доповідались і обговорювались на десяти науково-технічних конференціях та семінарах:

- Науково-технічна конференція молодих вчених «Актуальні проблеми інформаційних технологій» (АРЈТ-2021)(19 – 20 жовтня 2021р., м Київ);
- XXVII Міжнародна науково-практична конференція «Multidisciplinary academic research and innovation»(25–28 мая 2021р., м.Амстердам);
- VIII Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (11–12 листопада 2021р., м Львів);
- VIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Об’єднані наукою: перспективи міждисциплінарних досліджень» (17–19 листопада 2021 р., м.Київ);

- International Scientific And Practical Conference “Information Security And Information Technologies”: Conference Proceedings (13 –19 September 2021, Kharkiv – Odesa); Scopus
- 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, (15-16 December, Kyiv, 2021);Scopus
- XI Міжнародна науково-практична конференція (3–5 червня 2022 р., м. Луцьк,.) ;
- V Міжнародна науково-практична конференція. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)” (27 – 28 жовтня 2022 р., м. Київ.);
- Modern information, measurement and control systems: problems, applications and perspectives’2022. (MIMCS’2022). (November 4 –5, 2022, Antalya, Turkey); Scopus
- 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT) (Kyiv,15-17 December 2022).

Публікації.

За результатами досліджень опубліковано 17 наукових праць. Основні наукові положення викладено в 8 наукових статтях [1–6, 8] у спеціалізованих фахових виданнях України, одна наукова стаття [7] у наукометрічної базі Scopus. Із них дві наукові статті [1, 8] опублікована одноосібно. За матеріалами виступів на міжнародних науково-технічних конференціях опубліковано 9 тез доповідей [9–17], з яких одна публікація [12] входить до наукометричної бази Scopus.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, трьох розділів, висновків, двох додатків на 7 сторінках та списку використаних джерел з 117 найменувань на 16 сторінках. Повний обсяг дисертації складає 177 сторінок друкованого тексту, з них 147 сторінок основного тексту у тому числі містить 44 рисунки та 25 таблиць.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ МОДЕЛЕЙ ТА МЕТОДІВ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ З УРАХУВАННЯМ ПАРАМЕТРІВ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ МЕРЕЖ

1.1. Аналіз загроз персональним даним з урахуванням впливів на інформаційні мережи

У минулому підходи до захисту персональних даних переважно зосереджувалися на виявленні та моніторингу загроз. Сучасна стратегія орієнтована на оцінювання та зниження ризиків, що дозволяє запобігти використанню вразливостей у програмному забезпеченні, які можуть завдати шкоди. Фахівці з інформаційної безпеки раніше концентрувалися на виявленні загроз, тоді як сьогодні їх основна увага спрямована на управління ризиками. Стрімкий розвиток Інтернету та соціальних мереж значно посилив небезпеку витоку персональних даних. Зважаючи на постійний розвиток кібератак, який вимагає безперервного вдосконалення методів протидії, можна дійти висновку про необхідність оновлення існуючих та створення нових способів захисту персональних даних в інформаційних мережах. Це особливо актуально для глобально-локальних мереж, тісно пов’язаних із соціальними платформами.

Соціальна мережа (СМ) – соціальна структура, утворена індивідами або організаціями в якій підтримуються соціальні відносини [62].

Послуги соціальних мереж кардинально еволюціонують у взаємодії між людьми, стаючи сьогодні фактично переважним сервісом в Інтернеті [62, 107] (рис. 1.1–1.3).

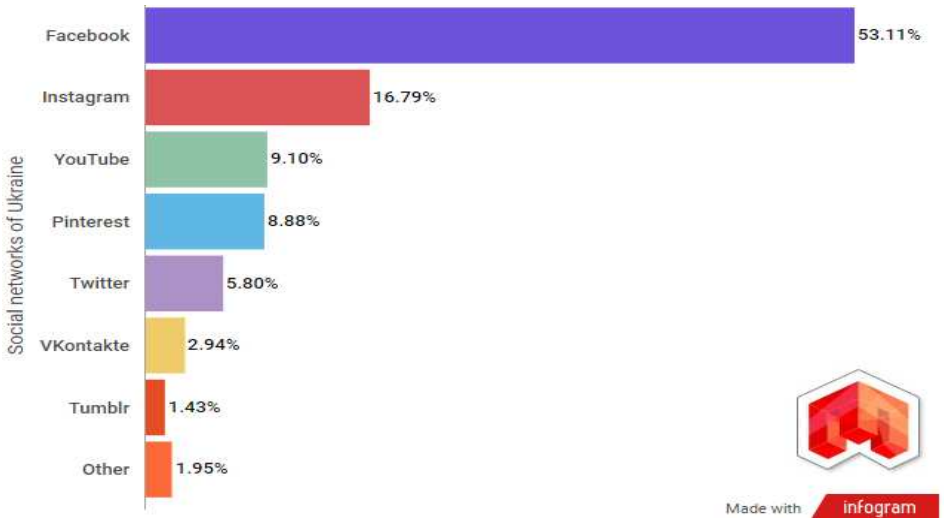

Рис. 1.1 Статистика використання соціальних мереж в Україні, % (2024р.)

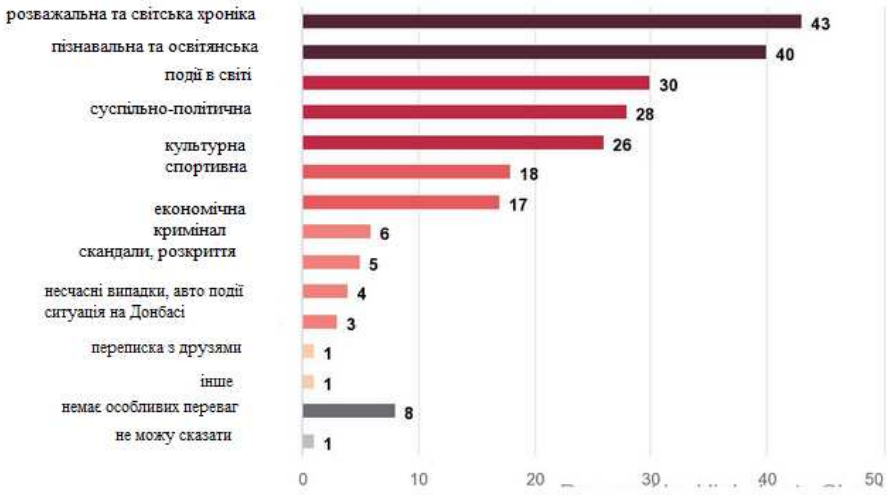

Рис. 1.2 Переваги, що віддають українці питанням у СМ, у відсотках (2024р.)

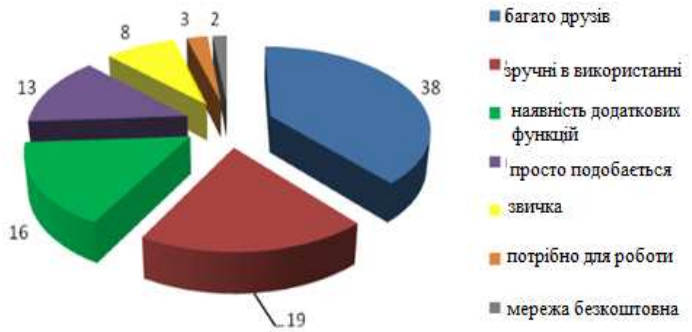

Рис. 1.3 Користувачі в СМ, у відсотках в залежності від потреб (2024 рік)

Дослідження диференціації соціальних мереж

Загалом, соціальна мережа (СМ) являє собою систему, що складається із сукупності суб'єктів та встановлених між ними взаємозв'язків.[104]. Розрізняють реальні та віртуальні (Інтернет–соціальні мережи (ІСМ)) (рис. 1.4).

Реальні соціальні мережі (РСМ). У соціальних науках термін "соціальна мережа" (СМ) стосується відносин, які об’єднують окремих осіб. Приклади таких зв’язків можна знайти між членами родини, сусідами або колегами. Оскільки учасниками цих мереж є реальні люди, їх часто називають реальними соціальними мережами.

Віртуальні соціальні мережі (ВРМ). Багато реальних соціальних мереж мають цифрове або віртуальне представлення. Наприклад, бази даних для публікації наукових праць можуть створювати мережі співавторства, цитувань або співпраці. Іншим прикладом є бази даних, такі як Інтернет-база даних фільмів [21, 24].

Аналіз персональних даних, розміщених в інтернет-соціальних мережах. Основні дані, що зберігаються в інформаційно-соціальних мережах (ІСМ), складаються з інформації, яку користувачі та їхні відвідувачі самостійно створюють і підтримують. Їх можна класифікувати за такими категоріями [15, 18, 21, 24]:

- особисті контактні дані, які характеризують користувача;
- підключення, що відображають зв’язки в трафіку соціальної мережі;
- інтереси користувача;
- автобіографічна інформація;
- спілкування, яке охоплює всі взаємодії з іншими користувачами ІСМ через систему обміну повідомленнями (СОМ).

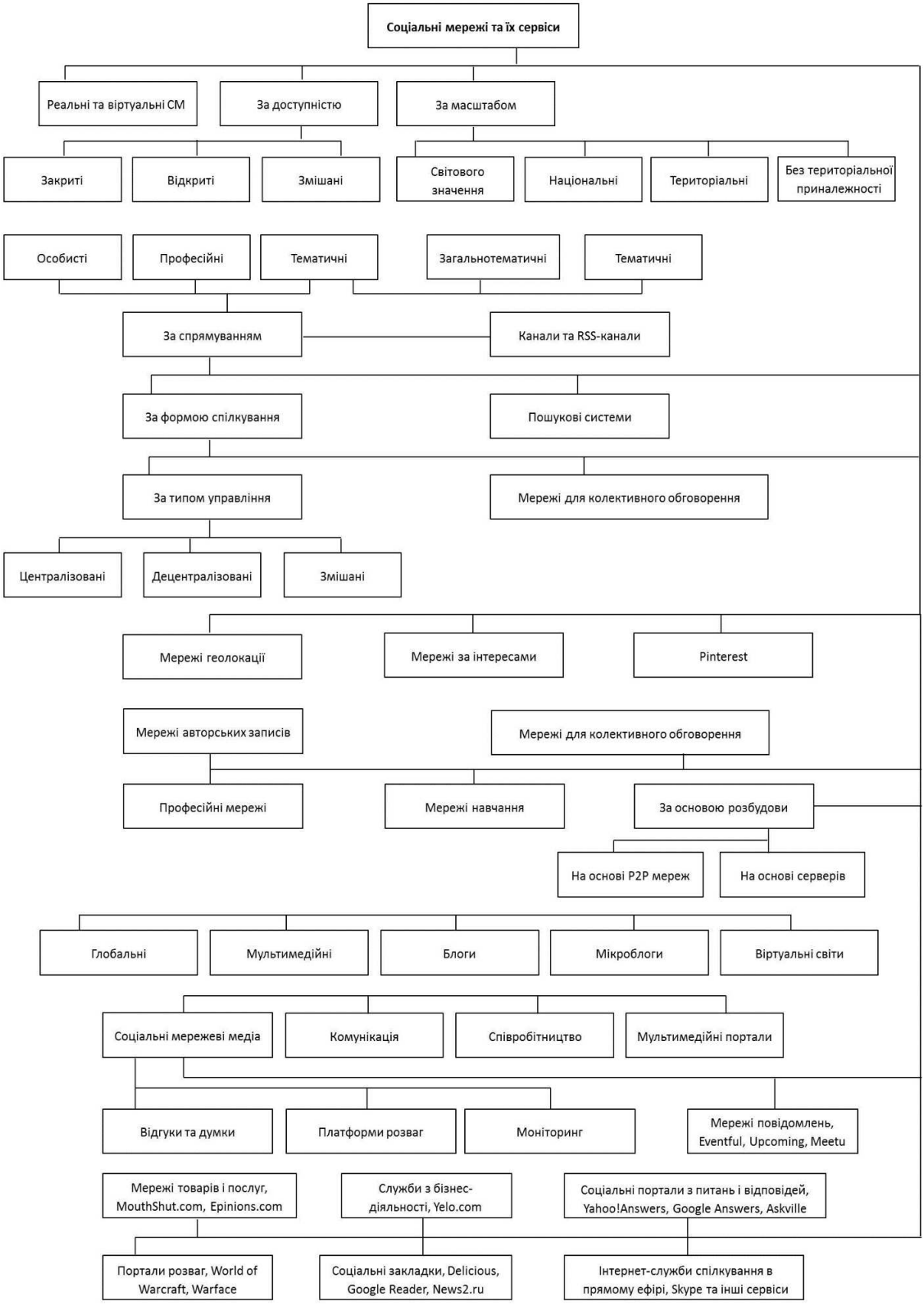

Рис. 1.4 Фрагмент класифікації ІСМ та їх сервісів

Ці типи даних формують персональну інформацію, яку користувач надає безпосередньо у системі інформаційної соціальної мережі (ІСМ). Додаткові дані про користувача часто створюються іншими учасниками ІСМ та стають доступними всередині платформи. Користувачі часто залишають короткий опис про себе, де вказують свої професійні якості, погляди, навички та цілі. Розділ "Зв'язки" демонструє коло знайомств користувача, надаючи список контактів із можливими позначками типу відносин (сім'я, колеги, друзі, партнери по спорту тощо). На платформах, орієнтованих на дозвілля або з акцентом на приватність, користувачів можуть просити надати інформацію про їхній статус у відносинах, а також профілі їхніх контактів.

Користувачі також можуть запитувати рекомендації від інших, які часто містять детальні дані про них і пояснюють характер їхнього зв’язку. Інтереси відображають захоплення та вподобання користувача, наприклад, улюблені фільми, музичні стилі, релігійні, сексуальні чи політичні погляди, а також хобі, фотографії, відео з особистого життя, підписки на фан-сторінки та членство у тематичних групах.

Автобіографічна інформація включає дані про професійну діяльність і освіту: відвідувані школи, університети, підвищення кваліфікації, здобуті звання, сертифікати, професійні навички. Вона також може деталізувати займані посади, їхню тривалість, тип, обов’язки та досягнення.

Деякі платформи додатково запитують про членство в професійних організаціях, участь у громадських чи політичних службах (клубах, асоціаціях, партіях), нагороди, відзнаки та рекомендації від інших осіб.

Комунікація описує, які повідомлення обмінюються між користувачами і з ким саме. Платформи ІСМ зазвичай надають можливості для обміну приватними повідомленнями, асинхронного спілкування через дошки оголошень і записи в гостьових книгах, які користувач може зробити видимими або прихованими для

інших, а також синхронного спілкування через чати. Це приклади прямих форм комунікації, ініційованих користувачем.

Однак існують і непрямі способи комунікації, що реалізуються іншими функціями платформ, наприклад, використання сервісів посилання повідомлень (СПП), таких як тести, вікторини або "подобається", а також публічні чи цільові запрошення на заходи.

Інформація про користувача може бути оприлюднена непрямо через коментарі, відгуки або примітки, залишені іншими користувачами. Часто такі анотації залишаються загальнодоступними на тривалий час, оскільки користувачі не завжди звертають увагу на ці записи. Інформація також може стати доступною через висловлювання сторонніх осіб на форумах, у групах за інтересами або в коментарях.

Будь-який цифровий контент, створений користувачем, може призвести до розголошення даних інших осіб. Наприклад, деякі платформи обмежують можливість публікувати фотографії, на яких зображені інші люди, якщо сам користувач не присутній на фото. Проте це не виключає публікації спільних фотографій, де зображені інші користувачі, які можуть бути позначені та безпосередньо пов’язані з цим зображенням. Крім того, до цих фотографій можуть додаватися коментарі.

Аналіз загроз контролю доступу

Більшість платформ ІСМ дозволяють користувачам налаштовувати конфіденційність через функції контролю доступу. Зокрема, користувач може регулювати видимість своєї активності в мережі, контактів зі списку, доступ до професійної інформації, завантаженого контенту чи розміщених повідомлень.

Функції конфіденційності зазвичай передбачають визначення, яка інформація підлягає захисту, і встановлення списку осіб або груп із правами

доступу. Відвідувачі можуть бути розподілені на групи, як-от "друзі", "друзі друзів", "усі" або створені користувачем категорії, наприклад, "сім'я" чи "колеги" [7, 17, 21, 104, 110] тощо. Наприклад, функція керування пошуком файлів дозволяє користувачеві контролювати доступ до своєї програми для інших користувачів. Це дає можливість окремим користувачам ІСМ приховувати певні елементи особистої профільної інформації від обраних контактів. Крім того, дані, пов'язані з онлайн-ідентифікаторами, приватними або груповими комунікаціями, такими як коментарі, позитивні чи негативні позначки, можуть бути захищені засобами обмеження щодо набору функцій мереж та даних (рис. 1.5).

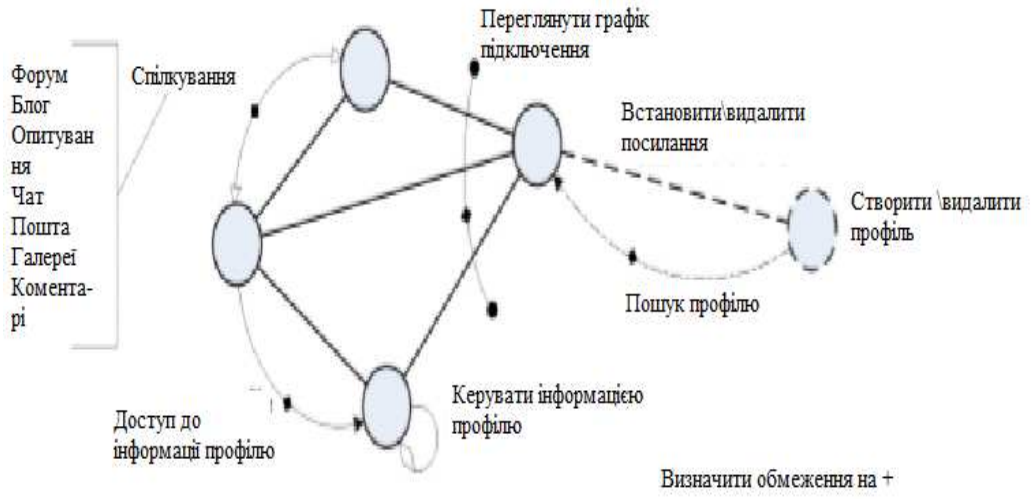

Рис. 1.5 Основні функціональні можливості типової платформи ІСМ

Проблему конфіденційності даних користувачів можна розглядати як завдання контролю за подальшим використанням цих даних. Доступ до вмісту програми має надаватися безпосередньо користувачем, і управління доступом повинно бути таким же надійним, як і сама програма. Однак цього недостатньо для забезпечення конфіденційності особистої інформації. Наприклад, якщо програма містить кілька інформаційних блоків, доступ до кожного з них повинен налаштовуватися окремо. Крім того, для забезпечення конфіденційності зв'язку необхідні методи, що гарантують:

• анонімність, тобто користувачі повинні мати можливість доступу до ресурсів чи послуг без розкриття своєї особи;

• захист від несанкціонованого збору інформації, що гарантує, що жодна третя сторона не може збирати дані про учасників спілкування та зміст їхніх повідомлень;

• відсутність зв'язку, що означає, що неможливо визначити, чи належать два повідомлення одному відправнику або отримувачу;

• неперевірність, що вимагає, щоб жодна третя сторона не могла відстежити історію дій користувачів у системі. Це вимагає забезпечення як анонімності, так і відсутності зв'язків між діями користувачів.

1.2. Аналіз відомих моделей оцінки захисту персональних даних з урахуванням специфіки соціальних мереж

Головною загрозою витоку персональних даних з мережи є соціальні мережі. Найбільший ринок для крадіжки персональних даних – це соціальні мережі. Вони містять величезну кількість особистої інформації користувачів, яку активно шукають зловмисники. На сьогодні соціальні мережі є потужними базами даних, що охоплюють різноманітну інформацію про мільйони людей по всьому світу. Чим більше людина взаємодіє в цих мережах, тим легше зібрати про неї інформацію без особливих зусиль [1, 2, 10, 23, 26, 114].

Простий образ будь-якої мережі - вузли та зв'язки, що з'єднують ці вузли. Роль вузлів у соціальних мережах виконують люди, ми з вами, а роль зв'язків – соціальні комунікації, соціальні потреби, відносини. Цей образ зображується (представляється) графом (мультиграфом) з безліччю вершин та дуг. Якщо граф не порожній, його структура може описуватися безліччю варіантів, яка розпадається на підмножини ізоморфних графів. Таким графам відповідає й

інший - матричний опис. З позиції структури соціальних мереж їх класифікація можлива математичними (алгебраїчними) методами.

Через пандемію робота в онлайн стала новою нормою у всьому світі. Незважаючи на те, що робота в онлайн має свої переваги, такі як гнучкість у часі та безпека від пандемії, віддалена робота є величезним ризиком для безпеки підприємств та особистих даних співробітників, які передають конфіденційні дані та інформацію у своїй мережі. На карту поставлені заходи безпеки мережі та безпека приватної та корпоративної інформації. Потрібні посилення роботи з конкретними протоколами безпеки, такими як SSL, TLS, VPN, IPSec і т.д., щоб запобігти будь-якій можливій загрозі атаки та захистити певну віддалену команду від кібератак. Відсутність безпеки корпоративного рівня – найбільша загроза для організацій та найпривабливіша мета для кіберзлочинців.

Мотиви та цілі збору даних.

Спостерігається збільшення кількості атак, орієнтованих на викрадення інформації (рис. 1.6).

Активні користувачі соціальних мереж мають на 30% вищий ризик стати жертвами, оскільки їхня інформація частіше може бути розкрита. Одним з джерел для злочинців є велика кількість особистої інформації, розміщеної на сторінці в соцмережі. Основною проблемою соціальних мереж є довіра до осіб у списку «друзів». Безтурботне прийняття пропозицій «дружби» від маловідомих або незнайомих людей може призвести до серйозних наслідків. Очевидно, що рівень довіри до осіб у списку «друзів» зазвичай вищий, ніж до випадкових користувачів. Це може бути корисно, адже створює лояльну аудиторію навколо бренду, компанії чи особи. Але водночас це відкриває двері для зловмисників.

Рис. 1.6 Мотиви і цілі збору даних

«Дружній» стиль спілкування, поширений у соцмережах, може вводити в оману, створюючи хибне відчуття, що навколо лише друзі та доброзичливці, з якими можна вільно ділитися будь-якою інформацією. Друга загроза полягає в так званому маскараді, або підміні особистості [2,15,71]. Третя загроза стосується злому облікових записів користувачів на соціальних ресурсах.

Ще однією проблемою є звичка використовувати однакові імена користувачів та паролі для корпоративних мереж і зовнішніх соціальних ресурсів. Крім того, не можна забувати, що соцмережі стали основними розповсюджувачами вірусів і троянів. Іншою загрозою для компаній є зростання трафіку, особливо через перегляд відеоконтенту, що може негативно впливати на економіку. Для зменшення витрат можна обмежити доступ до відео контенту для тих працівників, чиї функціональні обов'язки не вимагають перегляду такого контенту.

Небезпеки соціалізації.

Соціальні мережі є втіленням сучасних веб-технологій і об'єднують усі можливі загрози Інтернету. Ці загрози можна умовно поділити на кілька основних груп:

1. **Web-атаки**. Оскільки соціальні мережі є веб-додатками, вони можуть бути використані хакерами для атак на вразливості браузерів. Для таких атак можуть застосовуватися інструменти, як-от троянські програми, фальшиві антивіруси, соціальні хробаки, які для свого поширення використовують листування друзів, тощо [55, 86, 88].
2. **Крадіжка паролів і фішинг**. Оскільки для ідентифікації в соціальних мережах використовуються паролі, достатньо дізнатися цей конфіденційний код, щоб мати змогу відправляти рекламу або здійснювати інші заборонені дії від імені іншого користувача [2, 15, 86].

Cookies — це невеликі фрагменти даних, які веб-сервер зберігає на комп'ютері користувача для зберігання інформації, специфічної для нього, та для використання цієї інформації для різних цілей [10, 25].

Cookies можливо вкрасти. Найпростіший спосіб зробити це — отримати доступ до комп'ютера користувача. Виконати це через Інтернет-з'єднання значно важче, але викрадення файлів cookies у такий спосіб називається зломом сесії [89].

Cookies можна підмінити. Підміна cookies означає зміну його вмісту.

Витік інформації. Соціальні мережі можуть стати інструментом для витоку важливої інформації компанії або для підриву її репутації.

Трекери соціальних мереж. Соціальні мережі використовують трекери на своїх сайтах, щоб відстежувати вашу активність, перегляди та взаємодію в Інтернеті. Це дає компаніям змогу збирати інформацію про вашу історію перегляду та підвищувати ефективність реклами. Навіть якщо ви не користуєтеся соціальними мережами, трекери все одно можуть збирати дані.

Міжсайтові відстежуючі cookies — це куки, які слідують за вами від одного сайту до іншого, збираючи інформацію про вашу онлайн-активність. Це часто відбувається без вашого відома та згоди. Дані компанії та аналітичні фірми використовують ці куки для створення профілів, збору інформації про ваші інтереси та для націлювання вас на відповідну рекламу.

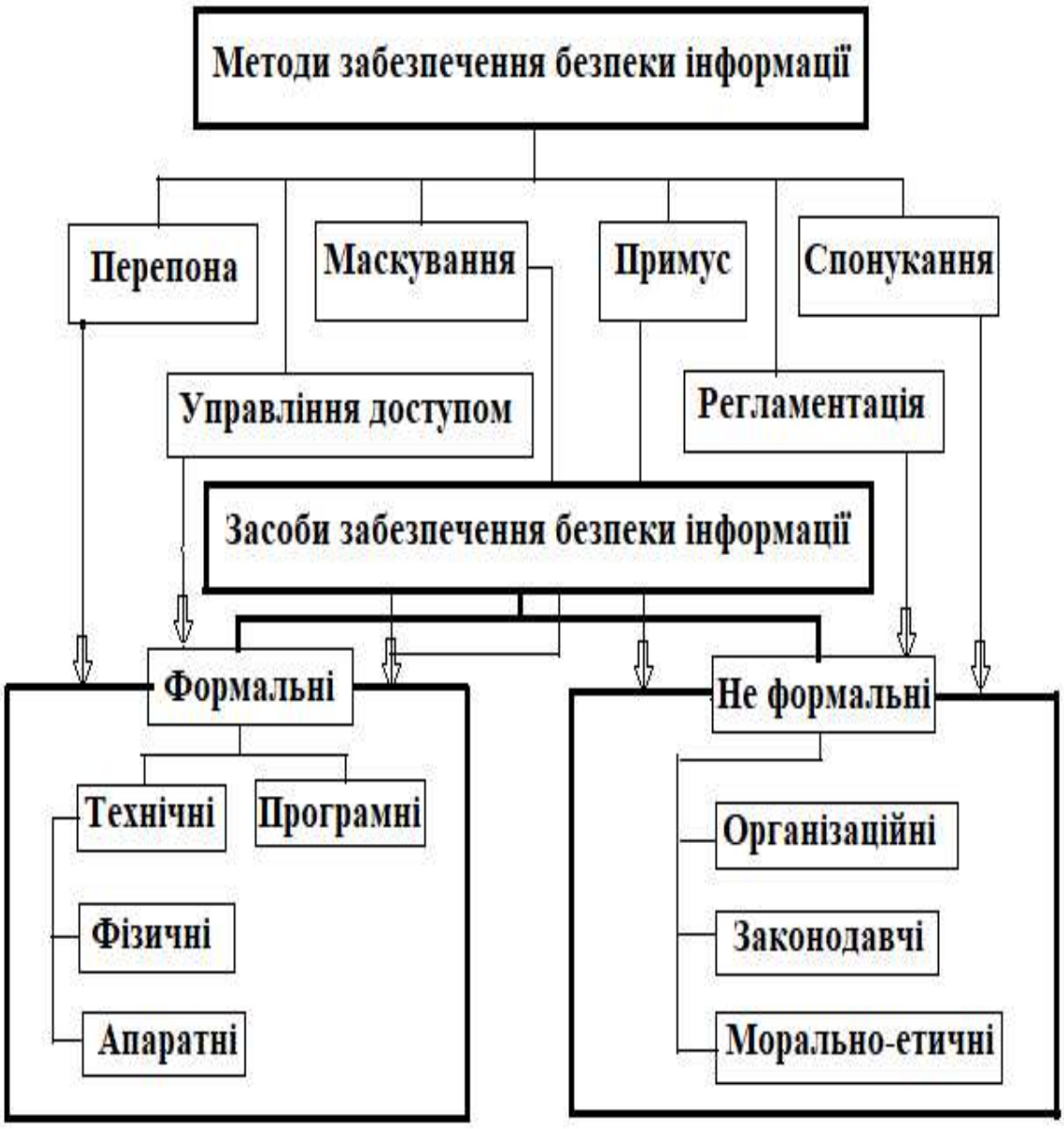

Рис. 1.7. Методи та засоби захисту інформації в соціальних мережах [72]

Блокування вмісту, що відслідковує ваші дії, може допомогти прискорити завантаження сторінок, але деякі елементи можуть не працювати належним чином або взагалі не з'являтися. Методи та засоби захисту інформації в соціальних мережах представлені на рис. 1.7.

Класифікація моделей захисту інформації, представлена на рис.1.8.

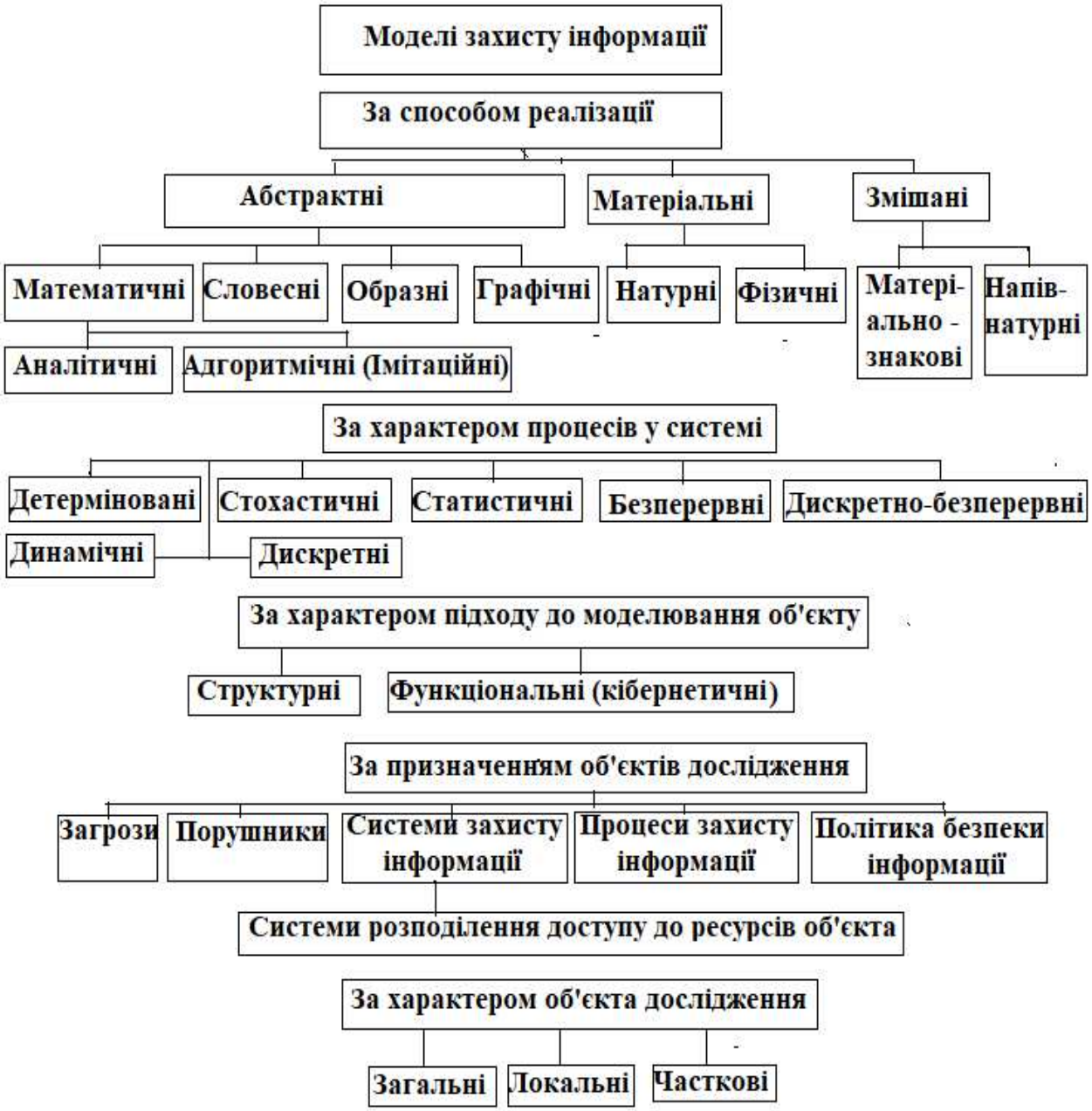

Рис. 1.8. Класифікація моделей захисту інформації [70]

Згідно [7, 20-23,79] моделі впливу загроз описуються за допомогою графа, де відповідні значення λ_a і μ_a визначають інтенсивності переходів, а S_1 представляє виникнення реальної загрози атаки. Інші загрози атаки обчислюються за наступними формулами:

$$T_{oya} = 1/\lambda_a,$$
$$\mu_a = \frac{\lambda_a K_v}{1-K_v} = 1/T_в. \qquad (1.1)$$

З урахуванням наведеного, складність реалізації загрози вразливості (S_y) можна трактувати як ймовірнісну міру обсягу інформації $I(P_{oy})$, якою зловмисник повинен володіти для здійснення цього впливу. Відповідно, вона може бути визначена наступним чином [16-19, 80, 91]

$$S_y = I(P_{oy}) = -\log_2(1-P_{oy}). \qquad (1.2)$$

Якщо розглядати атаку як процес послідовного використання зловмисником виявлених та невиправлених у системі вразливостей, що мають визначені характеристики P_{oyr} і S_{yr}, $r = 1,...,R,$ тоді запроваджується кількісна оцінка складності атаки $I(P_{oa})$, яку позначимо як S_a де $S_a = I(P_{oa})$. Ця характеристика визначається кількістю інформації, якою повинен володіти порушник для здійснення успішної атаки. Загроза, обумовлена R виявленими та невиправленими вразливостями системи, виникає за умови, що події виявлення реальних загроз є незалежними, а для здійснення атаки потрібно одночасна наявність усіх вразливостей, які формують цю загрозу.

$$S_a = I(P_{oa}) = -\log_2(1-P_{oa}) = -\log_2 \prod_{r=1}^{R}(1-P_{oya}). \qquad (1.3)$$

де: $P_{оа} = 1 - \prod_{r=1}^{R}(1 - P_{оуr})$ - ймовірність того, що вплив буде реальним в будь-який момент часу.

Нехай втрати від несанкціонованого доступу до інформації (через її розкрадання, видалення або модифікацію) становлять Cінф. Тоді ризик втрат, пов'язаних з загрозою безпеки інформаційної системи в цілому (характеристика впливу на безпеку інформаційної системи $P0a$), можна оцінити наступним чином. [30-33, 51-53, 77]

$$R_{C_{інф}} = C_{інф}(1 - P_{оа}). \tag{1.4}$$

Отже, використовуючи побудовану апроксимуючу функцію для загрози атаки, можна визначити ймовірність виникнення реальної загрози на конкретну інформаційну систему, враховуючи готовність порушника до її реалізації в будь-який момент часу t експлуатації системи. Це дозволяє оцінити ймовірність фатальної відмови через реальну атаку $P_{Ауа}(t)$ та, відповідно, величину потенційних втрат $R_{C_{інф}}(t)$.

$$R_{C_{інф}}(t) = C_{інф} P_{Ауа}(t). \tag{1.5}$$

Існує дуже поширена модель Zero Trust Ця модель пропонує переглянути стратегію безпеки. Вона передбачає недовіру до всіх, навіть внутрішніх, учасників мережі. Модель базується на аналізі, хто і чому має доступ до мережі, як учасники отримали її та як довго підключені. Крім того, потрібно розуміти, до якої інформації є доступ кожного учасника. Пристрій під час повторного підключення до системи повинен проходити верифікацію. Але ця модель не враховує вплив деяких параметрів розповсюдження інформації.

Розвідка загроз (аналіз загроз) є ключовим елементом інформаційної безпеки, оскільки дозволяє заздалегідь визначити найбільш серйозні загрози для конкретного бізнесу. Це дає змогу оцінити потенційні небезпеки, які можуть бути націлені або вже впливають на організацію, її працівників, клієнтів та партнерів. Такі загрози можуть призвести до втрат доходів, репутації, перебоїв у наданні послуг та інших негативних наслідків. З допомогою аналізу загроз організації можуть визначити пріоритети найбільш ймовірних проблем і направити свої ресурси на вирішення найбільш критичних питань. Модель загроз включає кілька етапів [62]:

- вимоги до моделі (структура моделі захисту);
- збір даних;
- обробка;
- аналіз;
- результати аналізу;
- зворотній зв'язок.

Модель дає можливість швидко та ефективно отримати необхідні дані, проаналізувати їх, попередити клієнтів та надати їм рекомендації щодо способів запобігання можливої атаці.

У [34, 54,] наведена математична модель впливу на криптографічну систему

$$I_j^e = \varphi_i^{-1}(K_i^*, E_i + e). \tag{1.6}$$

де: $E_i + e$ - порушник, який вносить помилку «*e*» в криптограму і передає $E_i + e$ в точку приймання. В результаті відновлюється недостовірна інформація ключем φ_i^{-1}. Порушник також може несанкціоновано зчитувати інформацію з інформаційної системи. Сучасні рішення щодо захисту персональних даних

більше не можуть базуватися лише на одній технології; вони потребують підходу, що поєднує багаторівневі технології та концепцію «нульової довіри» (zero trust), щоб запобігти можливим порушенням безпеки. При комплексному аналізі різних видів порушень захисту персональної інформації в соціальних мережах, з урахуванням якісно–кількісних характеристик інформації, що циркулює в мережі, необхідно враховувати її вразливість за параметрами впливу. Це важливо для ефективної боротьби з невідомими зловмисниками.

1.3. Аналіз існуючих наукових методів захисту персональних даних

Методи захисту персональних даних у інформаційних мережах потребують постійного удосконалення. Особливо це стосується методів захисту від атак за допомогою соціальної інженерії. Це обумовлено тим, що методи атак за допомогою соціальної інженерії використовують помилки користувачів.

Соціальна інженерія відноситься до нетехнічних типів стратегії кібератак, які базуються на взаємодії між людьми та маніпуляціях таким чином, щоб людина порушила стандартні правила захисту інформації [48, 43, 56,].

Для такого типу атак не потрібно бути хакером та знати багато технічної інформації, тому зловмисники активно використовують даний напрямок нападу. Набагато легше отримати бажане завдяки методу соціальної інженерії, ніж зламувати комп’ютерну мережу та програмне забезпечення. Закон України “Про інформацію” окреслює конфіденційну інформацію як інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою [77]. Закон України “Про захист персональних даних” [76] визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Це розповсюджене визначення даного поняття - та воно є найбільш узагальненим. Перелік

відомостей, які належать до персональних даних, змінюється від однієї країни до іншої.

Сучасні підприємства, частіш за все, створюють кіберзахист, орієнтуючись на кібератаки. Такі системи мають високий рівень надійності, але при цьому залишаються вразливими для однієї з багатох загроз.

Загрози соціальної інженерії, засновані на маніпуляціях людською свідомістю. За загальною статистикою, станом на сьогодні соцінженерія так чи інакше застосовується у 97% націлених атак, при цьому технічні вектори іноді взагалі не використовуються або використовуються мінімально. Фахівці захисту інформації станом на сьогодні, на перші місця серед загроз інформаційної безпеки ставлять методи соціальної інженерії, а ряд експертів роблять висновки, що якщо соціальна інженерія поєднается з технологіями машинного навчання та штучного інтелекту, то суспільство отримає загрозу, яку можливо порівняти з глобальним потеплінням та ядерною зброєю. У самих просунутих варіантах соціальна інженерія - це витончена галузева наука «професійних» команд шахраїв та технічних фахівців різних профілів.

Згідно з українським законодавством не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини [55].

Загрози персональним даним можливо описати у вигляді загроз несанкціонованого використання та поширення персональних даних.

За згодою суб’єкта конфідеціальних даних персональна інформація іноді може оброблятися та зберігатися розпорядником, мету та відповідальність у цей час визначає володар даних. Таким чином, володар та розпорядник несуть відповідальність за цілостність довіреної їм інформації. Будь-які дані зараз

зберігаються в інформаційних системах, а отже, мова їде про загрози персональним даним, які зберігаються та обробляються в ІС.

Усі загрози можна умовно поділити на загрози, які можуть бути реалізовані внаслідок атак, та на такі, які не залежать від атак [87, 89].

Загрозами не пов’язаними з цілеспрямованими атаками можуть бути:

- загрози, що не пов'язані з діяльністю людини: форс мажорні обставини, стихійні лиха та природні явища;
- загрози, що мають соціально-політичний характер: страйки, диверсії, війна, локальні конфлікти, що супроводжуються нападом на об'єкт, який має інформаційні ресурси;
- помилкові дії та/або умисні порушення персоналом і користувачами інформаційної системи загальних вимог до відповідних організаційно правових та технічних вимог;

Захист від загроз, які не залежать від нападу та атак, регулюється інструкціями, розробленими та затвердженими уповноваженими особами або службами розпорядника персональних даних, з урахуванням специфічних умов функціонування інформаційної системи, а також чинних нормативних документів.

Захист від загроз повинен забезпечуватися за допомогою захисних заходів та засобів, які використовуються інформаційною системою та призначені переважно для протидії атакам.

Атаки за допомогою соціальної інженерії відбуваються в один або кілька кроків [15].

На рис. 1. 9. схематично зображений життєвий цикл атаки [15].

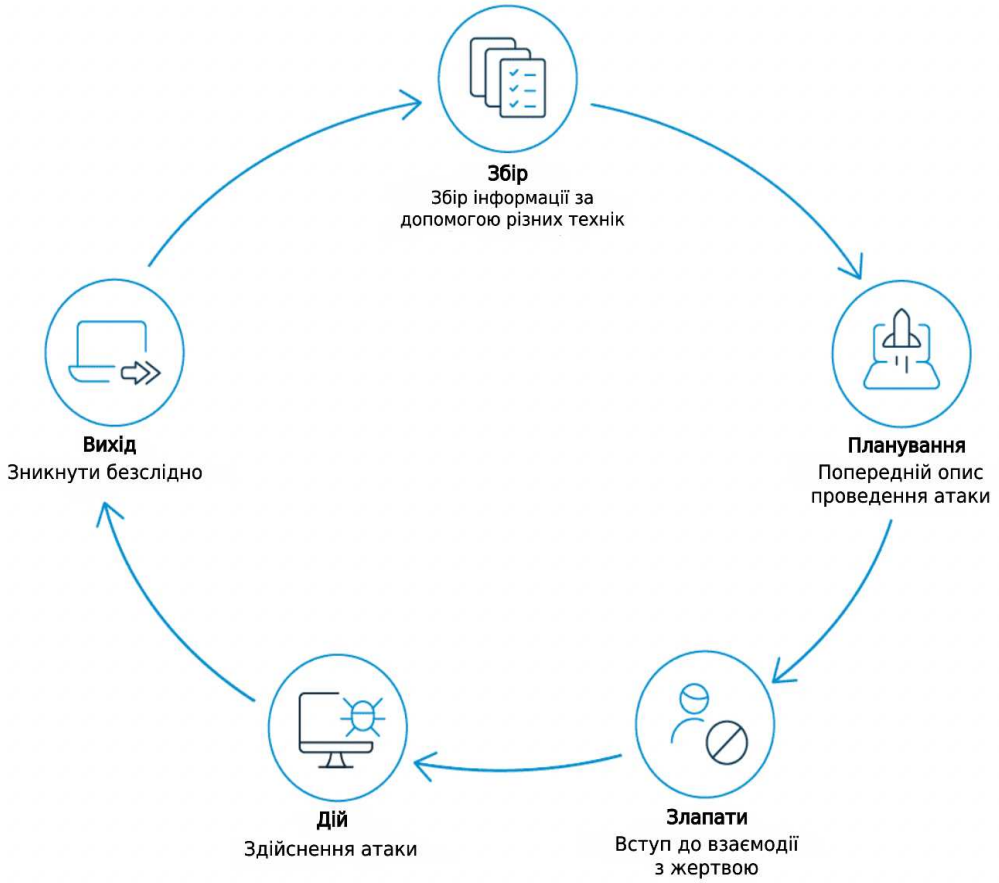

Рис. 1.9. Життєвий цикл атаки [15]

Згідно цій схемі, існують наступні етапи підготовки та здійснення атаки:

1. Збір інформації. Імовірність успіху атаки залежить від цієї фази, тому логічним є те, що зловмисники приділяють цьому етапу найбільшу частину свого часу. Інформація може збиратися різними засобами та методами. Маючи вірну інформацію, зловмисник може призначити вектор нападу, це можливо паролі, ймовірні відповіді окремих осіб та потім уточнення цілі. На цьому етапі нападник дуже добре ознайомлюється з потенційною жертвою.

2. Планування. На цьому етапі нападник вже дуже добре ознайомлений з потенційною жертвою формулює конкретний план нападу під дану особу.

3. Встановлення контакту з потенційною жертвою. На цьому етапі зловмисник встановлює контакт з потенційною жертвою та вибудовує довірливі стосунки з нею. Це дуже критично, оскільки якість встановленого контакту визначає рівень співпраці та рівень, з яким жертва буде допомагати зловмисникові досягти мети. Це може бути особисте спілкування по телефону або розмова з секретарем або співробітниками у приміщені. Іноді цей етап може бути більш масштабним, наприклад таким, як побудова онлайн-знайомства та встановлення стосунків із жертвою за допомогою або фальшивого профілю на сайті знайомств, або у соціальних мережах.

Після цього зловмисник узагальнює та у подальшому використовує як зібрану інформацію, так і встановлений контакт, не викликаючи ніяких підозр. Потім відбувається взаємодія зловмисника та жертви.

4. Виконання атаки. Це фаза коли зловмисник досягає своєї кінцевої мети. Як правило, напад або атака є короткочасною та закінчується ще до того, як жертва починає розуміти, що відбувається.

5. Вихід з атаки. Зловмисник намагається прибрати цифрові відбитки будь-якого свого перебування.

Загалом зловмисник досягає двох цілей. По-перше, жертва не розуміє, що напад відбувся. По-друге, зловмисник приховує повністю свою особу. Це добре спланована та плавна стратегія виходу, це є метою нападника та останнім актом в атаці.

Сфера застосування методів соціальної інженерії достатньо широка, однак можливо визначати основні напрямки [60 – 63]:

- збір відкритої інформації про об’єкт нападу зі соцмереж, якими вона користується, а також іншої інформації. Наприклад імен, під якими вона з’являється у мережі Інтернет, це відбувається через ведення діалогу з жертвою або з її оточенням у службах обміну інформацією;

- отримання персональної інформації про об’єкт нападу або атаки;
- отримання інформації про об’єкт нападу, інформації необхідної для забезпечення несанкціонованого доступу до системи, пароля та інших відомостей про неї шляхом входження в довіру до обраної жертви;
- примушення жертви до дій, необхідних шахраю. Наприклад, проникнення у мережу організації для дестабілізації зі певною метою роботи її основних вузлів;
- загальна дестабілізація роботи організації з метою повного її знищення;
- фішинг та інші способи викрадення паролів.

З часом з’являються нові типи впливу на людей, а отже і типи нападу та атак. На рис.1.10. зображені основні типи атак соціальної інженерії [95–97].

Основне припущення які ми використовуемо у роботі, це те що основним видом атаки на персональні дані будемо враховувати фішинг атаку.

Частіше за все зловмисники використовують даний тип нападу використовуючи електронну пошту. Відтак існують найпопулярніші сценарії. Наприклад, коли зловмисник надсилає фішинговий лист, він намагаєтеся змусити жертву виконати певні дії, щоб отримати реальні дані для подальшої атаки, або встановити шкідливе програмне забезпечення як частину більш широкомасштабної спроби проникнення.

Фішингова атака матиме більше шансів бути успішною, якщо атака розроблена під конкретного користувача. Зловмисник створює ілюзію того, що електронний лист отримано саме з надійного джерела, це підвищує ймовірність того, що користувач прочитає цей лист.

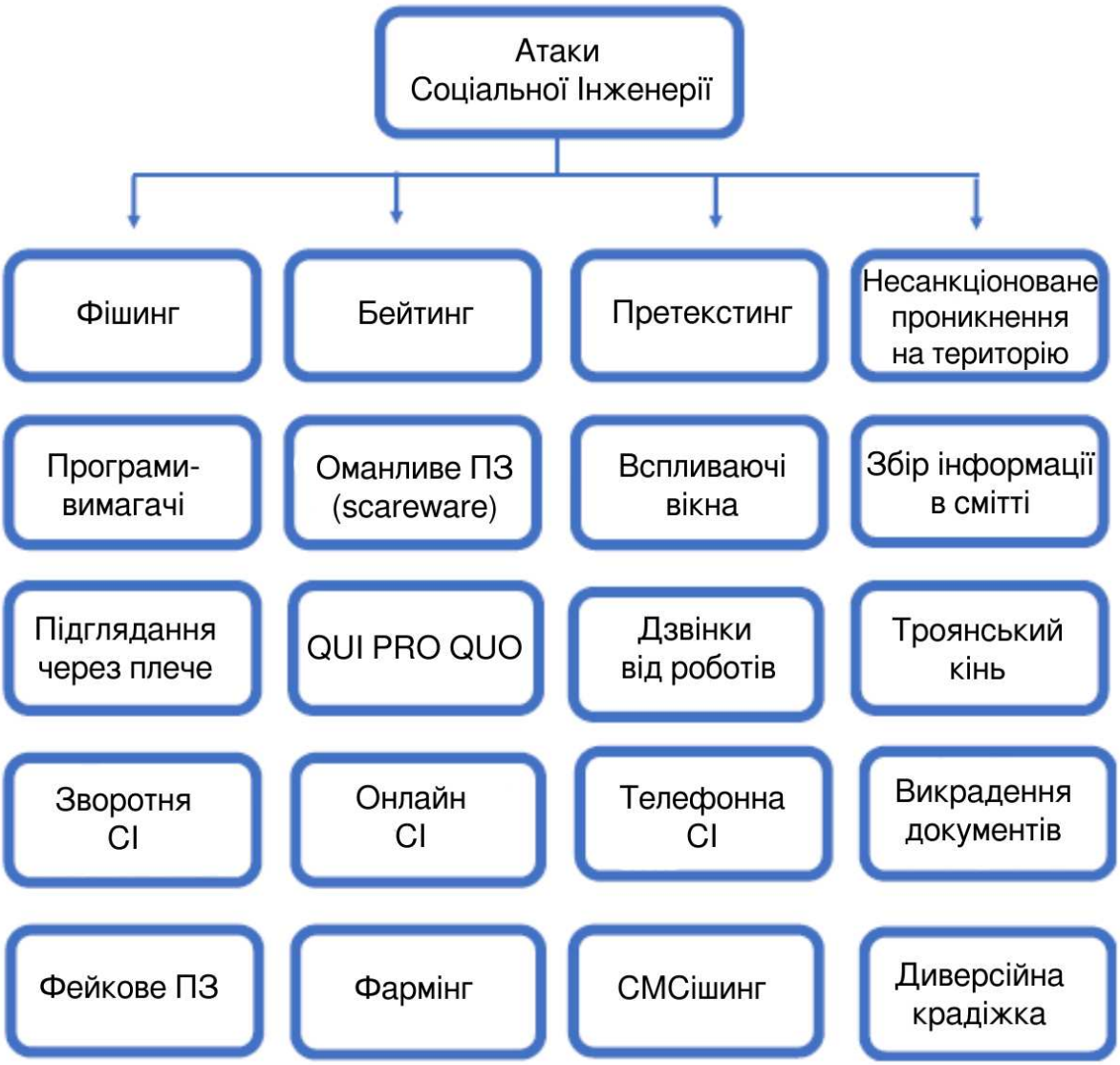

Рис. 1.10. Основні види атак соціальної інженерії [95]

Усі атаки такого типу можуть представлени у вигляді 5 груп (рис 1.11): спрямований фішинг, полювання на корпоративних китів, телефонний фішинг, інтерактивний фішинг голосової відповіді та компромісний фішинг для ділової електронної пошти [43].

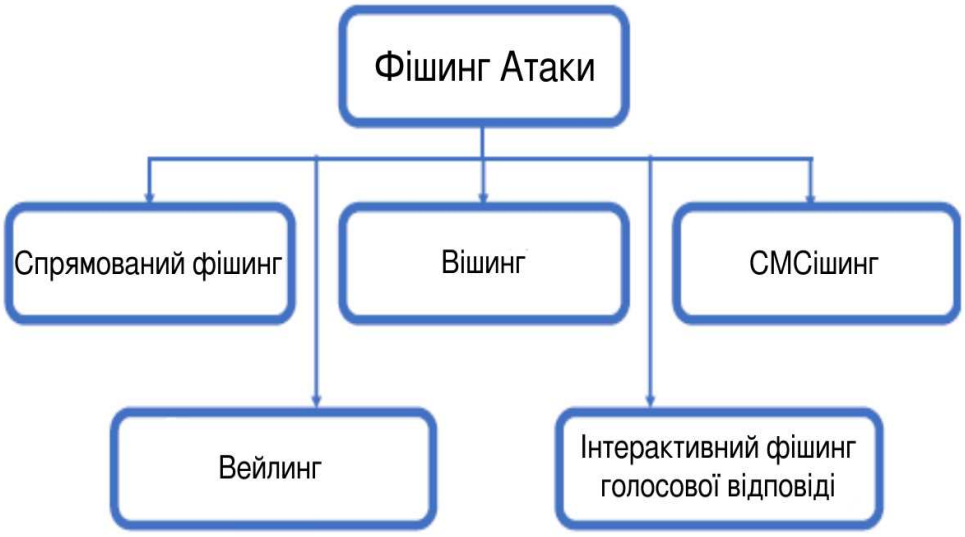

Рис. 1.11. Основні різновиди фішинг атак [43]

Спрямований фішинг (Spear phishing) – це цілеспрямована фішингова атака. Найчастіше жертвами спрямованого фішингу є високі посадові особи, які мають доступ до більшої конфіденційної інформації, аніж пересічний робітник [43].

Вішинг (англ. Vishing від поєднання Voice та Fishing) або телефонний голосовий фішинг – це такий тип атаки, коли кіберзлочинець дзвонить за номером телефону й за допомогою створення відчуття невідкладності ситуації змушує людину вчиняти дії проти своїх інтересів [43].

СМС фішинг (Smishing) – це вид фішингу, який використовує текстові повідомлення на мобільних телефонах [43] .

Вейлінг (*Whaling* полювання на корпоративних китів) – це фішингова атака, що спрямована на осіб, які мають повний доступ до інформації у межах організації, наприклад, її вище керівництво [43].

Інтерактивний фішинг голосової відповіді виконується за допомогою інтерактивної системи голосового реагування [43].

Виявлення фішингових атак.

Можливо виокремити два основних підходи до виявлення фішингу [16]:

1) *Навчання користувачів*: користувачів можливо навчити краще розуміти природу фішингових атак, це у результаті допоможе коректно розрізняти фішингові та справжні повідомлення [17].

2) *За допомогою програмних засобів*: цей підхід має на меті заповнити прогалину, яка виникає через помилку користувача або неуміння розрізняти програмним або іншим способом фішингові та легітимні повідомлення.

Розпізнавання фішингової атаки – це завжди початкова точка протидії фішинговим атакам. На рис. 1.12 показана схема підходів до розпізнавання фішингових атак [37].

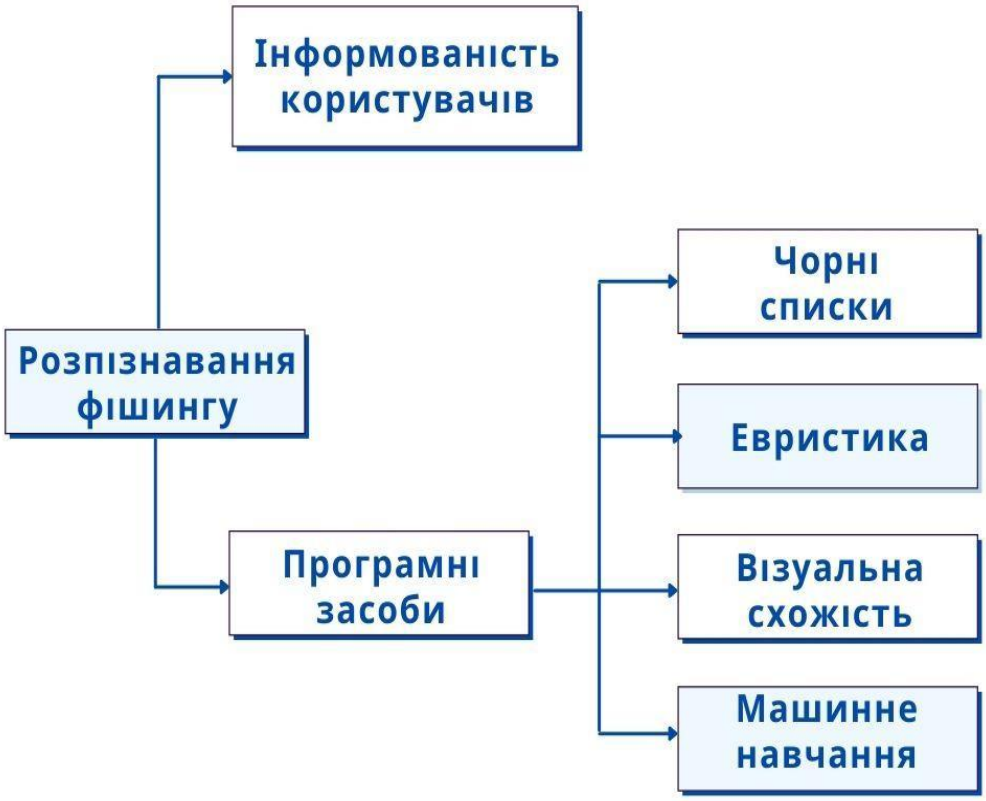

Рис. 1.12. Схема алгоритму розпізнавання фішингових атак [37]

Ефективність виявлення такого типу атак може бути покращена за рахунок навчання класифікатора.

Програмний підхід до виявлення**.**

Чорні списки. Це постійно оновлюванні списки, що містять раніше виявлені фішингові URL-адреси. Головним недоліком даної методології є затримка в оновленні списків.

Білі списки. Це є чимось протилежним до чорних.

Евристичні методи виділяють певні характеристики веб-сторінки для того, щоб визначити легітимність веб-сайту, а не залежати від будь-яких попередньо скомпільованих списків. Це перевага евристичних методів [18, 19]

Методи візуальної схожості. Це методи розрізнення фішингових сайтів та легітимних сайтів за зовнішнім виглядом сайтів. Зазвичай фішингові сайти є майже точними копіями справжніх, щоб у користувача не виникали сумніви щодо легітимності ресурс [22–23].

Машинне навчання [12] забезпечує спрощені та ефективні методи аналізу даних, останнім часом демонструючи багатообіцяючі результати у проблемах класифікації в реальному часі.

На рис. 1.12. наведені два підходи до виявлення фішингових атак: навчання користувачів та програмний підхід. Для цієї роботи було обрано більш детально розглядати підхід навчання користувачів.

Незалежно від наявних навичок чи здібностей, усі люди в організації мають пройти навчання з антифішингу. Для боротьби з фішингом існує багато методів донавчання користувачів. На рисунку 1.13 зображені деякі з основних методів навчання користувачів [29].

Лекції. Це один з найстаріших методів і він досі лишається одним із найпоширеніших, незважаючи на свої недоліки.

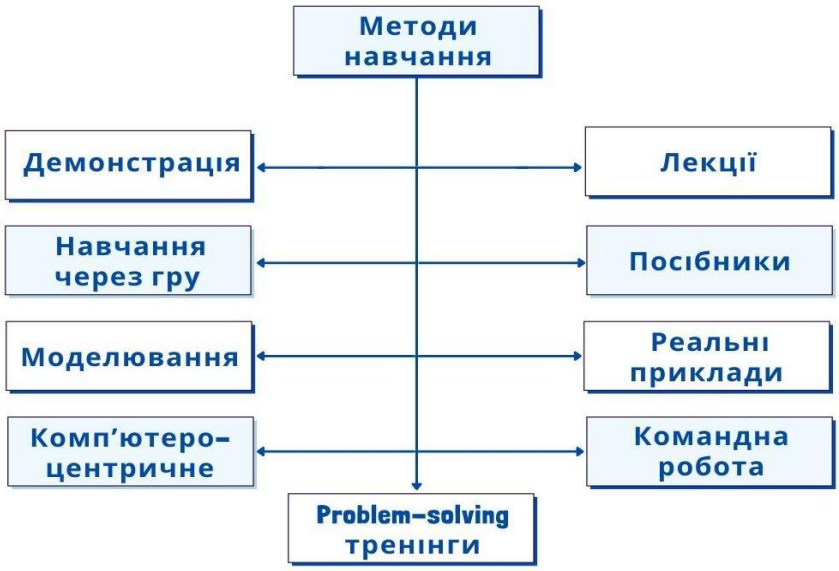

Рис. 1.13. Методи навчання користувачів [29]

Попри те, що цей метод досі користується популярністю для навчання користувачів, він має недоліки, зокрема наступні:

- для лекцій потрібні досвідчені лектори;
- потрібен інтерактивний підхід та плотна взаємодія лектора з аудиторією, інакше користувачі, як правило, швидко втрачають концентрацію і інтерес;
- від співробітників очікується, що вони навчатимуться у однаковому темпі та з однаковим розумінням, а це зовсім не так;
- нажаль, виявленню фішингових атак у реальному часі не можливо навчити лише на лекціях, для успіху потрібно залучати інші ресурси.

Навчальні посібники і мануали. У навчанні користувачів навчальний посібник та методичний матеріал є необхідним для поглиблення знань з теми. За допомогою посібників та методичного матеріалу користувачи можуть дізнатися, як можна практикувати захист від атаки вдома. Існує багато різновидів навчальних посібників та методичного матеріалу, наприклад:

- робочі зошити ;

- інструкції для самостійної роботи, які користувачі можуть виконувати у вільний час;
- довідкові посібники;
- роздатковий матеріал містить загальну інформацію, яка доповнює матеріал, який викладає лектор.

Але недоліком посібників є те, що користувачі можуть не зрозуміти деякі важливі поняття та просто читати матеріал.

Навчання на реальних прикладах. Це ретельне дослідження конкретного випадку або ситуації в реальному часі. Такий метод дає можливість зробити процес навчання набагато реалістичним. Метою вивчення конкретного випадку-нападу є краще зрозуміти проблему. Таким чином, лектори надають детальні описи ситуації, дають пояснення.

Групове навчання. Користувачі можуть поглибити свої знання під час командної роботи. Спільне навчання може допомогти слухачам покращити свою продуктивність. Недоліком цього методу навчання є те, що всі залежать один від одного.

Тренінг із вирішення проблем – це такий тип навчання, під час якого користувач вчиться знаходити найкраще ефективне рішення проблеми.

Демонстрація – включає покрокове навчання.

Навчання через гру. Існує кілька способів практикувати фішинг, але один з найпоширеніших – це гра.

Навчання на основі моделювання є високоефективним і економічно вигідним методом навчання слухачів у реальному часі в контрольованому середовищі.

Комп'ютерне навчання – це такий метод навчання, який покладається на використання цифрових технологій.

Проведений аналіз дозволяє зробити висновок, що потрібно удосконалення методу захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. Удосконалення здійснюється шляхом поєднання двох методів. Методів які спрямовані на підвищення ефективності навчання користувачів. Удосконалений метод на відміну від існуючих складається у поєднанні двох методів: методу навчання на реальних прикладах, та навчанні при розв'язуванні задач.

1.4. Постановка наукового завдання

Аналіз роботи програмних засобів та систем захисту інформації показав, що розробка системи захисту персональних даних у соціальних мережах з урахуванням їх особливостей є складною і багатогранною проблемою. Тому підвищення надійності систем захисту інформації, забезпечення виявлення впливів, розпізнавання загроз та створення методологічних основ захисту інформації в інформаційних мережах є важливими та невідкладними завданнями.

Нині удосконалення систем виявлення зовнішніх впливів базується на наступних напрямках [70 – 73]:

– застосування принципів виявлення сигналів зовнішніх впливів для визначення їх характерних параметрів;

– використання вдосконалених методів остаточного розпізнавання зовнішніх впливів та ідентифікації загроз.

Це не є достатньо для забезпечення комплексного захисту особистих та персональних даних користувачів.

Проведене дослідження процесу функціонування систем захисту інформації дозволяє зробити наступні висновки:

1. Остаточно не вирішена проблема з виявленням зовнішніх впливів на мережі з метою порушення цілісності, конфіденційності та доступності інформації користувачів.

2. Розробка методів та методик розпізнавання зовнішніх атак на інформаційні мережі, які зберігають персональні дані, потребує удосконалення.

3. Проблема виявлення ознак зовнішніх впливів та загроз досі не вирішена остаточно, що може призвести до несанкціонованого доступу до персональних або приватних даних користувачів.

Виходячи з проведеного дослідження, виникає наукове завдання щодо розробки науково-методичного апарату захисту особистих даних з урахуванням специфіки соціальних мереж.

Більшість наукових досліджень мають описовий та дослідницький характер, орієнтуючись на вирішення окремих завдань захисту інформації та баз даних, і тому не можуть служити методологічною основою для розробки системи забезпечення безпеки персональних даних. Отже, на основі проведеного аналізу та результатів вивчення наукових публікацій, дисертацій, патентів, монографій і практичних робіт, встановлено, що на сучасному етапі розвитку прогресивних інформаційних технологій існує об'єктивне протиріччя між загальним характером існуючих математичних моделей захисту персональних даних та необхідністю підвищення захищеності персональних даних у соціальних мережах

Для вирішення виявлених протиріч необхідно вирішити **актуальне наукове завдання** *щодо розробки науково-методичного апарату захисту персональних даних з урахуванням специфіки соціальних мереж*.

Реалізація запропонованого науково-методичного апарату дозволить визначити ефективну структуру науково-методичного забезпечення захисту персональних даних у соціальних мережах.

Мета дисертаційної роботи полягає у підвищенні захищеності персональних даних у соціальних мережах за рахунок врахування специфіки соціальних мереж: запізнення реагування на атаку; показника комплексної довіри, урахування параметра розширення соціальних мереж, урахування

сильних і слабких зв’язків та оцінки економічних витрат на захист персональної інформації у мережах.

Для досягнення поставленої мети в дисертації необхідно вирішити такі наукові завдання:

1) здійснити порівняльний аналіз існуючих моделей та методів щодо оцінювання ефективності захисту персональних даних;

2) розробити математичну модель захисту персональної інформації в соціальних мережах;

3) удосконалити метод оцінки поведінки системи захисту персональної інформації;

4) здійснити подальший розвиток методу деперсоналізації даних для захисту персональної інформації в мережах;

5) провести математичне моделювання з метою підтвердження достовірності методу оцінки стійкості системи захисту персональних даних.

Висновки до розділу 1

У розділі 1 зроблено аналіз існуючих моделей та методів щодо оцінювання ефективності захисту персональної інформації в інформаційному просторі, що дає можливість зробити такі висновки:

1. На основі аналізу практики та теорії побудови та використання інформаційних мереж встановлено об’єктивне протиріччя між необхідністю підвищення рівня інформаційної безпеки та недосконалістю системи захисту інформації та і можливостями існуючих методів, які використовують інформаційні мережі.

2. Аналіз існуючих методів захисту інформації в інформаційних мережах показав їх обмеженість. Не завжди враховується ступінь довіри між користувачами. При виявленні зовнішніх впливів (атак) не враховується швидкість змін параметрів як самих впливів так і параметрів системи захисту.

Тому проблема захисту персональної інформації не вирішувалася комплексно. У сучасних наукових працях основна увага зосереджена на гіпотезах захисту інформації, а більшість досліджень має описовий та дослідницький характер. Проблема розпізнавання зовнішнього впливу та його віднесення до загрози практично не розглядається, а методи вдосконалення процесу розпізнавання впливів не реалізуються. Більшість наукових робіт орієнтовані на вирішення окремих завдань захисту інформації та баз даних і не можуть бути застосовані як кінцеві методи забезпечення захисту даних у соціальних мережах. Недосконаліть і обмеження існуючих наукових методів у процесі захисту інформації в соціальних мережах не дозволяють забезпечити достатній рівень захисту даних особистості чи груп користувачів у цих мережах. Це додатково підтверджує актуальність сформульованого у дисертації наукового завдання щодо розробки моделі та методів захисту персональних даних з урахуванням специфіки соціальних мереж. Вирішення цієї проблеми має суттєве значення для проектування та модернізації існуючих систем захисту інформації. Відсутність аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

3. У рамках сформульованого наукового завдання поставлені наукові задачи, щодо розробки моделей та методів захисту інформації у соціальних мережах. З метою підтвердження отриманих результатів поставлено завдання провести математичне моделювання, розробити рекомендації та виконати оцінку теоретичних результатів.

РОЗДІЛ 2
РОЗРОБКА МАТЕМАТИЧНОІ МОДЕЛІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ З УРАХУВАННЯМ СПЕЦИФІКИ СОЦІАЛЬНИХ МЕРЕЖ

Крадіжка особистих даних – це злочин, у якому зловмисник отримує дані іншої особи та використовує особистість жертви для шахрайства. Тому проблема розробки та дослідження математичних моделей захисту особистих даних є актуальною.

2.1. Визначення параметрів оцінки захисту соціальних мереж

Американський соціолог Марк Грановеттер здійснив один із найвідоміших досліджень у сфері аналізу мереж. Він продемонстрував, що слабкі зв'язки є значно ефективнішими, ніж сильні, у вирішенні багатьох соціальних завдань, зокрема під час пошуку роботи. Це явище він назвав "силою слабких зв'язків".

Ідея алгоритму базується на спостереженнях за поведінкою мурах у процесі пошуку найкоротшого шляху від гнізда до джерела їжі. Модель цього процесу виглядає наступним чином: мураха випадково рухається від гнізда, і, знайшовши їжу, залишає на зворотному шляху слід. Цей слід приваблює інших мурах поблизу, які, найімовірніше, теж підуть цим маршрутом. Повернувшись у гніздо, вони підсилюють шлях за маршрутом. Якщо існує кілька маршрутів, то на коротшому з них встигне пройти більше мурах за той самий час. Таким чином, короткий шлях стає більш привабливим, тоді як довгі маршрути поступово зникають через випаровування феромонів.

Процес починається з розміщення мурах у вершинах графа, після чого вони починають рух. Напрямок їхнього руху визначається за ймовірнісним підходом, що ґрунтується на виразі такого типу.

$$P_i = \frac{l_i^q f_i^q}{\sum_{k=0}^{n} l_k^q f_k^q}, \qquad (2.1)$$

де P_i – ймовірність переходу шляхом i;

l_i – величина, обернена до ваги (довжині) i-го переходу;

f_i – кількість феромонів на i-му переході;

q – величина, що визначає «жадібність» алгоритму;

p – величина, що визначає «стадність» алгоритму і $q + p = 1$.

До основних методів аналізу соціальних мереж належать [71, 82–84]: методи теорії графів, які охоплюють дослідження орієнтованих графів і відповідних матриць, що використовуються для аналізу структурних взаємозв'язків між учасниками мережі; методи оцінки локальних характеристик учасників, зокрема таких, як центральність, впливовість, позиція та належність до певних підгруп; а також методи, які включають моделі марківських процесів.

Графічні моделі. Соціальну мережу можна математично представити у формі графа

$$G = (V, E),$$

де V - множина вершин графа;

E – множина ребер графа;

$|V| = N$ – кількість вершин у графі.

У графі соціальної мережі вершинами є учасники, а ребра означають наявність відносин між ними. Відносини можуть бути як спрямованими, так і не спрямованими.

Можливо виділити три типи моделей графів [71]:

1. Стохастичні блокові моделі задаються матрицею A розміром $N \times N$, де N – число груп (блоків) учасників.

Елемент $a_{ij} \subset [0,1]$ показує щільність зв'язків між учасниками мережі, які належать до групи v_i, та учасниками, що належать до групи v_j.

2.Імовірнісні графові моделі задаються матрицею A розміру $N \times N$, де N – число учасників мережі. Елемент $a_{ij} \subset [0,1]$ показує ймовірність взаємодії учасника v_i та учасника v_j протягом певного періоду часу.

3. Звичайні графові моделі також задаються матрицею A зв'язності розміру $N \times N$.

Аналіз центральності та інших локальних властивостей. Щоб визначити відносну важливість (вагу) вершин графа, застосовують поняття центральності – близькість до центру графа. Слід зазначити, що йдеться не про геометричну центральність при візуалізації графа відносин.

Центральність за ступенем (Degree centrality) визначається як кількість зв'язків, інцидентних вершині: $C_D = \deg(v)$

Виділяють вхідні та вихідні зв'язки. Вхідні зв'язки характеризують популярність людини, що характеризують його оточення у мережі. Отриману величину можна нормувати, розділивши на загальну кількість учасників у мережі.

Проте учасник мережі, що має велику кількість друзів, може бути пов'язаний з рештою графа невеликою кількістю ребер. Тому вводиться таке поняття, як Центральність поблизу (Closeness centrality). Де центральність поблизу є показником, наскільки швидко поширюється інформація в мережі від одного учасника до інших. Як міра відстані між двома учасниками використовується найкоротший шлях по графу (геодезична відстань). Так, безпосередні друзі учасника перебувають з відривом 1, друзі друзів – з відривом 2, друзі друзів друзів – з відривом 3 тощо. Далі береться сума всіх відстаней і

нормується шлях по графу. Отримана величина називається віддаленістю вершини одна від одної.

Близькість визначається як величина, зворотна віддаленості

$$C_c(v) = \frac{N-1}{\sum\limits_{t \in \frac{V}{v}} d_G(v,t)}, \tag{2.2}$$

де $d_G(v,t)$ - найкоротший шлях від вершини *v* до вершини *t*.

Іншими словами, центральність по близькості дозволяє зрозуміти, наскільки близький учасник, що розглядається, до всіх інших учасників мережі. Таким чином, важливо не тільки наявність безпосередніх друзів, але щоб і у самих цих друзів теж були друзі.

Центральність за посередництвом (Betweenness centrality). Ще однією рисою учасника є його значущість у процесі поширення інформації. Центральність розраховується як число найкоротших шляхів між усіма парами учасників, що проходять через аналізованого учасника

$$C_B(v) = \frac{Q_{st}(v)}{\sum\limits_{s \neq v \neq t \in V} Q_{st}}, \tag{2.3}$$

де *Qst* – загальна кількість найкоротших шляхів з вершини *s* до вершини *t*;

Qst (v) – кількість найкоротших шляхів з вершини *s* до вершини *t*, що проходять через вершину *v*.

Для нормалізації потрібно розділити кількість пар вершин, крім самої вершини *v*, тобто для орієнтованого графа потрібно розділити на (*N*-1)×(*N*-2), для неорієнтованого – на величину, рівну (*N*-1)×(*N*-2)/2. Недоліком центральності за посередництвом є її обчислювальна складність.

Центральність за власним вектором (Eigenvector centrality). Нехай центральність аналізованого учасника – x_v, а центральність його безпосередніх друзів (сусідніх вершин) x_j , x_k , x_l та далі. Центральність за власним вектором визначається як сума центральностей сусідніх вершин, поділених на константу λ, тобто $x_v = (x_j + x_k + x_l)/\lambda$. Виписавши аналогічні рівняння всім друзям, отримаємо вектор невідомих $X = (x_1 ,...,x_v ,...,x_n)$. Правила складання визначаються матрицею суміжності $A=(a_{vt})$, тобто a_{vt}=1, якщо вершина v з'єднана з вершиною t, a_{vt} = 0 – інакше. Далі потрібно вирішити рівняння $AX = \lambda X$, тобто знайти власні значення та власні вектори матриці A. Отримане завдання можна переписати інакше

$$C_E(v) = x_v = \frac{1}{\lambda}\sum_{t\in M} x_t = \frac{1}{\lambda}\sum_{t\in G} a_{vt}x_t, \tag{2.4}$$

де $M(v)$– безліч вершин, сусідніх з вершиною v;

λ – константа.

Власний вектор, що відповідає найбільшому власному значенню, утворений центральностями відповідних учасників мережі.

Таким чином, чим більше в учасника друзів і чим вони ближчі до нього, тим більша його центральність. Правильне і зворотне: чим більша центральність учасника, тим більша центральність його друзів. Недоліком центральності за власним вектором є обчислювальна складність.

Узагальненням центральності за рівнем є центральність Каца (Katz centrality).

$$C_{Katz}(i) = \sum_{k=1}^{\infty}\sum_{j=1}^{n}\alpha^k(\alpha^k)_{ji}, \tag{2.5}$$

де $a \subset [0,1]$ – частка участі віддалених вершин, що визначається як коефіцієнт загасання.

Центральність Каца можна розглядати як модифіковану форму центральності на основі власного вектора

$$C_{Katz}(i) = x_i = \sum_{j=1}^{n} \alpha_{ji}^{k} (x_{ij} + 1). \quad (2.6)$$

Центральність можливо обчислити за допомогою алгоритму ранжування посилань (PageRank), який використовується в пошуковій системі Google. В основу покладено принцип «важливості» веб-сторінки: чим більше посилань на сторінку, тим вона «важливіша»

$$C_{PageRank}(i) = x_i = \alpha \sum_{j=1}^{n} \alpha_{ij} \frac{x_j}{L(j)} + \frac{1-\alpha}{N}, \quad (2.7)$$

де $L(j) = \sum_{j} \alpha_{ij}$ кількість вершин, сусідніх з вершиною j (або кількість вихідних j зв'язків у орієнтованому графі).

Даний алгоритм відрізняється від обчислення центральності за власним вектором та центральністю Каца наявністю коефіцієнта перерахунку *L(j)*. Слід зауважити також, що у алгоритмі посилального ранжування використовується зворотна індексація матриці суміжності a_{ji} проти обчисленням центральності за власним вектором.

Крім перерахованих методів визначення центральності існує велика кількість введених некласичним чином способів обчислення цієї характеристики мережі.

Далі алгоритм базується на припущенні, що якісні сайти рідко посилаються на низькоякісні, тоді як останні часто посилаються на надійні ресурси. TrustRank — це показник, який оцінює рівень довіри до сайту, зокрема його ймовірну

відсутність спаму. Чим більше вихідних посилань має сайт, тим менший рівень довіри передається через кожне з них. Рівень довіри (TrustRank) зменшується зі збільшенням відстані між сайтом і початковим набором надійних ресурсів.

Сила структурної позиції учасника є основним показником, який є визначальним в розбіжності учасників мережі. Для виміру даної характеристики вводиться [8] індекс GPI (Genuine Progress Indicator) сили учасника v_i

$$GPI_i = \sum_{k=1}^{g-1} (-1)^{k-1} P[i]_k, \tag{2.8}$$

де $P[i]_k$ число шляхів довжини k, що не перетинаються, проходять через вершину v_i . Сила учасника v_i у порівнянні з силою учасника v_j обчислюється як

$$GPI_{ij} = GPI_i - GPI_j.$$

Для аналізу стійкості групової структури в часі використовується наступний підхід. Спочатку створюється тривимірна матриця, де рядки представляють оцінки взаємодій між учасником і всіма іншими, надані іншими учасниками; стовпці відображають самооцінки взаємодій учасника; а третя вісь відповідає часовим періодам.

Далі застосовуються методи зменшення розмірності даних, такі як метод головних компонентів, щоб виконати проєкцію вершин мережі в евклідовий простір меншої розмірності. Це дозволяє описати взаємозв’язки між рядками та стовпцями матриці. Результати використовуються для візуалізації змін статусу учасників мережі в контексті змін статусів підгруп [56].

Отриману проєкцію можна кластеризувати за допомогою стандартних методів, як-от статистичні алгоритми (наприклад, метод k-середніх) [79] або ієрархічні підходи. Ієрархічні методи мають перевагу в тому, що результати

кластеризації можна представити у вигляді дендрограми, яка відображає не лише розбиття графа на групи, але й ієрархію груп та підгруп. Основною складністю таких методів є вибір відповідної метрики відстані (наприклад, найкоротшого шляху між вершинами) або подібності (similarity).

Найчастіше застосовуються заходи подібності, використовують косинусний коефіцієнт (cosine similarity, також відомий як коефіцієнт $O_{\text{хаі}}$) і коефіцієнт Жак-кара (Jaccard coefficient). Кластеризацію можна проводити не тільки знизу вгору, а також зверху вниз, тобто спочатку вся мережа розглядається як одна група, а на кожній ітерації відбувається послідовне відділення по одному зв'язку.

Структурна еквівалентність учасників мережі. Цей підхід є протилежністю дослідженню пов'язаних груп. Учасники вважаються еквівалентними, якщо вони займають однакові позиції в соціальній структурі мережі, тобто мають однакову структуру та тип взаємодій з іншими. При цьому еквівалентність учасників не передбачає обов’язкової взаємодії між ними. Як міра еквівалентності може бути щільність зв'язків зі структурними підгрупами учасників мережі [110, 117]. Поряд із структурною еквівалентністю використовується регулярна еквівалентність учасників. У цьому випадку учасники еквівалентні, коли вони однаково взаємодіють із учасниками одного типу.

Для визначення структурної еквівалентності двох учасників необхідно порівняти структуру їх взаємодій з іншими учасниками, тобто потрібно порівняти відповідні стовпці у матриці зв'язків графа. Це може бути здійснено за допомогою обчислення відстані між цими векторами (наприклад, за метрикою Евкліда або Чебишева) або коефіцієнтів зв'язку (наприклад, кореляції Пірсона). Для спрямованих графів необхідно враховувати ребра, що входять і виходять, з цією метою одночасно розглядаються дві відповідні матриці.

На наступному етапі у матрицях для кожного типу зв'язків переставляються стовпці таким чином, щоб згрупувати ті з них, які відповідають структурно еквівалентним учасникам. В результаті матриця розбивається на структурні блоки, у кожному з яких обчислюється густина. Далі будується нова матриця зв'язків між знайденими структурними блоками, наприклад, за таким правилом: якщо щільність зв'язків між двома блоками вище, ніж середня щільність зв'язків у початковій матриці, то відповідний елемент нової матриці дорівнює 1, в протилежному випадку він дорівнює 0. Такі матриці називаються блоковими моделями і є засобом побудови рольових алгебраїчних виразів [113, 116].

Рольові алгебри. Цей підхід до аналізу соціальних мереж зосереджений на дослідженні логіки взаємодій між учасниками мережі за допомогою блокових моделей. Визначимо матриці симпатії та антипатії наступним чином

$$LIKE = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad DISLIKE = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.9}$$

Тепер можемо аналізувати комбінації взаємодій учасників мережі, перемножуючи відповідні матриці.

Аналіз діад і тріад. Діади — це комбінація з двох учасників мережі (вершин) і всіх взаємодій (ребер) між ними. Аналіз діад дозволяє оцінити ймовірність існування ребра між учасниками, виявити залежність від їхніх властивостей, а також визначити умови і напрями передачі інформації.

Для тріад, які складаються з трьох взаємодіючих учасників, додатково аналізується транзитивність взаємодій, що дає змогу вивчити складніші структурні взаємозв’язки в мережі.

Важливим показником є сила зв'язків між учасниками, що характеризують взаємодію та відповідну йому ребро графу. Слабкі зв'язки є важливими

джерелами інформації [74 –77], оскільки вони допомагають отримати додаткові відомості про учасника або спільноту, в якій він знаходиться.

Стохастичні моделі. Основна концепція ймовірнісних моделей орієнтованих графів полягає в тому, що будь-яку соціальну мережу можна інтерпретувати як реалізацію випадкового двовимірного бінарного масиву. Застосування статистичних моделей в аналізі соціальних мереж наведено в [102]. Також пропонується використовувати методи машинного навчання та аналізу даних для розрахунку відносної автокореляції, щільності зв’язків і низки інших характеристик мережі. Докладніше про стохастичні моделі можна переглянути в [107].

Аналіз-граф розвитку мережі. У роботах [77-79] Розглянуто різноманітні підходи до аналізу еволюції мережі, які базуються на парадигмі вилучення асоціативних правил (association-rule mining) та дослідженні частотних моделей (frequent-pattern mining). Спочатку обчислюється набір частотних моделей графа, який описує характерні еволюційні механізми, та знаходять правила еволюції графа, які задовольняють заданому обмеженню мінімальності довіри.

Проблема отримання веб-графів, що тимчасово розвиваються, розглянута в [111]. Прогнозування формування зв'язків. Моделі еволюції графа зазвичай створюються з метою оцінки загальностатистичних властивостей існуючих графів. Можна також здійснити обчислення ймовірності з'єднання двох конкретних вершин у мережі через певний проміжок часу. Ця задача, що базується на аналізі еволюції соціальної мережі в динаміці, відома як проблема прогнозування зв'язків.

Нехай дана коротка характеристика соціальної мережі в момент часу t і заданий майбутній час t_0. Завдання полягає в тому, щоб передбачити нові зв'язки, які, швидше за все, з'являться в мережі за проміжок часу $[t_0, t_1]$. Для її вирішення в [95] застосовується автоматичне моделювання процесу розвитку соціальної

мережі із залученням деяких характеристик мережі, таких як кількість спільних сусідів, геодезична відстань (найкоротший шлях), впливовість вершини, момент першого влучення у соціальну мережу.

Існують моделі прогнозування виникнення зв'язків, засновані на машинному навчанні, що використовують особисту інформацію про користувачів. Іноді застосовують ієрархічні, імовірнісні (марківські) та реляційні моделі для виявлення зв'язків між користувачами.

В інших моделях [65 – 67] за основу пропонується обирати властивості користувачів.

Методи з урахуванням онтологій. Дослідження [68, 69] показали, що оцінити параметри соціальних мереж (діаметр, кількість учасників, середню довжину шляху та ін) можна за допомогою онтологій. Таким чином жодна з моделей не вирішила питання комплексного підходу до виявлення загроз особистим даним у соціальних мережах

2.2. Розробка моделі захисту персональних даних з урахуванням параметру запізнення реагування на атаку

Одним із найбільших ринків для крадіжки особистих даних є ринок інформаційних мереж, зокрема соціальні мережі, де зберігається велика кількість персональних та приватних даних користувачів, які стають об'єктом для зловмисників.

Соціальна мережа – соціальна структура, утворена індивідами або організаціями в якій підтримуються соціальні відносини [72]. Соціальні мережі та мережи інтернет є одним із основних способів спілкування. Соціальні мережі становлять дедалі більшу частку спільних мереж. Сама мережа формує нові властивості, стаючи самостійним чинником. В останні роки бачення проблеми кібербезпеки почало суттєво змінюватися, оскільки людина все частіше перестає

бути суб’єктом кіберзлочинності, перетворюючись на об’єкт сам по собі, а не лише своїх фінансово-економічних інтересів і можливостей.

Ця проблема стає особливо актуальною в умовах посилення цифрового гуманістичного напряму освіти та зростання впливу соціальних мереж на життя людини. Захист персональних даних у сучасному інформаційному середовищі є одним із ключових аспектів забезпечення безпечного використання можливостей сучасних технологій.

Послуги інтернет ресурсів та соціальних мереж кардинально еволюціонують [106]

Основна інформація, що зберігається в Інтернет соціальних мережах це [107-108]:

- особисті дані, що описують особу користувача;
- особисті інтереси користувача;
- інформація про бібліографічні дані користувача;
- спілкування через сервіс посилки повідомлень (СПП).

Для збереження конфіденційності зв’язку необхідно застосовувати методи, спрямовані на захист будь-якого виду інформації, що стосується:

- анонімності, користувачі повинні отримувати доступ до ресурсів чи послуг, не розкриваючи власну особу;
- незабезпеченість, щоб жодна третя сторона не мала збирати інформацію про сторони, що спілкуються, та зміст їх спілкування;
- незв'язність, що вимагає отримання двох повідомлень, жодна третя сторона не має змоги визначати, чи обидва повідомлення було надіслано тим самим відправником.

Щоб передбачити охоплення та тривалість нападу на персональні дані, треба звернутись до моделювання передачі вірусу – шкідливого коду у мережі. Моделі можуть відрізнятися за рівнем деталізації. Деякі з них описують лише

процес зараження та нейтралізації атаки на базу персональних даних. Інші враховують додаткові аспекти, наприклад, наявність бази шкідливих кодів, що накопичується з часом. Таким чином, рівень деталізації моделі визначається характеристиками атаки на базу персональних даних, поширення якої система захисту має зупинити.

Розглянемо модель SIR. Назва моделі — це абревіатура назв класів: *S* - уразливі (susceptible), *I* - ті, що заразилися і розповсюджують вірус (infectious), і *R* - ті, хто відбив атаку і отримав імунітет від такого роду нападу (recovered). Через поділ на класи модель SIR називається компартментальною (від англ. Compartment - відсік)

Модель SIR добре відображає реальність лише у випадку, якщо не потрібно моделювати додаткові процеси, наприклад, згасання системи захисту з часом, повторна успішна атака. Тому проста модель SIR добре застосовується до систем, які мають постійний захист від атак такого роду, тобто атаки такого роду вже не можуть досягти результату.

Для захисту персональних даних, треба уникнути шкідливого проникнення у систему зберігання даних. Тому потрібно розширити класи, які будемо використовувати при побудові моделі.

Розглянемо компартментальні моделі із додатковими класами, які призначені для моделювання інших типів атак на систему зберігання персональних даних. Найчастіше використовуються такі класи:

E — вірус, що заразив пристрій або файл але своєчасно заражений об’єкт перебуває в інкубаційному періоді, не поширюючи вірус (exposed). Модель SEIR, відповідно, допомагає моделювати розповсюдження вірусних атак, що виявляються не відразу.

C - об’єкт вилікувано, але продовжують поширювати вірус (carrier). Модель carrier state використовується для моделювання таких заражень, які

можуть переходити в хронічну стадію, так що заражений об’єкт продовжує заражати інших.

D – об’єкт не виконує свої функції (dead). Цей клас буде особливо важливий у моделях поширення шкідливого коду із високою ймовірністю порушення доступу та цілісності даних.

Наприклад, модель SEIS означає, що об’єкт спочатку є вразливим для атаки типу (*S*), потім хтось із частин об’єкта заражається і вступає в інкубаційний період – залишається у мережи але не розпосюджуется (*E*), після деякого часу або обставин об’єкт починає заражати інших (*I*), але зрештою знову переходить у клас вразливих – якщо вірус не видаляється.

Можливі інші варіанти переміщень між класами моделі [7, 9, 19]:

- SIRS: для заражених об’єктів, після лікування яких залишається тимчасовий імунітет-засіб лікування, і об’єкти, що вилікувані, але через якийсь час знову стають вразливими;
- SIS: спрощена модель для вірусів, для яких не виробляються антивірусні заходи.

Крім того, різні набори класів можуть використовуватись у різних типах моделей. Стандартні моделі будуються на звичайних диференціальних рівняннях, які описують співвідношення об’єктів різних класах у кожен час. Однак у таких моделях не враховуються важливі деталі: різний ступінь уразливості об’єктів до такого роду атаки чи закономірності локальних контактів між об’єктами.

Тому необхідно розробляти моделі, які включають різні класи об’єктів, й особливості їх взаємодій.

За основу візьмемо модель Лотка – Вольтера, математична модель Хижак – Жертва. Передбачаємо, що лікування від зараження об’єктів вірусами потребує часу. Тому удосконалення моделі у першому наближенні будемо робити за

рахунок введенням запізнення у диференціальні рівняння класичної моделі Лотка – Вольтера.

Нехай *t* - час здійснення атаки та її відбиття, *x(t)* – функція яка описує атаку у момент часу *t*, *y(t)* – функція яка описує поведінку об'єкта також у момент часу *t*.

Визначимо функцію для нападника

$$f(t) = \frac{c \cdot x(t) \cdot y(t)}{(1 + dx(t))}.. \tag{2.10}$$

Функція (2.10) відповідає за успішний напад на об'єкт.

Для пояснення рівняння розкладемо функцію на складові:

$$f(t) = \frac{c \cdot x(t) \cdot y(t)}{(1 + x(t))} = \frac{x(t) \cdot c}{dx \cdot (1 + x(t))} + \frac{c \cdot y(t)}{dt}. \tag{2.11}$$

Перша складова виразу (2.11) $\frac{x(t) \cdot c}{dt \cdot (1 + x(t))}$ буде відповідати за кількість нападників, друга складова $\frac{c \cdot y(t)}{dt}$ буде відповідати за ліквідування нападників (вірусів). Обидві складові описують взаємодію Нападник - Об'єкт.

Зробимо припущення: не будемо враховувати різницю між різними видами вірусів та методами її знешкодження, також не будемо враховувати тимчасове зростання вірусів та методів їх знешкодження. Тоді математична модель прийме вигляд

$$\begin{cases} \dfrac{dx(t)}{dt} = k_1 \cdot x(t) - b \cdot x(t) \dfrac{dy(t)}{dt} y(t) + a_1 \cdot (t - \Delta t_1) \\ \dfrac{dy(t)}{dt} = k_2 \cdot y(t) - \dfrac{dx(t)}{dt} \cdot \dfrac{c \cdot x^2(t)}{(1 + x(t))} + \dfrac{c \cdot y(t - \Delta t_2)}{t} \end{cases}, \tag{2.12}$$

де:Δt_1 – час необхідний для підготовки нападу;

Δt_2 – час необхідний для підготовки систем захисту;

$(t-\Delta t_1)$ –кількість можливих варіантів нападу у попередній момент часу;

$(t-\Delta t_2)$ –кількість можливих варіантів нападу у попередній момент часу.

Одразу робимо припущення, що Δt_1 та Δt_2 набагато менші за час t.

Для успішного функціонування системи необхідно щоб вона була стійкою, тобто щоб будь-яке збурення чи напад не міг вивести систему з рівноваги (робочого стану). Інакше кажучи щоб система була стійкою. З цією метою проаналізуємо систему рівнянь (2.12) на стійкість.

Для цього розкладемо $x(t-\Delta t_1)$ та $y(t-\Delta t_2)$ у ряд Тейлора зі збереганням тільки лінійних членів за Δt_1 та Δt_2, підставимо ряди які ми отримали у систему рівнянь, отримуємо

$$\begin{cases} \dfrac{dx(t)}{dt}(1 + a_1 \Delta t_1) = -k_1 \cdot x(t) - b \cdot x(t) \dfrac{dy(t)}{dt} + a_1 \cdot x(t) \\ \dfrac{dy(t)}{dt}(1 + \dfrac{c}{d} \Delta t_2) = -k_2 \cdot y(t) - \dfrac{c \cdot y(t)}{d \cdot (1 + x(t))} + \dfrac{c \cdot dx(t)}{dt} \end{cases}. \tag{2.13}$$

Лінеарізуемо систему по $\tilde{x}$ та $\tilde{y}$, отримуємо

$$\begin{cases} \dfrac{dx(t)}{dt} L_1 = -k_1 \cdot (\tilde{x} + x_0) - b \cdot (\tilde{x} + x_0) \cdot (\tilde{y} + y_0) + a_1 \cdot (\tilde{x} + x_0) \\ \dfrac{dy(t)}{dt} L_2 = -k_2 \cdot (\tilde{y} + y_0) - \dfrac{c \cdot (\tilde{y} + y_0)}{d \cdot (1 + d \cdot (\tilde{x} + x_0))} + \dfrac{c \cdot (\tilde{y} + y_0)}{dt} \end{cases}, \tag{2.14}$$

де $L_1 = (1 + a_1 \Delta t_1)$, $L_2 = (1 + \frac{c}{d} \Delta t_2)$ - постійні коефіцієнти.

Після перетворень отримуємо систему:

$$\begin{cases} \frac{d\tilde{x}(t)}{dt} L_1 = \tilde{x} \cdot (-k_1 \cdot -b \cdot y_0 + a_1) - b \cdot x_0 \cdot \tilde{y} \\ \frac{d\tilde{y}(t)}{dt} L_2 = \tilde{y} \cdot (\frac{c}{d} - k_2 - \frac{c}{d \cdot (1 + d \cdot x_0)}) + \tilde{x} \cdot \frac{c \cdot y_0}{(1 + d \cdot x_0)} \end{cases}, \quad (2.15)$$

У системі 2.15 перше рівняння описує поведінку нападника, а друге рівняння поведінку системи. Система диференціальних рівнянь є розробленою моделлю системи захисту персональних даних у інформаційних мережах. У даному випадку ця система є системою диференціальних рівнянь з запізненням.

2.3. Розробка моделі захисту персональних даних з урахуванням параметру загальної довіри

Розробка моделі захисту персональних даних використовує базовий підхід на базі виразу

$$D = \langle D_j, D_n, D_m, D_k \rangle \quad (2.16)$$

де D – загальна довіра;

D_j – довіра на надання послуг;

D_n – довіра делегування;

D_m – довіра доступу до користувача;

D_k – довіра яка визначає міру віри.

Розроблена модель вираз 2.16 яку можливо записати у вигляді

$$\begin{cases} \tilde{X} = D - \frac{1}{L_1} \cdot [\tilde{x} \cdot (-k_1 \cdot -b \cdot y_0 + a_1) - b \cdot x_0 \cdot \tilde{y}] \\ \tilde{Y} = \frac{1}{L_2} \cdot [\tilde{y} \cdot (\frac{c}{d} - k_2 - \frac{c}{d \cdot (1 + d \cdot x_0)}) + \tilde{x} \cdot \frac{c \cdot y_0}{(1 + d \cdot x_0)}] \end{cases}, \quad (2.17)$$

де $\tilde{X}$ - описує поведінку нападника, $\tilde{Y}$ - описує поведінку система захисту.

Такий параметр як комплексна довіра буде впливати не тільки на параметри системи захисту, а ще на нападника. Можливо розглядати декілька варіантів втрати довіри. Ми зосередимось на двох крайніх випадках, а саме повну втрату довіри тоді $D_i \leq 0$ та повну довіру. Після проведення моделювання це дозволить з'ясувати поведінку системи на граничних режимах та наддасть можливість визначати поведінку системи захисту персональних даних у граничному діапазоні значення комплексної довіри.

Таким чином вираз 2.17 це система рівнянь яка відображає математичну модель системи захисту персональної інформації з урахуванням таких параметрів, як запізнення реагування на атаку та параметра комплексної довіри.

2.4. Розробка моделі захисту персональної інформації за рахунок урахування параметра розширення мереж

В останні роки різко зріс інтерес до дослідження великих мережевих структур, таких як Інтернет, складні соціальні мережі. Неосяжні розміри та складність мереж зумовили зростання різноманітності їх стохастичних моделей та становлення теорії випадкових графів.

Одним із найбільш широко відомих видів випадкових графів є граф Ердеша-Реньї [31–35]. Його генерують на *N* вершинах: будь-яку пару випадково, з ймовірністю *p*, пов'язують ребром. Різні характеристики такого графа -

коефіцієнт кластеризації, діаметр, ймовірності появи тих чи інших підграфів та інші виражені через його параметри N і p [39]. Локальний ступінь k зв'язності його вершин має біномний розподіл ймовірностей, її середнє значення - $\langle k \rangle = p(N - 1)$. Надалі цікавитимемося нескінченними чи дуже великими графами. При $\langle k \rangle$=const біноміальний розподіл ступеня вершин графа Ердеша-Реньї стає пуассонівським (звідси друга назва цього графа – пуассонівський граф). Граф Ердеша-Реньї є найпростішим випадковим графом. Наявність зв'язку між будь-якими двома його вершинами визначається "чистою випадковістю", незалежно від наявності та конфігурації зв'язків між іншими вершинами. При моделюванні низки реальних мереж їх коректне використання не можливе. Це спричинило появу великої кількості робіт, присвячених дослідженню інших видів випадкових графів [49 – 51].

Виходячи з цих висновків у якості базової часткової моделі візьмемо модель великих мережевих структур, що формуються за правилом кращого зв'язування (називається ще правилом "багаті стають багатшими"). Модель Альберта Барабаші та Річки Альберта.

Ця модель є випадковим динамічним графом. Вільні кінці ребер кожної нової вершини приєднуються переважно до вершин, багатих зв'язками: ймовірність p_i з'єднання ребра з i-ю вершиною графа пропорційна локальному ступеню зв'язності k_i цієї вершини

$$P(k_i) = \frac{k_i}{\sum_j k_j}. \qquad (2.18)$$

Зі зростанням графа Барабаші-Альберт (БА) ряд його числових характеристик сходиться до стаціонарних значень. Так, відома стаціонарна ймовірність Q_k того, що випадково обрана вершина графа БА має ступінь зв'язності k [62–64, 99]

$$Q_k = \frac{2m(m+1)}{k(k+1)(k+2)}, \quad k \geq m, \tag{2.19}$$

де m - кількість орієнтованих дуг;

k - кількість ступень вершин у яку заходить дуга (ступень зв’язаності).

Р. Альберт та А. Барабаші назвали запропонований граф та його модифікації scale-free (безмасштабними) графами.

Актуальність розвитку теорії scale-free графів обумовлюється широкою сферою їх застосування та значимістю одержуваних на їх основі результатів. До найбільш важливих з них можна віднести оптимальні стратегії боротьби з інфекцією в інформаційних та соціальних мережах, поширення методів теорії критичних явищ на завдання аналізу стійкості великих мереж та багато інших.

Саме тому, у якості базової моделі, будемо використовувати модель граф Барабаші-Альберт (графа БА).

Для удосконалення моделі захисту персональної інформації зробимо асоціативний ряд, Інтернет - це графи. Будемо уявляти собі вершини цього графа сайти в інтернеті, а ребра цього графа, спрямовані, як гіперпосилання між цими сайтами. Тобто, якщо є один сайт, який посилається на інший, ми проводимо направлене ребро. Якщо таких посилань кілька, скажімо, є кілька сторінок, на які посилаються інші сторінки, то ми проводимо, відповідно, кілька ребер. Ребра можуть бути спрямовані у різні боки, і можуть виникати навіть петлі. Адже зрозуміло, що всередині кожного сайту можуть бути сторінки, які також один одного цитують.

В оригінальному формулюванні авторів принцип кращого зв'язування сформульовано наступним чином [72, 97]: реєструючи зростаючий характер мережі і починаючи з невеликої кількості m_o вершин, на кожному кроці часу ми додаємо нову вершину з $m < m_o$, ребрами, які пов'язують нову вершину з m

вершинами, вже існуючими у системі. Включно з кращим зв'язуванням, ми вважаємо, що ймовірність *P* того, що нова вершина буде пов'язана з вершиною і, залежить від зв'язності k_i; цієї вершини так, що $P(k_i) = \frac{k_i}{\sum_j k_j}$. Після *t* кроків часу модель приводить до випадкової мережі з $t + m_o$, вершинами та m_t ребрами».

Як виявилося, ідея кращого зв'язування та графи БА пояснюють зростання не лише Інтернету, а й багатьох інших зростаючих мереж, у тому числі й соціальних. Тому саме з метою удосконалення моделі захисту персональної інформації ми обираємо метод графів БА. Враховуючи особливість розширення соціальних мереж, а саме то, що зв'язок між елементами частіш за все є нелінійним. Будемо використовувати графи з нелінійним правилом переважного зв'язування (НППЗ). Відповідно до [4], для вирощування графа з НППЗ використовується початковий граф з кількох вершин, пов'язаних ребрами. Нова вершина графа та інцидентні їй ребра мають назву приріст графа. Вершини графа зі ступенем *k* мають функцію переваги (вагову функцію) *f(k): f(k))* > 0, якщо $g < k < M$, інакше *f(k)* = 0 (для випадка $g>1$). Імовірність зв'язування ребра (дуги) приросту з вершиною графа, що має *N* вершин, визначається у вигляді

$$p_i = \frac{f(k_i)}{\sum_j f(k_j)}, \quad i, j = 1,..., N. \tag{2.20}$$

Кожне прирощення є вершиною з випадковим числом *x* інцидентних їх ребер. Кількість ребер у прирощенні визначається як випадкова величина $x \in \{g, g+1,..., h\}$, яка має дискретний розподіл ймовірностей $\{r_k\}$.

Ймовірність $r_k = P(x = k) > 0$ при $g < k < h$, $\sum_{k=g}^{h} r_k = 1$. При цьому $h<M$ кінцеве.

Таким чином, алгоритми генерації графа з НІПС задається параметрами *f(k)* та $\{r_k\}$, що задовольняють перерахованим вище обмеженням.

З урахуванням проведених досліджень система рівнянь яка описує модель системи захисту персональної інформації з урахуванням розширення соціальних мереж за нелілейним законом буде мати вигляд

$$\begin{cases} \tilde{X} = D - \dfrac{1}{L_1} \cdot [\tilde{x} \cdot (k_1 \cdot b \cdot y_0 + a_1) - b \cdot x_0 \cdot \tilde{y}] \\ \tilde{Y} = \dfrac{1}{L_2} \cdot [\tilde{y} \cdot (\dfrac{c}{d} - k_2 - \dfrac{c}{d \cdot (1 + d \cdot x_0)}) + \tilde{x} \cdot \dfrac{c \cdot y_0}{(1 + d \cdot x_0)}] + \dfrac{2m(m+1)}{k(k+1)(k+2)} \end{cases}. \quad (2.21)$$

Або

$$\begin{cases} \tilde{X} = D - \dfrac{1}{L_1} \cdot [\tilde{x} \cdot (k_1 \cdot b \cdot y_0 + a_1) - b \cdot x_0 \cdot \tilde{y}] \\ \tilde{Y} = \dfrac{1}{L_2} \cdot [\tilde{y} \cdot (\dfrac{c}{d} - k_2 - \dfrac{c}{d \cdot (1 + d \cdot x_0)}) + \tilde{x} \cdot \dfrac{c \cdot y_0}{(1 + d \cdot x_0)}] + Q_k \end{cases}. \quad (2.22)$$

Таким чином вираз 2.21 це система рівнянь яка відображає математичну модель системи захисту персональної інформації з урахуванням таких параметрів, як запізнення реагування на атаку, параметра комплексної довіри та урахування параметра розширення мереж.

Висновки до розділу 2

Розкрито і запропоновано розробку та удосконалення моделі захисту персональних даних з урахуванням специфіки соціальних мереж, що акумулюється у наступному:

1. Представлено дослідження існуючих моделей соціальних мереж у площині видів їх загроз. Проаналізовано дані кібератак на персональні дані

користувачів. Визначенні параметри оцінки захисту мереж на основі аналізу моделей графів соціальних мереж.

2. Визначено параметри для оцінювання рівня захисту соціальних мереж, які включають аналіз міри центральності, перевірку гіпотези щодо ланцюга спільних знайомих, а також обчислення коефіцієнта щільності, що визначається як відношення кількості ребер у досліджуваному графі до максимально можливої кількості ребер у повному графі з таким самим числом вершин. Окрім того, враховано силу структурної позиції учасника в мережі. Це дозволило здійснити аналіз захищеності персональних даних у контексті загальної структури соціальних мереж.

3. Розглянуто підходи до застосування моделей дослідження інформаційних мереж. Обґрунтовано базова загальна модель захисту персональних даних у мережах. Обрані основні параметри захисту мереж від яких залежить система захисту персональних даних. До цих параметрів відносяться: параметр запізнення реагування на атаку, параметр комплексної довіри, параметр розширення соціальних мереж та параметр сильних та слабких зв’язків у мережах.

4. Вперше розроблена модель захисту персональних даних у інформаційних мережах зі урахуванням специфіки соціальних мереж, а саме: запізнення реагування на атаку з метою її припинення або подолання її наслідків. Досліджена реакція запізнення системи захисту особистих даних на можливі атаки з метою пошкодження цілісності, порушення конфіденційності та доступу.

РОЗДІЛ 3
РОЗРОБКА МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ З УРАХУВАННЯМ СПЕЦИФІКИ СОЦІАЛЬНИХ МЕРЕЖ

Глобальні мережі стали частиною життя мільйонів людей, які отримали вільний, відносно нескладний, самостійний доступ до інформації, а також можливість спілкування з іншими без обмежень, пов'язаних з географічною відстанню.

Цифрове суспільство, будучи по суті одним із етапів постіндустріального суспільства, має, що найменше, низку особливостей, серед яких можна назвати: посилення ролі інформації та знання у житті суспільства; масове впровадження інформаційних технологій, що дозволило створення глобального інформаційного простору; стрімкий розвиток інформаційних комунікацій [57–59]. У той же час у висновках дослідників простежуються неоднозначні оцінки і наростаюча настороженість з приводу цифровізації суспільства, що набирає обертів, і розширення кіберпростору [73–75].

3.1. Удосконалення методу оцінки поведінки системи захисту персональної інформації

Виходячи з поставленої мети щодо необхідності забезпечення ефективного захисту персональної інформації необхідно з’ясувати при яких параметрах функціонування інформаційної мережи система буде стійкою. Тобто які граничні параметри у моделі захисту допустимі. Запропонована математична модель захисту персональних даних складеться з системи диференціальних рівнянь нормальної форми. Завданням дослідження є удосконалення методу фазової площини, а точніше застосування якісної теорії диференціальних рівнянь для визначення поведінки системи захисту персональної інформації під впливом зовнішніх факторів.

Удосконалення методу буде полягати, утому, що не вирішується ні точно, ні наближено диференціальні рівняння та у загалі не робляться числові обчислення. Математичне тлумачення доводить, що усі рішення будуть знаходитися у межах, яку називають фазової площиною, а усі рішення умовно представлені фазовою крапкою. Фазова крапка, що рухається, малює криву, яка має назву фазової траєкторії [2, 17]. Іншими словами через кожну крапку фазової траєкторії проходить фазова крива. Кожна крапка фазової траєкторії є рішенням системи диференціальних рівнянь. Відповідно до цього стан фізичної системи, що описується автономною системою, зображується точкою $x = (x_1, \ldots x_n)$ n-вимірного простору. Така точка називається фазовою точкою, а стани фізичної системи відповідають точкам певної області (де визначені праві частини) і що останню область називають фазовим простором [17].

Для визначення стійкості скористуємось теоремами Ляпунова. Існує кілька понять стійкості: стійкість по Ляпунову, орбітальна стійкість та стійкість за Пуассоном [55]. Стійкість по Ляпунову розглядає відстань між сталою та збудженою траєкторіями.

$$\forall \varepsilon > 0 \quad \exists \delta > 0 : \left\| x_0 - \tilde{x}_0 \right\| < \delta \Rightarrow \left\| x(t) - \tilde{x}(t) \right\| < \varepsilon. \tag{3.1}$$

Орбітальна стійкість характеризує мінімальну відстань між фазовою точкою обуреної траєкторії в даний момент часу і орбітою (зазвичай це замкнута крива, що відповідає фазовій траєкторії) руху, що досліджується. Траєкторія, стійка за Ляпуновим, завжди орбітально стійка; зворотне твердження в загальному випадку не вірно. Отже, орбітальна стійкість є більш слабка вимога, ніж стійкість за Ляпуновим. Стійкість за Пуассоном є найслабшою вимогою. Вона означає, що фазова траєкторія не залишить обмеженої фазової області простору при $t \to +\infty$: провівши нескінченно тривалий час усередині цієї області,

фазова траєкторія неминуче повертається в скільки завгодно малу околиця початкової точки.

Одним із практичних прийомів побудови квадратичної функції Ляпунова може бути побудова знакопостійної лінійної комбінації диференціалів квадратичних функцій фазових змінних системи. Диференціали квадратичних функцій фазових змінних визначаються з диференціальних рівнянь обуреного руху при множенні останніх на відповідні фазові змінні. Якщо це вдається (похідна допоміжної функції – знакопостійна) та умова її позитивної визначеності є водночас і умовою асимптотичної стійкості нульового рішення, то порушення цієї умови (позитивної визначеності) тягне за собою нестійкість нульового рішення.

Умови асимптотичної стійкості виконуються у всій фазовій площині, це свідчить про те, що будь-яка траєкторія збурення з плином часу прагне початку координат (стаціонарного режиму), тобто областю тяжіння є вся фазова площина.

За відсутності нелінійних членів похідна функції Ляпунова дорівнювала б нулю, отже, система лінійного наближення стійка (випадок чисто уявного коріння). Як зазначалося це критичний випадок пари чисто уявного коріння. В даному випадку нелінійні члени призвели до асимптотичної стійкості нульового рішення (область тяжіння вся фазова площина).

Фазові портрети (фазові діаграми) описують стан системи, показують як динамічні змінні залежать друг від друга. Головна перевага фазових портретів у тому, що вони будуються без рішення системи рівнянь. Використовуючи методи оцінки стійкості за Ляпуновим можливо зробити висновок: якщо фазовий портрет має фокус, точку куди збігаються лінії фазової траєкторії, то система стійка. Якщо розбігаються тоді система нестійка.

Запропанований удосконалений метод фазової площини ілюструє повне розмаїття можливих станів системи й описує картину її динаміки. Проведене

застосування методу, моделювання та отримані результати, підтверджують, що адаптація методу зроблена адекватно. Визначення стійкості системи захисту персональних даних з урахуванням специфіки функціонування соціальних мереж можливо робити за допомогою методу фазової площини. Що і доведено у роботі. Таким чином використання методу фазової площини є удосконаленим методом для дослідження стійкості моделі захисту персональної інформації.

3.2. Розробка допоміжного методу захисту персональної інформації зі врахуванням розповсюдження таргетованої інформації у соціальних мережах

Розробку методу захисту персональної інформації з врахуванням розповсюдження таргетованої інформації у соціальних мережах можливо представити у вигляді наступного алгоритму:

1. Початок.

2. Крок 1: Виявити групу користувачів, потім користувача для якого призначена таргетована інформація, обрати об'єкт нападу.

3. Крок 2: Визначити самого впливового користувача, якій є лідером розповсюдження таргетованої інформації.

4. Крок 3. Знайти можливість змусити лідера поширити таргетовану інформацію. Або знайти можливість розповсюджувати інформацію від імені лідера, використовуючи різні методи соціальної інженерії.

5. Кінець.

Метод розповсюдження таргетованої інформації у соціальних мережах можливо представити сукупністю вихідних даних та результатів роботи, які дозволять формалізувати різні сценарії атак на ресурс.

Сукупність вихідних даних та результатів роботи загального методу поширення таргетованої інформації у соціальних мережах представлені у таблиці 3.1.

Таблиця 3.1

Параметри узагальненого методу розповсюдження таргетованої інформації у інформаційної мережи

Вхідні параметри	Сукупність звязків	Особисти параметри користувача
1	2	3
Вхідні параметри: $X = \{x_1, ..., x_j\}$ – користувачі ONS	$x_1 = \{x_1^i \mid i = 1, n\}$ – ідентифікатор і користувача	x_1^1 – графічне зображення користувача, x_1^2 – ПІБ, x_1^3 – логін користувача, x_1^4 – вік, x_1^5 – характеристика користувача (інтереси, приналежність до спільнот, соціальних мереж, освіта, місце проживання тощо)
	$x_2 = \{x_2^j \mid j = 1, m\}$ – пости користувача соціальної мережі	x_2^1 – кількість постів, x_2^2 – кількість коментарів до постів, x_2^3 – геолокація постів.
	$x_3 = \{x_3^\gamma \mid \gamma = 1, s\}$ – оцінки постів та повідомлень	x_3^1 – кількість оцінок інших користувачів «мені подобається», x_3^2 – кількість репостів повідомлень ін. користувачів спільнот x_3^3 - кількість повідомлень в інших соціальних мережах, x_3^4 – кількість повідомлень особистого діалогу користувача
	$x_4 = \{x_4^\lambda \mid \lambda = 1, \beta\}$ – друзі і підписники	x_4^1 – кількість підписників користувача, x_4^1 – кількість друзів
	$x_5 = \{x_5^\sigma \mid \sigma = 1, p\}$ – профіль сторінки користувача	x_5^1 – закритий профіль, x_5^2 – відкритий профіль
	$x_6 = \{x_6^k \mid k = 1, \tau\}$ – пости	x_6^1 – кількість постів користувача, x_6^2 – силки на особисті сайти, інші соціальні мережі, x_6^3 – кількість репостів

	$x = \{x^d \mid d = 1, w\}$ – ціль зловмисника	x^1 – фінансова вигода, x^2 – самоствердження перед самим собою, x^3 – самоствердження перед лицем певної спільнотиа/групи соціальної мережі, x^4 – відплата знайомим користувачам, суспільству, світовій системі x^5 – відплата роботодавцю x^6 – перевага в конкурентній боротьбі, x^7 – задоволення хуліганських мотивів, x^8 – задоволення інтересів, дослідницьких цілей
Вхідні параметри внутрішних станів алгоритма $Z = \{z_1, ..., z_\gamma\}$ – використання методів соціальної інжене-рії користувачем ONS	$z_1 = \{z_1^i \mid i = 1, k\}$ – використання методів отримання доступу до даних авторизації	z_1^1 – використання нових вразливостей соціальної мережі і різних протоколів передачі даних, z_1^2 – використання відомих вразливо-стей і протоколів передачі даних, z_1^3 – розповсюдження силок на сайти, які вміщають відомі шкідливі програми, z_1^4 – розповсюдження копій відомих шкідливих програм, z_1^5 – розповсюдження силок на сайти, які містять нові самописні шкідливі програми, z_1^6 – поширення копій нових самописних шкідливих програм, z_1^7 - розповсюдження силок на фішингові
		сайти; z_1^8 – використання атаки прямого перебору; z_1^9 – використання атаки по словнику, z_1^{10} – використання веселкових таблиць, z_1^{11} - взлом акаунта, z_1^{12} – взлом поштового ящика користувача, z_1^{13} -використання та ознайомлення з файлами із конфіденційною інформацією шляхом використання доступа до мережі організації, z_1^{14} – крадіжка і ознайомлення з файлами із конфіденційною інформацією шляхом використання фізичного доступу до комп'ютера користу- вача

	$z_3 = \{z_3^\tau \mid \tau = \overline{1,\omega}\}$ – використання методів соціальної інженерії, спрямованих на друзів лідера соціальної мережі	z_3^1 – використання методів отримання доступу до даних авторизації ($z_1 = \{z_1^i \mid i = \overline{1,k}\}$) для взлому друга лідера, z_3 – встановлення домовленостей з другом лідера ONS під видом розповсюдження благодійної інформації соціального спрямування z_3^3 – встановлення домовленостей з другом лідера соціальної мережі під видом розповсюдження реклам- ної інформації з обіцянками ви- нагороди як лідера, так і друга, z_3^4 – встановлення домовленостей з другом лідера ONS для розповсюдження інформації апелюючи до інших скритих мотивів (самоствердження, отримання інформації).

Деталізація внутрішніх станів загального методу поширення таргетованої інформації у соціальних мережах закладена в основу методу захисту інформації.

Для подальшого розвитку методу захисту користувачів від таргетованої інформації, необхідно виявити межі інформаційного обміну користувачів у Інтернеті та соціальних мережах. Для цього потрібно досліджувати поведінку користувачів у різних ситуаціях, пов'язаних із поширенням таргетованої інформації у соціальних мережах. Тобто метод захисту користувачів від таргетованої інформації набув подальший розвиток за рахунок досліджування поведінки користувачів у різних ситуаціях.

Для перевірки адекватності зазначеного методу використовувалися статистичні данні.

Вибірка даного дослідження являє собою 2499 користувачів соціальних мереж Twitter, Facebook, що є модераторами (адміністраторами) спільнот користувачів. За віком, це молодь у віці від 17 до 30 років. Усі 2499 користувачів брали участь у тестовому опитуванні щодо ситуацій поширення небажаної

таргетованої інформації у соціальних мережах та протидії поширенню інформації такого змісту [153]. Користувачі соціальних мереж, нажаль, беруть участь у численних ситуаціях, пов'язаних із поширенням таргетованої інформації, як у ролі жертви, так і у ролі потенційного зловмисника. Завдяки цьому на користувачах можливо вивчати процес прийняття рішення, фактори у ситуаціях підвищеного ризику поширення таргетованої інформації та небажаної інформації загалом у соціальних мережах.

У дослідженні всі тестові опитування фірмою Dragon Capital, були анонімними та проводилися протягом 6 місяців 2021 – 2023 років. Опитування проводилося за допомогою тестових бланків, результати опитування обробляли у статистичному пакеті Statistica 12.6. Усі респонденти дали письмову згоду та добровільно погодилися на участь у дослідженні [103].

У статистичному дослідженні вивчався вплив соціальної інформації, а саме ситуаційних та особистісних параметрів на підвищення ймовірності поширення небажаної інформації. Для цього було зібрано інформацію від респондентів про ситуації, отримання небажаної інформації. Приймалось, що ситуація отримання таргетованої інформації визначається як примусове доведення потенційним зловмисником інформаційного повідомлення засобами соціальних мереж до потенційної жертви для досягнення своєї мети.

Ситуація поширення небажаної інформації передбачає масову передачу потенційним зловмисником інформаційних повідомлень користувачам соціальних мереж. Саме передачу інформаційних повідомлень користувачам соціальних мереж для досягнення головної мети. Ситуація протидії розповсюдженню небажаної інформації – це ситуація, у якій отримання та поширення небажаної інформації користувачем, не відбулося з будь-якої причини. Наприклад, блокування підозрілого сповіщення, або блокування ботів що розсилають небажану інформацію.

Значення параметрів тестового опитування були представлені у бінарній шкалі. Усі параметри приймали значення або "0", або "1", що дозволяє виявляти заходи зв'язку між ними. Відповідно до теорії обробки соціальної інформації (TOCI) проаналізуємо процес прийняття рішення зловмисником у ситуації поширення таргетованої інформації. TOCI – це соціальний когнітивний підхід, заснований на припущенні, що людина «входить у соціальну ситуацію з набором біологічно обмежених можливостей та з базою даних про свій минулий досвід» [103].

Середній вік респондентів становив 22 роки. З них 74,99% чоловіків, решта - жінки. Більше половини респондентів мають закінчену вищу освіту (65,98%). Більшість респондентів зазначили належність до нижчому класу (70,99%), так як респонденти – це студенти, основним джерелом яких є стипендія та випадковий заробіток. Інші респонденти відносять себе до середнього класу у 26% випадків – це респонденти магістранти та аспіранти, які мають можливість повноцінно працювати і займатися наукою. Статистика сімейного стану респондентів також свідчить про те, що студенти в період здобуття вищої освіти не перебувають у шлюбі 69,03%, мають цивільного партнера 23,97%, а в офіційному шлюбі перебувають лише 7% [103].

Таким чином за допомогою подальшого розвитку методу, який враховує поведінки користувачів у різних ситуаціях, ми з’ясували на яку соціальну аудиторію найбільше впливає розповсюдження небажаної інформації. Отримані дані підтверджують висновки, щодо соціальної активності користувачів за віком та соціальним положенням. Ці дані цілком відповідають реальній ситуації обміну інформацією у соціальних мережах, що підтверджує адекватність розробленого алгоритму.

3.3. Розробка допоміжного методу визначення оцінок ефективності системи захисту персональних даних

Труднощі визначення кількісних і якісних оцінок ефективності системи захисту персональних даних (СЗПД), а отже, і об'єктивного підтвердження ефективності СЗПД, грунтуються на недосконалості існуючого нормативно-методичного забезпечення інформаційної безпеки, а також у підходах, що склалися в інформаційних технологіях, які принципово відрізняються від розроблених у традиційній інженерії. Також недостатньо опрацьовано систему показників інформаційної безпеки та не визначено в повному обсязі критерії безпеки.

Розглянемо існуючі якісні та кількісні методи аналізу ефективності систем захисту персональних даних (СЗПД). Для оцінки ефективності необхідно мати обґрунтований критерій. У науковій літературі виділяють кілька типів критеріїв [111]:

- критерії типу «ефект-витрати», які дозволяють оцінювати досягнення цілей функціонування СЗПД за заданих витрат (економічна ефективність);
- критерії, що оцінюють якість СЗПД та дозволяють відсіяти варіанти, які не відповідають встановленим обмеженням;
- штучно сконструйовані критерії для оцінки інтегрального ефекту (наприклад, «лінійне згортання» окремих показників, методи теорії нечітких множин).

Дослідження показують, що на сьогодні відсутній універсальний підхід до вирішення завдань цього класу, що призводить до використання різноманітних методів оцінки, які не завжди взаємопов’язані. Аналіз існуючих методів свідчить, що жоден з них не позбавлений недоліків. Тому для оцінки ефективності СЗПД необхідно щоразу обирати комбінацію різних методів. У той же час основною метою побудови та функціонування СЗПД, у загальному випадку, є досягнення необхідного рівня інформаційної безпеки у глобальній інформаційній системі.

Для досягнення мети створення загального методу СЗПД має бути можливість успішного вирішення наступного комплексу завдань [110]:

– збирання, обробка та аналіз подій безпеки, що надходять у систему з безлічі гетерогенних джерел;
– оперативна оцінка захищеності інформаційних та інших критично важливих ресурсів;
– аналіз та управління ризиками безпеки інформаційної системи;
– виявлення розбіжностей інформаційних ресурсів і бізнес-процесів з внутрішніми політиками безпеки та приведення їх у відповідність один з одним.

Виходячи з цього, необхідно зробити вибір показників, що використовуються при розробці СЗПД, та сформувати вимоги до неї (рис. 3.1).

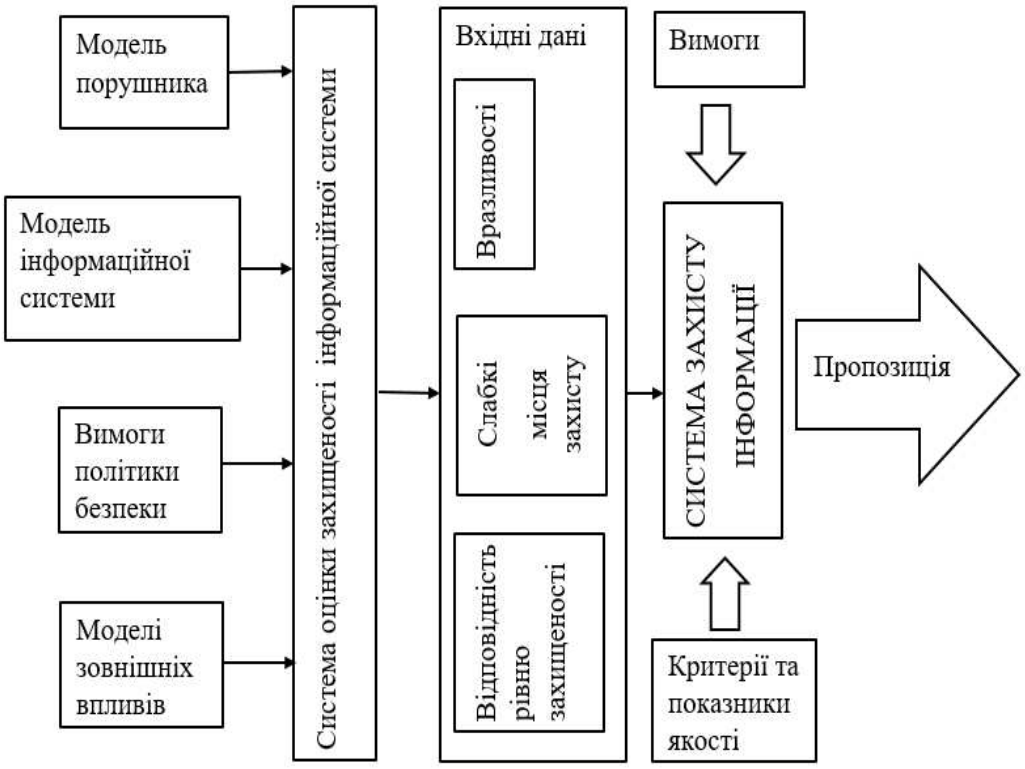

Рис. 3.1. Модель застосування системи захисту на об'єктах інформаційної діяльності [75, 101]:

Так як у процедурі прийняття рішення, саме при оцінці ризику СЗПД істотне значення має моделювання об'єкта захисту та поведінка зловмисника, то доцільно запропонувати показники захищеності персональних даних, які можливо буде використовувати для оперативної оцінки захищеності персональних даних та інших критично важливих ресурсів.

Вибір показників захищеності даних ґрунтується на [58 – 67]:

– формуванні графа атак та залежностей сервісів на основі даних про топологію мережі, обліку навичок та позиції порушника й формування профільних графів атак;

– аналізі подій, що відбуваються в системі, для відстеження поточної ситуації з безпеки;

– обчисленні показників захищеності на основі цих даних.

Але у цьому підході закладено необхідність розробки модуля моделювання загроз. Це вимагатиме реалізації дуже чіткої побудови графів можливих атак та дій порушника, з прив'язкою до діючих бюлетенів та стандартів у галузі опису вразливостей та визначення оцінки ризиків [96 – 98]. Тому для оцінки рівня захищеності СЗПД пропонується на першому етапі використовувати показники захищеності мережевого рівня, що базуються на топології інформаційної системи: вразливість хоста (АРМ), критичність (слабкість) хоста, а також розширити список за рахунок оригінальних показників, що визначаються застосуванням інструментальних засобів оцінки захищеності (рис. 3.2).

У загальному випадку доцільно використовувати SCAP.

SCAP (Security Content Automation Protocol) –визначає три процеси: пошук та виправлення вразливостей, автоматичне налаштування конфігурацій, а також оцінку рівня безпеки.

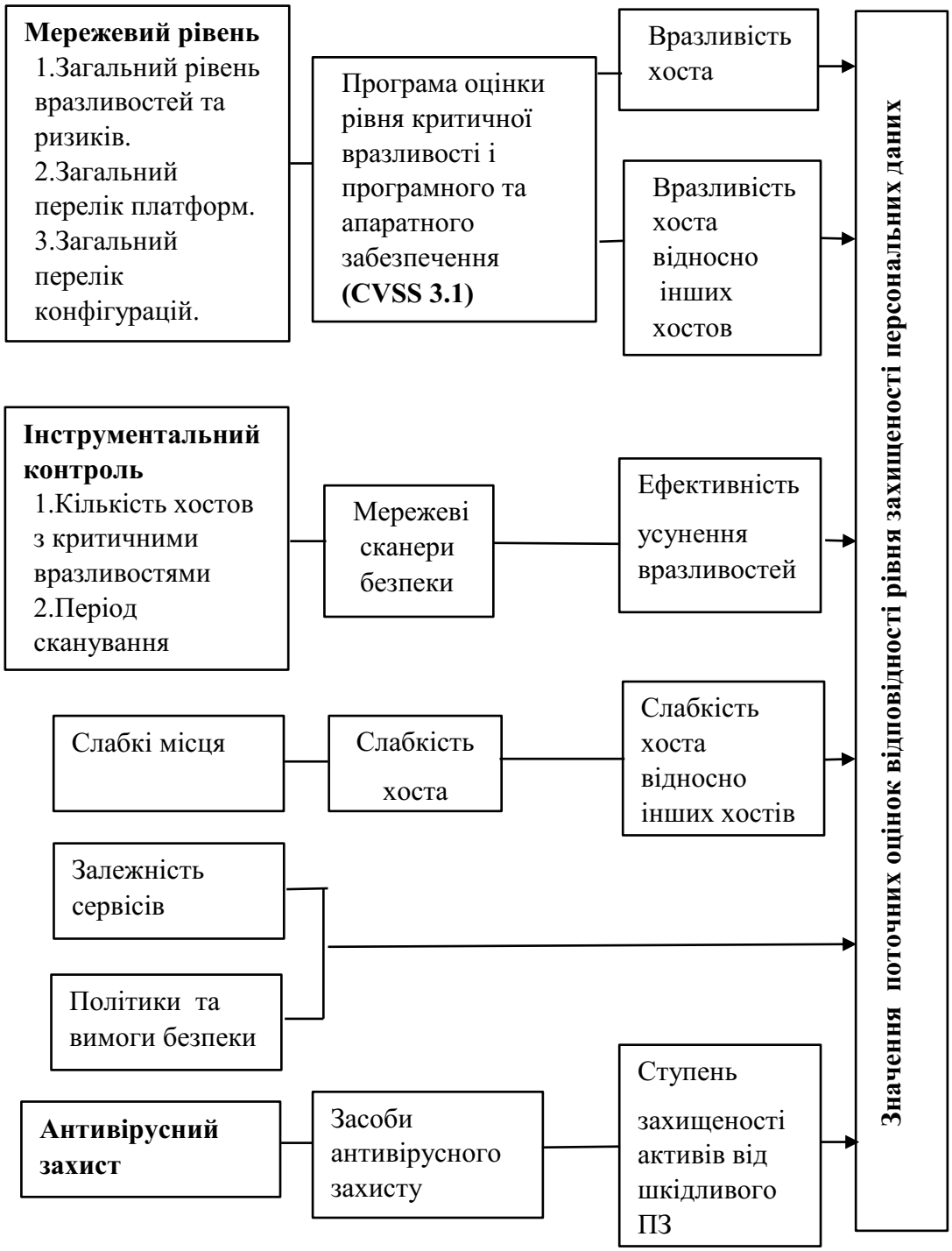

Рис. 3.2. Структура критеріїв оцінки відповідності рівня захищеності

SCAP включає чотири мови: XCCDF, OVAL, OCIL, ARF; чотири схеми ідентифікації: CCE, CPE, SWID, CVE та дві метрики: CVSS, CCSS.

Тобто SCAP включає переліки, виражені з використанням стандартизованих специфікацій: загальний перелік конфігурацій, що використовується для визначення топології обчислювальної мережі, загальний перелік платформ і загальний перелік вразливостей та ризиків, що використовуються для визначення характеристик хостів. При цьому оцінка певних особливостей уразливості (наприклад, слабких місць програмного забезпечення та проблем конфігурації безпеки) й визначення кількісного значення впливу даної вразливості дозволяють проводити її вимірювання та оцінку для оцінки рівня захищеності інформаційних систем. Такий підхід виправданий і появою вітчизняної бази опису вразливостей.

Розглянемо показники захищеності мережного рівня, що базуються на показнику «уразливість хоста» на основі відомих уразливостей та базової оцінки нової версії CVSS v3.1 Ratings.

Згідно з новим стандартом, метрики експлуатації розраховуються для вразливого компонента, а метрики впливу для атакованого [101– 104]. У CVSSv2 не було можливості описати ситуацію, в якій вразливий компонент і атакований різняться.

Показник уразливість хоста. Показник вразливісті хоста визначимо на основі відомих вразливостей та базової оцінки нової версії CVSS v3.1 Ratings

$$Vulnerability\ (H_k) = \sum_{i=1}^{n} Critical_{basescore(vi)}, \qquad (3.2)$$

де H_k, - хост у складі інформаційної системи з k-им порядковим номером, $k = [1,M]$.

Характеристика параметра «уразливість хоста» проводиться в процесі налаштування системи і варіюється в інтервалі від 1 до 10.

В існуючих методах «жорстка» оцінка межі, може вплинути на якість оцінювання шляхом відсічення впливу вразливостей з меншим значенням. Але при цьому корелюючими властивостями з іншими вразливими, тому у розробленій загальній методиці доцільно цей параметр зробити змінним, щоб користувач системи міг коригувати його самостійно.

Показник слабкість хоста. Показник слабкість хоста визначається на основі стандартів CWE і CWSS

$$Weakness\,(H_k) = \sum_{i=1}^{n} Critical_{CWSS_{score(wi)}}, \tag{3.3}$$

де H_k, - хост у складі інформаційної системи з k-им порядковим номерром, $k = [1,M]$.

Завдання параметра слабкості хоста виконується в процесі налаштування системи і варіюється в інтервалі від 1 до 100. Зробимо припущення та запропонуємо граничний параметр слабкості хоста встановити на значенні, що дорівнює 60. Однак, і в цьому випадку, доцільно цей параметр також зробити змінюваним, щоб користувач системи міг коригувати його самостійно.

Розглянемо показники захищеності системного рівня, що базуються на функціонуванні інформаційної системи.

Показник залежності сервісів. Показник залежності сервісів використовується для визначення поширення шкоди. Показник виконання політик безпеки — оцінка ефективності політик безпеки, що реалізуються в інформаційній системі

$$Pol_{\sec(IS)} = \sum_{k=1}^{m} Pol_{\sec}\,(H), \tag{3.4}$$

де H_k, - хост у складі інформаційної системи з k-им порядковим номером, $k = [1,M]$.

$Pol_{\sec(IS)}(H_k)$ — нормоване значення відношення кількості реалізованих на хості H_k, політик безпеки до можливої їх кількості

$$Pol_{\sec(Hk)} = \frac{i_{Pol\_\sec}}{\max_{Pol\_\sec}} \times 100, \tag{3.5}$$

де $i_{Pol\_\sec}$ політик безпеки реалізованих на хості H_k;

$\max_{Pol\_\sec}$ — максимально можлива кількість політик безпеки, які підлягають реалізації на цьому хості з урахуванням вимог захисту персональних даних.

Показник виконання вимог безпеки. Показник виконання вимог безпеки, це оцінка співвідношення кількості вимог, що реалізуються в інформаційному середовищі з безпеки до загальної кількості вимог, що задаються

$$Treb_{\sec(IS)} = \frac{t_{treb\_\sec(IS)}}{\max_{Treb\_\sec}(IS)} \ , \tag{3.6}$$

де $t_{treb\_\sec}$ - кількість вимог безпеки реалізованих в інформаційній системі;

$\max_{Treb\_\sec}$ - максимально можливе число вимог безпеки, що підлягають реалізації у інформаційної системі з урахуванням вимог захисту інформації.

З урахуванням використання в ІС спеціалізованих засобів інструментального контролю захищеності (сканерів мережі, сканерів безпеки, антивірусних засобів тощо) до оцінок захищеності мережевого рівня можуть бути додані оцінки загальної захищеності системи: залежності сервісів, виконання політик та вимог безпеки, ефективність усунення вразливостей, ступінь захищеності активів від руйнівних програмних впливів.

Показник захищеності активів від руйнівних програмних дій. Показник захищеності активів від руйнівних програмних дій - оцінка ефективності функціонування антивірусного захисту:

$$\mathrm{Sec}_{activeRPV(IS)} = \sum_{k=1}^{m} \mathrm{Sec}_{activeRPV}(H_k), \tag{3.7}$$

$$\mathrm{Sec}_{activeRPV(Hk)} = w_1 \times Blok_p + w_2 \times Blok_{Malav} + w_3 \times Gr_{Host}, \tag{3.8}$$

де H_k, - хост у складі інформаційної системи з k-им порядковим номером, $k = [1,M]$;

$Blok_{Malav}$ - відсоток хостів з усуненим шкідливим ПЗ;

Gr_{Host} - кількість спрацьовувань системи автоматичного визначення загроз;

w_i - вагові коефіцієнти значень, підбираються експертним методом, на етапі формування моделі інформаційної системи.

Підсумкове значення оцінки захищеності персональних даних інформаційної системи у цьому випадку буде обчислення інтегрального показника оперативного рівня захищеності системи для подальшого аналізу при прийнятті рішень щодо безпеки.

Для отримання підсумкового рішення використовувався метод нечіткого моделювання, що позитивно зарекомендував себе в багатьох подібних дослідженнях. На основі теорії нечіткої логіки пропонується

$$\begin{cases} \Psi(IS) = \sum_{i=1}^{n} w_i q_i \\ \sum_{i=1}^{n} w_i = 1 \\ q_i \geq q_{\min} \end{cases}, \tag{3.9}$$

де q = [0,1]; w_i = [0,1]; i= [1,N];

ψ– загальний показник якості СЗПІ;

q_i - приватний показник якості СЗПІ;

q_{min} - мінімально допустиме значення і-го приватного показника якості СЗПІ;

w_i - ваговий коефіцієнт i-го приватного показника якості.

Таким чином, на основі теорії нечіткої логіки, пропонується вираз (3.9) для отримання підсумкового рішення. Тобто метод нечіткого моделювання, застосований для прийняття підсумкового рішення, щодо захищеності персональних даних у системі позитивно зарекомендував себе у теорії захисту інформації.

3.4. Розробка удосконаленого методу деперсоналізації даних для захисту персональних даних з урахуванням специфіки соціальних мереж

Захист персональних даних зводиться до впровадження технічних заходів захисту.

Базовий метод представляє декілька послідовних етапів, які необхідно пройти, щоб правильно організувати роботу з персональними даними.

Першим кроком потрібно визначити документи, які необхідно розробити організації; які обов'язки треба передбачити у посадових інструкціях працівників, які опрацьовують персональні дані в інформаційному ресурсі (системі); позначити поширені помилки та порушення при обробці персональних даних та ін.

Одним зі запропонованих варіантів методу захисту персональних даних може бути спосіб вирішення даної проблеми є знеособлення персональних даних. цього систему поділяють на взаємодіючі ділянки підсистеми.

Цей підхід дозволяє зменшити вимоги до рівня захисту даних, що, в свою чергу, призводить до зниження витрат на забезпечення їх інформаційної безпеки.

Знеособлення персональних даних зазвичай означає застосування алгоритмів, які унеможливлюють визначення приналежності даних конкретному власнику.

На практиці найпоширенішими способами знеособлення персональних даних є [108–110]:

- зменшення обсягу відомостей, які підлягають автоматизованій обробці, що дозволяє отримати набір даних, оптимальний для зберігання в інформаційних системах персональних даних;
- заміну частини даних на ідентифікатори, що дозволяє знизити рівень чутливості, оскільки система оперує не з конкретними персональними даними, а з ідентифікаційною інформацією без змістового контексту;
- зменшення деталізації деяких відомостей, що робить персональні дані менш точними. Це може бути досягнуто, зокрема, через групування загальних чи безперервних характеристик;
- заміну числових значень на мінімальні, середні чи максимальні значення, оскільки не завжди є необхідність обробляти конкретні персональні дані кожного суб'єкта;
- обробку груп даних в різних інформаційних системах, для чого систему поділяють на взаємодіючі підсистеми.

Цей метод можна застосовувати для оптимізації набору засобів захисту інформації, що використовуються в кожному сегменті. З одного боку, це призводить до зниження вартості захисту, а з іншого — зменшує надмірність інформації в тих випадках, коли дані розподілені нерівномірно по системі.

Перспективним підходом до вирішення цієї проблеми є перестановка персональних даних між різними суб'єктами. Такий метод має таку перевагу:

персональні дані зберігаються в одній системі, що значно знижує ймовірність успішного контекстного аналізу. [94 –99].

Розроблений метод деперсоналізації побудований на наступних принципах та припущенях:

– розбиття вихідної множини даних на підмножини, що дозволяє скоротити розмірність та спростити його практичну реалізацію;

– використання циклічних перестановок, що реалізує власне перемішування даних.

У якості вхідних даних візьмемо таблицю персональних даних Д ($д_1$, $д_2$, ..., $д_n$), де n - число атрибутів, а M - число рядків таблиці.

Далі розглянемо безліч даних, що відноситься до одного атрибуту – $д_i$ (i=1, 2 ..., n).

Це множина атрибута $д_i$, - A_i, містить M i елементів. Всі елементи кожної множини A_i, пронумеровані від 1 до M, і в таблиці Д ($д_1$, $д_2$, ..., $д_n$) сукупність елементів множин різних атрибутів з однаковими номерами називатимемо записом з відповідним номером. При цьому у вихідній таблиці кожен запис має певний сенс, пов'язаний з конкретним суб'єктом (фізичною особою), тобто містить персональні дані конкретної особи, визначеної у цьому ж записі.

Метод забезпечує перестановку даних кожної множини атрибутів вихідної таблиці покроково. На кожному кроці використовується принцип циклічних перестановок. Для пояснення методу зробимо наступне.

Проведемо розбиття множини A_i, на A_i ($M > A_i > 1$) непересічних підмножин A_{ij}, де число елементів підмножини A_{ij} дорівнює M_{ij} ($M > A_i > 1$), j = 1,2, ... k_i. Усі елементи кожної підмножини A_{ij} вважаємо занумерованими від 1 до M_{ij} , ці номери називатимемо внутрішніми номерами елементів підмножини. Зовнішній номер елемента в підмножині A_{ij}, має внутрішній номер k, позначимо, як m_{ijk} (1<

$m_{ijk}<M$), де m_{ijk} — це порядковий номер елемента на множині A_i, відповідний елементу з внутрішнім номером k.

Розбиття кожної множини має такі властивості [90 – 93]:

– $A_i = \bigcup_{j=1}^{Ki} A_{ij}$ - підмножини розбиття включають всі елементи множини A_i;

– $A_{ij} \neq \varnothing$, $A_{ij} \cap A_{im}$, для усіх j, m=1,2…k_i кожне з підмножин не пусте, а перетин любих двох підмножин пусте;

– $m_{ij1} = m_{i(j-1)}M_{i(j-1)}+1$ для усіх j, =1,2, ... K_i, - для будь-яких двох підмножин A_{ij} і $A_{i(j-1)}$ елемент з першим внутрішнім номером підмножини A_{ij} має на одиницю більший зовнішній номер, ніж зовнішній номер елемента з найбільшим внутрішнім номером підмножини $A_{i(j-1)}$;

– якщо $k_1>k_2$, то $m_{ijK1} > m_{ijK2}$ для усіх i= 1,2, .., n; j=1,2, ... K_i, - впорядкованість зовнішньої та внутрішньої нумерації для всіх множин та підмножин їх розбиття - збігаються;

– $M = \sum_{j-1}^{K_i} M_{ij}$ - сумарне число елементів усіх підмножин A_{ij} дорівнюється загальному числу елементів множини A_i.

Для кожної підмножини A_{ij}, визначимо циклічну перестановку (підстановку) $p_{ij}(r_{ij})$, що задається наступним чином

$$p_{ij}(r_{ij}) = \begin{pmatrix} 1 & 2 & \dots & (M_{ij}-1) & M_{ij} \\ (M_{ij}-r_{ij}+1) & (M_{ij}-r_{ij}+2) & \dots & (M_{ij}-r_{ij}-1) & (M_{ij}-r_{ij}) \end{pmatrix}. \qquad (3.10)$$

Тут елементи першого рядка множени, що стоїть у правій частині рівності, відповідають внутрішнім номерам елементів підмножини A_{ij} до перестановки (у вхідній таблиці), а елементи які знаходяться у другому рядку, відповідають

внутрішнім номерами елементів підмножини A_{ij}, що стоять на місцях із номерами, визначеними у верхньому рядку, після перестановки.

Таким чином, у перестановці (підстановці) $p_{ij}(r_{ij})$, проводиться циклічний зсув всіх елементів підмножини на число $r_{ij}(1<r_{ij}<M_{ij\text{-}1})$. Будемо називати величину r_{ij} параметром перестановок $p_{ij}(r_{ij})$. Цей параметр задається генератором випадкових чисел в інтервалі [1; $M_{ij\ \text{-}1}$]. Тоді усі перестановки для всіх підмножин множини A_i; можливо встановити набором (вектором) параметрів $r_i=(r_{i1},r_{i2},\ldots,r_{iKi})$. Вектор параметрів перестановок r_i; задає перший рівень алгоритму деперсоналізації, тобто перестановки першого рівня.

Розглянемо безліч $a_i=(a_{i1}, a_{i2},\ldots,a_{iKi})$, що складається з K_i елементів. Елемент a_i відповідає підмножині A_{ij}, де j=1,2, 3,...,K_i. Для цієї множини визначимо циклічну перестановку $p_{0j}(r_{0j})$

$$p_{0j}(r_{0j})=\begin{pmatrix} 1 & 2 & \ldots & (K_i-1) & K_i \\ (K_i-r_{0i}+1) & (K_i-r_{0i}+2) & \ldots & (K_i-r_{0i}-1) & (K_i-r_{0i}) \end{pmatrix}. \qquad (3.11)$$

Де елементи верхнього рядка множини перестановки відповідають вхідним номерам елементів множені a_i (підмножин A_{ij}), а елементи нижнього рядка матриці відповідають номерам елементів a_i множини, що стоять на місцях з номерами, визначеними у верхньому рядку, після перестановки.

Таким чином, у перестановці $p_{0j}(r_{0j})$ проводиться циклічний зсув елементів множини a_i (підмножин A_{ij}) на число $r_{0j}(1< r_{0j} < K_{i\ \text{-}1})$ - параметр перестановки. Цей параметр r_{0j} задається генератором випадкових чисел в інтервалі [1; $K_{i\ \text{-}1}$]. Цю перестановку називатимемо перестановкою другого рівня.

В результаті послідовного проведення перестановок першого та другого рівнів відбувається перемішування елементів множини A_i так, що змінюється нумерування цих елементів стосовно вхідної нумерації.

Визначимо нумерацію елементів множини A_i після проведення усіх перестановок. З урахуванням правил перемноження перестановок маємо наступну результуючу перестановку

$$p_i(r_{0i},r_i)=\begin{pmatrix} [1...M_{i(Ki-r01+1)}] & [(M_{i(Ki-r01+1)}+1)...(M_{i(Ki-r01+1)}+M_{i(Ki-r01+2)})]... \\ [m_{i(Ki-r01+1)}...m_{i(Ki-r01+1)}M_{i(Ki-r01+1)}] & [m_{i(Ki-r01+2)}...m_{i(Ki-r01+2)}M_{i(Ki-r01+2)}] \quad ... \\ ... \quad [M-M_{i(Ki-r01+1)}...M] & \\ ... \quad [m_{i(Ki-r0i)}...m_{i(Ki-r0i+2)}M_{i(Ki-r0i)}] & \end{pmatrix}$$

Тут верхній рядок множени містить порядкові номери елементів множини атрибута *I* відповідно до їх розміщення в стовпчику після перестановок, а нижній рядок - зовнішні номери елементів множини цього атрибуту, що відповідають їх розміщенню у вхідній таблиці даних.

Розглянутий метод деперсоналізації є перспективним для рішення задач із забезпечення захисту персональних даних саме у оброблюваних системах персональних даних.

Найбільша ефективність при застосуванні даного методу проявляється у разі, коли в ІС міститься велика кількість персональних даних суб'єктів, що забезпечує найбільший захист інформаційної системи.

Основним недоліком зазначених способів і те, що вони не гарантують відсутність можливості отримання персональної інформації у вигляді контекстного аналізу відкритої інформації, зокрема одержуваної із суміжних систем.

Виходячи з вищевикладеного потрібно розробити метод який був би позбавленій цих недоліків.

Пропонується розроблення методу, який буде враховувати додаткові специфічні параметрі функціонування мереж, що надає можливість позбавитися недоліків базового методу.

Першим кроком у розробці методу будемо вважати додаткове урахування параметру комплексної довіри. Причому саме врахування комплексної довіри може покращити захист персональної інформації. Додавання у метод деперсоналізації параметра комплексної довіри, додатково надає можливість покращити захист персональної інформації. Подальший крок у розробці методу деперсоналізації зображено на рис. 3.3, у якості алгоритму. На рис. 3.3. представлено алгоритм подальшого розвитку методу деперсоналізації.

Як видно з наведеного алгоритму у якості додаткового параметру враховується параметр комплексної довіри. Додатковою особливістю запропонованого алгоритму є те, що у якості головного критерія захищеності застосовується коефіцієнт захищеності системи.

Якщо при зовнішньому впливі та початкових умовах довіри, система є стійкою та не виходить з рівноваги, тоді усі початкові умови зберігаються і система працює стабільно.

Але якщо зовнішній вплив не дозволяє системі захисту впоратися з атакою, тоді треба змінити початкові умови та провести розрахунки з новим початковими умовами щодо атак, до тих пір поки система не зможе знешкодити наслідки атаки.

Рис.3.3 Алгоритм деперсоналізації з урахуванням параметру комплексної довіри

Таким чином першим блоком запропонованого методу є врахування комплексної системи довіри. Саме зміна параметрів комплексної довіри дозволить системі впоратися з зовнішнім впливом.

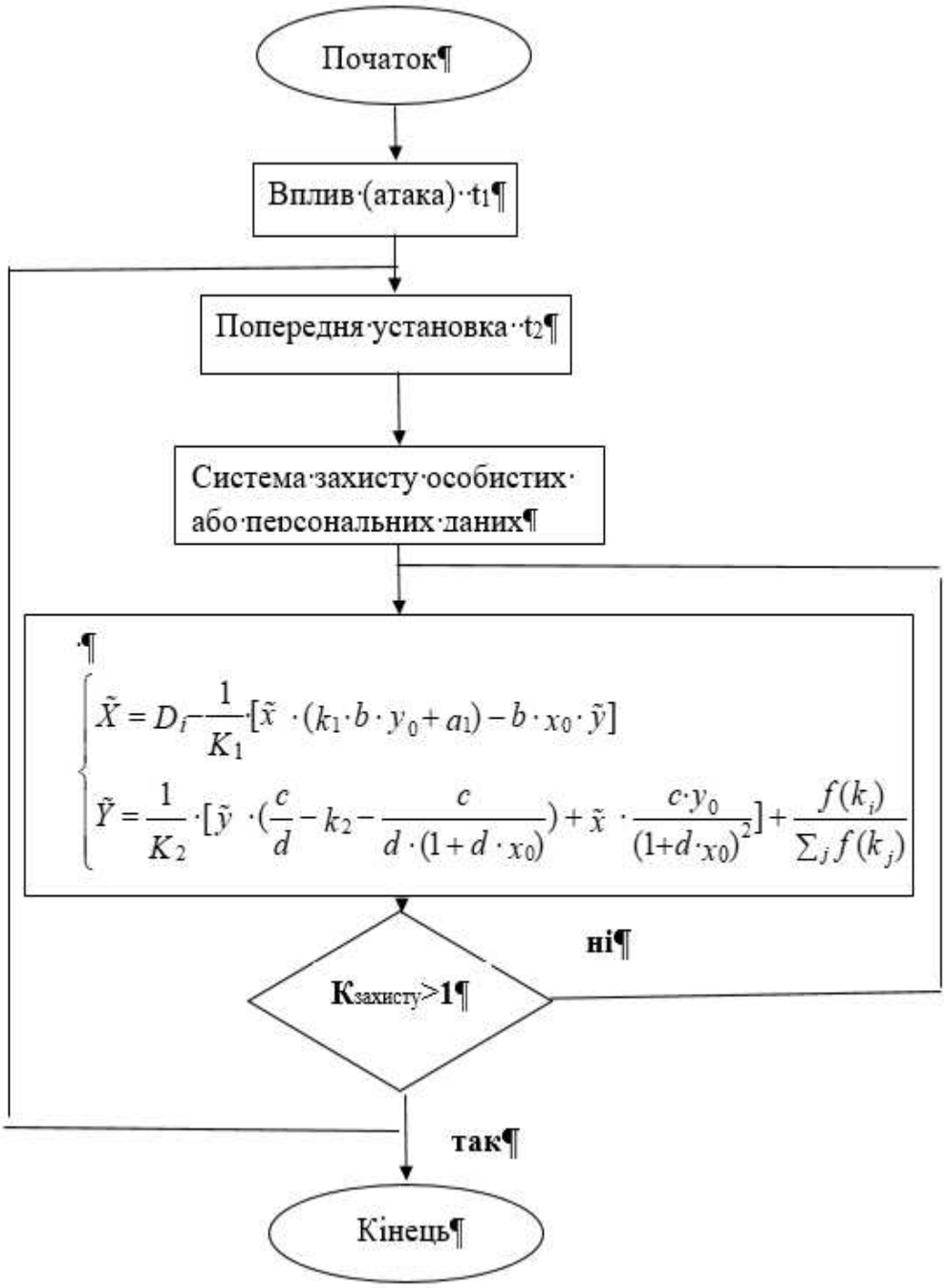

Рис. 3.4 Алгоритм деперсоналізації з урахуванням параметру комплексної довіри та розширення мереж

На рис. 3.4. представлено подальший розвиток алгоритму деперсоналізації з урахуванням параметру комплексної довіри та розширення соціальних мереж.

Вводимо параметр розширення соціальних мереж, який отримано при розробці математичної моделі системи захисту персональних даних.

Застосовуючи розроблену математичну модель отримуємо уточнені параметри системи, які додатково враховуються у початкових умовах алгоритму. Якщо система не впорається із зовнішнім впливом тоді параметри математичної моделі перерозраховуються і тоді вже нові початкові умови долучаються до алгоритму. Так робиться до тих пір поки не буде отримано стійку систему захисту персональних даних.

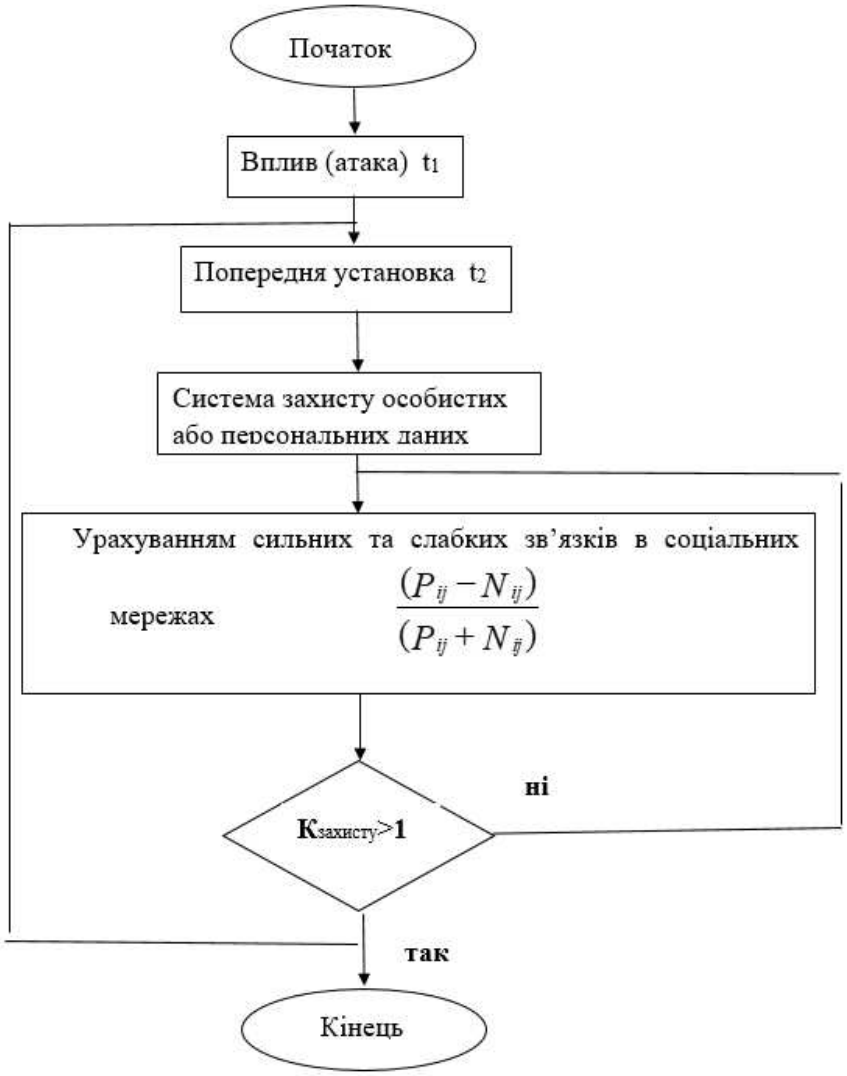

Рис. 3.5 Алгоритм деперсоналізації з урахуванням параметру комплексної довіри, розширення соціальних мереж та з урахуванням сильних та слабких зв'язків у мережах

На рис. 3.5 показано застосування третього кроку алгоритму деперсоналізації з урахуванням параметру комплексної довіри, а саме урахуванням сильних та слабких зв'язків в соціальних мережах. Тобто врахування сильних та слабких зв'язків це третій додатковий параметр покращення алгоритму системи захисту персональних даних.

Проводячи узагальнення подальшого розвитку методу системи захисту персональних даних можна відмітити, що додатково, практично відбуваються три етапи оптимізації параметрів системи захисту персональних даних. Оптимізація проходить по одному параметру, тобто однокритеріальна оптимізація. Але це відбувається на кожному з етапів. Загалом отримуємо три незалежних етапи однокрітеріальної оптимізації. Це, в свою чергу, дозволяє досягти оптимальних параметрів системи захисту вже на початковому етапі за значно менший час. Тому, що завдання однокрітеріальної оптимізації вирішуються дуже швидко та має чітке рішення, яке легко імплементувати у математичну модель для подальшого використання.

Висновки до 3 розділу

Розкрито сутність та запропоновано метод захисту персональних даних з урахуванням специфіки функціонування мереж, що полягає у наступному:

1.Розроблено метод захисту персональної інформації з урахуванням специфіки соціальних мереж, а саме метод деперсоналізації для рішення задач із забезпечення інформаційної безпеки персональних даних у оброблюваних системах персональних даних. Цей метод надає такі переваги: він забезпечує захист персональних даних від несанкціонованого доступу, включаючи запобігання порушенню цілісності інформації під час її витоку через технічні канали; гарантує доступність і забезпечує надійний доступ до персональних даних при легітимному запиті; персональні дані зберігаються в одній таблиці;

отримання персональних даних через контекстний аналіз або перебір є трудомістким і часто практично неможливим; параметри перестановки задаються генератором випадкових чисел, що підвищує стійкість алгоритму до злому.

2. Проведено оптимізацію системи забезпечення захисту персональної інформації у соціальній мережі. Оптимізація здійснена за рахунок послідовного проведення трьох етапів. Кожний етап це однокритеріальна оптимізація по одному параметру. Це дозволяє досягнути оптимальних параметрів системи захисту вже на початковому етапі за значно менший час. Тому, що завдання однокрітеріальной оптимізації вирішуються дуже швидко та має чітке рішення яке легко імплементувати у математичну модель для подальшого використання.

3. Розроблено допоміжний метод захисту персональної інформації з врахуванням розповсюдження таргетованої інформації у соціальних мережах.

Допоміжний метод захисту персональної інформації набув свій розвіток за рахунок досліджування поведінки користувачів у різних ситуаціях. Особливістю цього методу є об’єднання методів соціальної інженерії та алгоритмів оптимізації. А саме за допомогою методів соціальної інженерії враховуються поведінки користувачів у різних ситуаціях, з’ясовується на яку соціальну аудиторію найбільше впливає розповсюдження небажаної інформації. Це удосконалення цілком відповідає реальній ситуації обміну інформацією у соціальних мережах, що підтверджує адекватність розробленого алгоритму.

4. Розроблено універсальний метод захисту персональних даних з урахуванням специфіки соціальних мереж. Цей підхід враховує визначення шкідливих впливів на параметри захисту інформації в мережах і, на відміну від існуючих методів, застосовує систему диференціальних рівнянь, компоненти яких включають комплексні параметри атак. Урахування особливостей функціонування мережі є додатковою перевагою розроблених математичних

моделей безпеки інформації в соціальних мережах. Оцінка впливу кожного окремого параметра мережі на систему захисту, а також комплексного впливу всіх параметрів, дозволяє прогнозувати та розраховувати параметри захисту мережі, що має важливе значення при створенні нових соціальних мереж і модернізації існуючих. Додатковою перевагою цього методу є те, що вперше оцінка стійкості системи захисту здійснюється шляхом побудови фазових портретів системи та ретельного аналізу перехідних процесів. При цьому остаточне розв'язання системи диференціальних рівнянь не є необхідним.

РОЗДІЛ 4
ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ НАУКОВИХ РЕЗУЛЬТАТІВ

4.1. Результати математичного моделювання з метою підтвердження достовірності методу оцінки стійкості системи захисту персональних даних

Для розгляду стійкості моделі захисту персональних даних скористуємось розробленим методом оцінки стійкості системи захисту інформації. А саме методом фазових діаграм (фазовими портретами). Перевага методу полягає у тому, що фазові портрети будуються за рівняннями, які вирішувати не обов'язково. Сама поведінка фазових діаграм дає багато інформації про поведінку системи. А у нашому випадку дає можливість визначати стійкість системи захисту інформації.

Диференціальні рівняння математичної моделі описують поведінку динамічної системи та залежать від декількох параметрів, зміна яких буде призводити до зміни фазового портрету. Тому при математичному моделюванні в якості змінних будуть коефіцієнти диференціальних рівнянь які описують специфіку функціонування інформаційних мереж, а саме: параметр запізнення реагування на атаку, параметр комплексної довіри та параметр розширення інформаційної мережі.

При моделювання процесів оцінки стійкості системи була зроблена орієнтація на значення коефіцієнтів реалізації загроз, які у документах NIST зазвичай визначається в контексті оцінки ризиків у сфері інформаційної безпеки. Найбільш відповідним джерелом для цього є спеціальні публікації NIST, такі як NIST SP 800-30 і NIST SP 800-37, які охоплюють методології управління ризиками.

Так у NIST SP 800-30 оцінка ймовірності зазвичай розбивається на три рівні:

1. **Висока ймовірність** (High): загроза дуже ймовірно відбудеться через існуючі уразливості та недостатні механізми захисту.
2. **Середня ймовірність** (Moderate): загроза може відбутися за певних умов, але реалізація не є невідворотною.
3. **Низька ймовірність** (Low): ймовірність того, що загроза реалізується, є низькою через наявні заходи захисту або низьку експозицію.

У нашому випадку створена адаптація п'ятирівневої шкали на основі рекомендацій NIST, тоб то можна створити кастомізоване рішення для системи.

Запропонована п'ятирівнева шкала представлена у таблиці 4.1.

Таблиця 4.1

Запропонована оцінка ймовірності- п'ятирівнева шкала

№п.п	Назва загрози	Числове значення
1	Критична (Critical) — загроза практично гарантована через відсутність або дуже слабкі захисні заходи.	5
2	Висока (High) — дуже ймовірно, що загроза реалізується, оскільки уразливість добре відома та легко експлуатується.	4
3	Середня (Moderate) — ймовірність реалізації загрози існує, але з деякими обмеженнями (наприклад, атака складна або потребує специфічних умов).	3
4	Низька (Low) — малоймовірно, що загроза реалізується через наявність надійних механізмів захисту або низький інтерес атакуючих.	2
5	Занизька (Very Low) — дуже мала ймовірність того, що загроза відбудеться, через наявні сильні механізми захисту або незначну привабливість активів для атак.	1

Така шкала дає більш детальні оцінки ризиків, що наддасть більше контексту для прийняття рішень щодо стійкості системи захисту інформації.

Таким чином обираючи різні загрози, а у нашому випадку коефіцієнти у диференціальних рівняннях, можна визначати поведінку системи захисту та

оцінювати її стійкість. При моделюванні обирались різні коефіцієнти від занизьких до критичних. Що дозволило оцінити стійкість системи захисту на всьому діапазоні загроз від низької до критичної.

Побудуємо фазові портрети системи захисту персональних даних згідно диференціальних рівнянь розробленої математичної моделі вираз (2.26) для системи захисту персональних даних, які складаються з фазових траєкторій, при різних значеннях постійних коефіцієнтів K_1, K_2, k_1, k_2, b, c, $a1$, d, виразу (2.26). За фазовими портретами визначимо стійкість системи. Рисунок 4.1 побудовано із даних наведених у таблиці 4.2.

Таблиця 4.2.

K_1	K_2	k_1	k_2	b	c	a_1	d
1	**1**	**1**	**2**	**1**	**5**	**3**	**2**

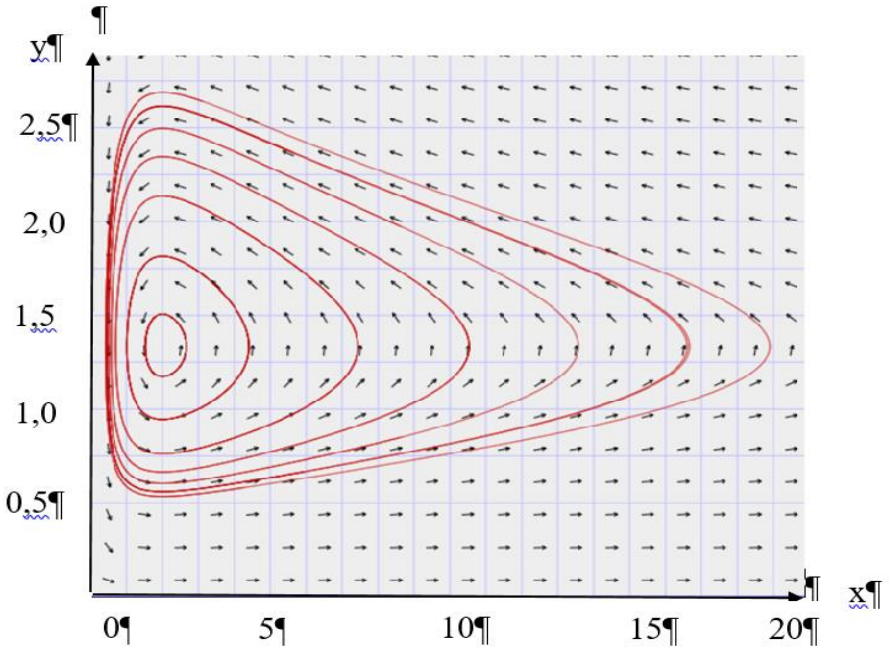

Рис.4.1. Фазовий портрет моделі системи захисту інформації з запізненням реагування на атаку, для параметрів наведених у табл.4.1

Рис. 4.2 для даних наведених у таблиці 4.3

Таблиця 4.3

K_1	K_2	k_1	k_2	b	c	a_1	d
1	**1**	**1**	**1**	**3.5**	**2.5**	**3**	**1.5**

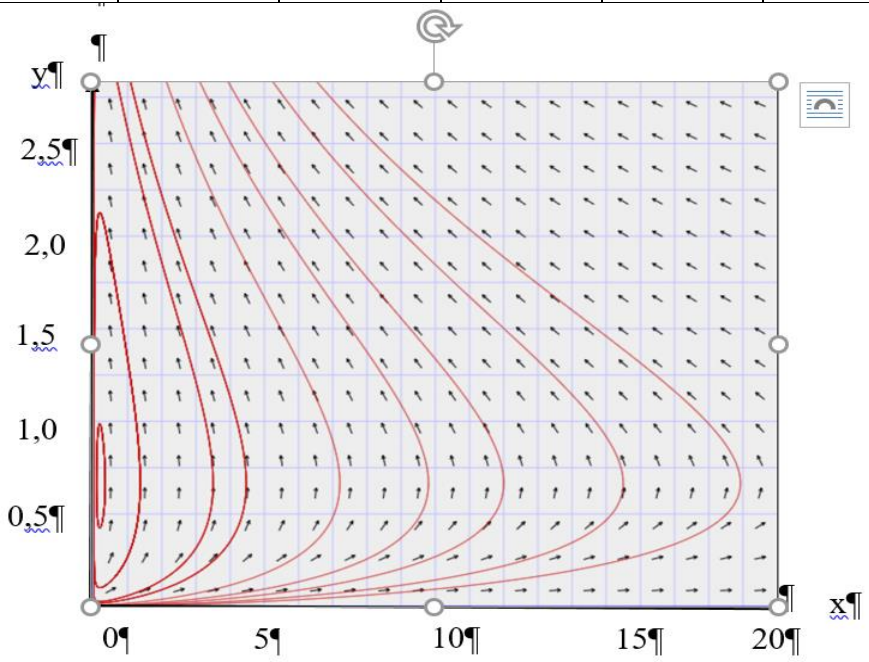

Рис.4.2. Фазовий портрет моделі системи захисту інформації з запізненням реагування на атаку, для параметрів наведених у табл.4.3

Аналіз фазових портретів системи диференціальних рівнянь із запізненням, дозволяє зробити висновок, що за теоремами Ляпунова, система стійка. Варто зазначити, що поведінку динамічної системи зручно аналізувати використовуючи методи якісної теорії диференціальних рівнянь, зокрема так званий метод фазової площини.

Взагалі кажучи, опис руху системи у вигляді залежності певної узагальненої координати від часу не є єдиним. Стан системи в будь-який момент часу визначається двома параметрами: координати та швидкості. Виходячи з цього стан системи може бути представлено у плоскій декартовій системі координат відповідною точкою. Таку точку називають відображаючою точкою, а площину – фазовою площиною [7].

Під час руху системи величини змінюються, а отже, відображаюча точка буде змінювати своє положення на фазовій площині. Геометричне місце відображаючих точок для заданого руху називається фазовою траєкторією. Сукупність усіх можливих фазових траєкторій системи називають її фазовим портретом [3 – 11].

Фазова площина ілюструю повне розмаїття можливих станів системи, й описує картину її динаміки.

Проведемо моделювання з урахуванням параметра комплексної довіри.

Проведені розрахунки довели, що такий параметр як комплексна довіра буде впливати не тільки на параметри системи захисту, а ще й на нападника.

Можливо розглядати декілька варіантів втрати довіри. Зосередимось на двох крайніх випадках, а саме повну втрату довіри тоді $D_i \le 0$, та повну довіру. Після проведення моделювання, це дозволить з'ясувати поведінку системи на граничних режимах.

Удосконалена математична модель системи захисту інформації з урахуванням параметру комплексної довіри буде описуватися наступним виразом

$$\begin{cases} \tilde{X} = D_i - \dfrac{1}{K_1} \cdot [\tilde{x} \cdot (k_1 \cdot b \cdot y_0 + a_1) - b \cdot x_0 \cdot \tilde{y}] \\ \tilde{Y} = \dfrac{1}{K_2} \cdot [\tilde{y} \cdot (\dfrac{c}{d} - k_2 - \dfrac{c}{d \cdot (1 + d \cdot x_0)}) + \tilde{x} \cdot \dfrac{c \cdot y_0}{(1 + d \cdot x_0)^2}] \end{cases}. \quad (4.1)$$

Для побудови фазових портретів системи захисту у залежності від параметру впливу довіри до персональної інформації, скористуємось даними таблиці 4.1.

Моделювання будемо проводити при роботі системи захисту інформації з позитивним та негативним показниками довіри.

Для аналізу поведінки моделі, а саме аналізу стійкості достатньо обрати діапазон зміни довіри від -1 до 1. Тобто від використання системою захисту недостовірної інформації до використання інформації яка надійшла від довіреного джерела.

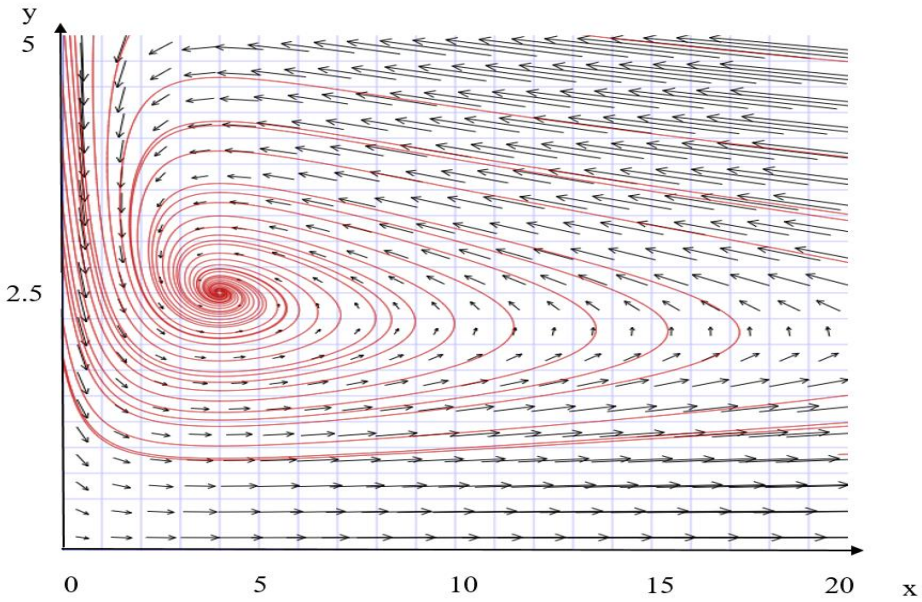

Рис. 4.3. Фазовий портрет моделі системи захисту інформації з запізненням реагування на атаку, для параметрів наведених, для параметрів наведених у табл. 4.1 та максимальної довіри

Аналіз фазового портрета наведеного на рис. 4.3. показав, що система захисту особистої інформації, яка описується розробленою моделлю (вираз 4.1) при використанні довіреної інформації або використанні інформації з довіреного джерела є стійкою. Практично вона не буде мати вплив від зовнішнього шкідливого втручання, що підтверджує адекватність розробленої моделі.

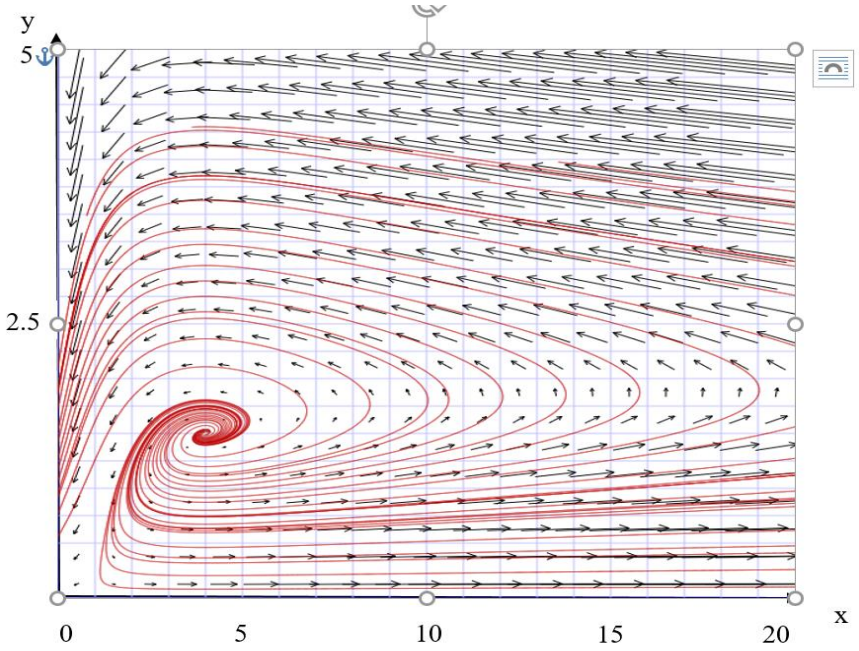

Рис. 4.4. Фазовий портрет моделі системи захисту інформації з запізненням реагування на атаку, для параметрів наведених у табл. 4.2 та відсутності довіри.

Аналіз фазового портрета наведеного на рис. 4.4. показав, що система захисту персональної інформації, яка описується розробленою моделлю, (вираз 4.1), при використанні інформації до якої відсутня довіра, або використанні інформації з підозрілого джерела є не стійкою.

Метод фазової площини полягає в дослідженні характеру вільних рухів нелінійних динамічних систем шляхом побудови їх фазових траєкторій на фазовій площині. Фазовий простір (простір станів), в загальному випадку, - це лінійний *n*-мірний простір, координатами якого є компоненти вектора станів, тобто змінні стану системи, що досліджується. При цьому простір вироджується в площину, яка називається фазовою площиною.

Фазова площина це координатна площина. Вісь абсцис показує саму змінну, для якої досліджується перехідний процес. Вісь ординат - швидкість зміни (перша похідна) цієї змінної.

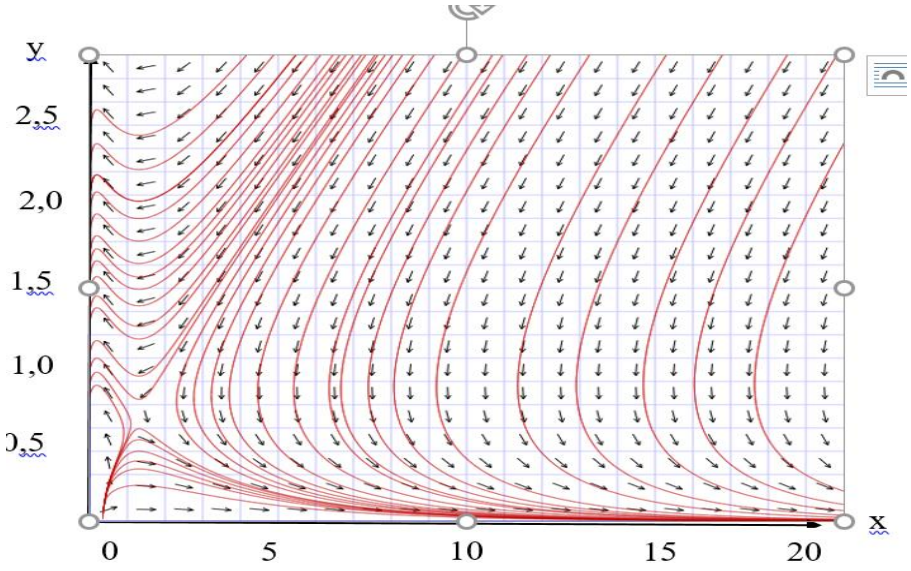

Рис. 4.5. Фазовий портрет системи диференціальних рівнянь з запізненням реагування на атаку, для параметрів наведених у табл. 4.2 з максимальним значенням довіри та зменшенням розширенням розміру соціальної мережи за логарифмічним законом

Графік на рис.4.5 враховує коефіцієнт довіри, він приймає максимальне значення, при параметрі захисту 0,7.

Аналіз графіка фазової площини наведеного на рис. 4.5 доводить, що система захисту особистої інформації при максимальному значені довіри стає умовно стійкім. Тобто при виході розмірів соціальної мережи за граничне значення система вже не у змозі забезпечити захист даних користувача.

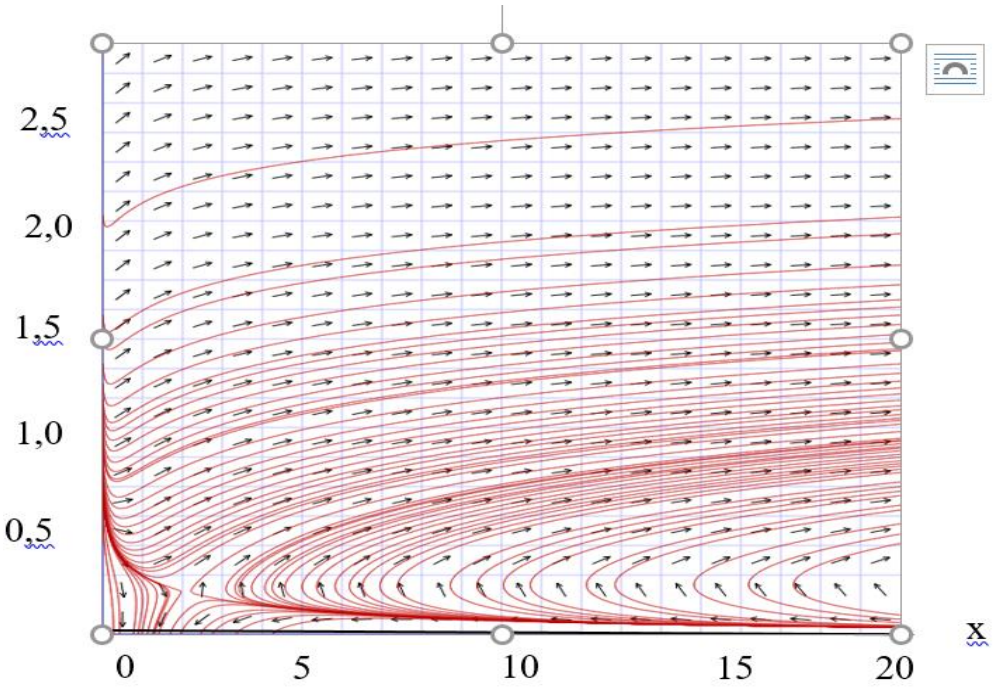

Рис. 4.6. Фазовий портрет системи диференціальних рівнянь з запізненням реагування на атаку, для параметрів наведених у табл. 4.2 з максимальним значенням довіри та розширенням розміру соціальної мережи за логарифмічним законом

Графік на рис.4.6 враховує коефіцієнт довіри, він приймає максимальне значення, при параметрі захисту 0,25.

Зробивши аналіз фазової площини побудованої за розробленою моделлю при максимальних значеннях довіри та розширенням розміру соціальної мережі за логарифмічним законом, можна зробити висновок, що система захисту особистої інформації при максимальному значені довіри та зростанні мережі, стає умовно стійкою. Тобто при виході розмірів соціальної мережи за граничне значення система вже не у змозі забезпечити захист даних користувача.

Зробивши порівняльний аналіз графіків наведених на рис. 4.5. та 4.6. можна зробити висновок, що при зростанні соціальної мережі за логарифмічним законом рівень стійкості системи захисту зменьшується з 0,7 до 0,25. Це відповідає дійсності та підтверджує адекватність розробленої моделі.

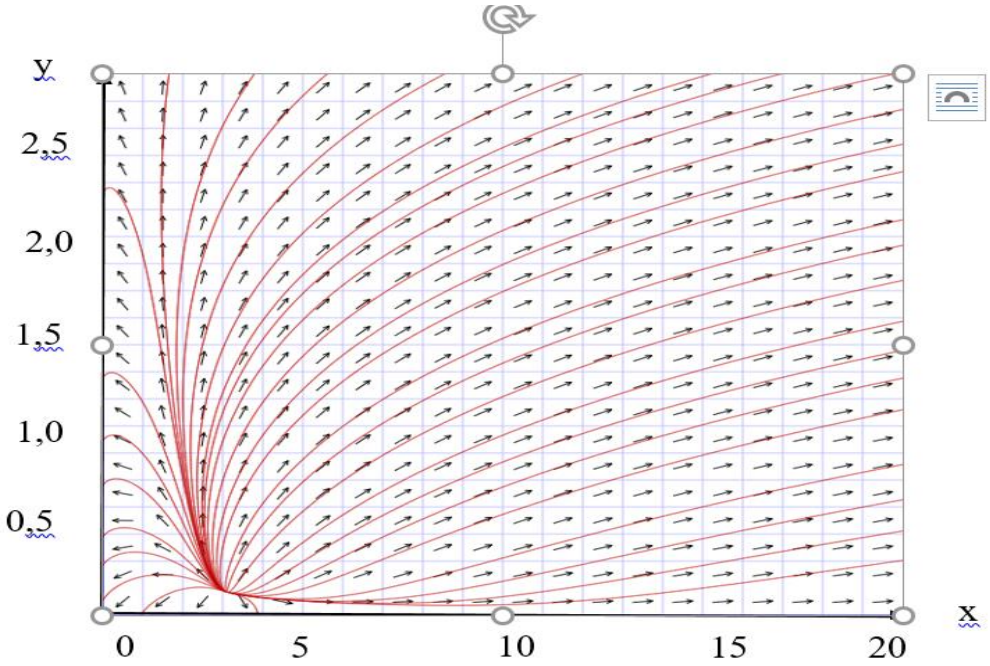

Рис. 4.8. Фазовий портрет системи диференціальних рівнянь з запізненням реагування на атаку, для параметрів наведених у табл. 4.2 з максимальним значенням довіри, розширенням розміру соціальної мережі за логарифмічним законом без впливу на систему

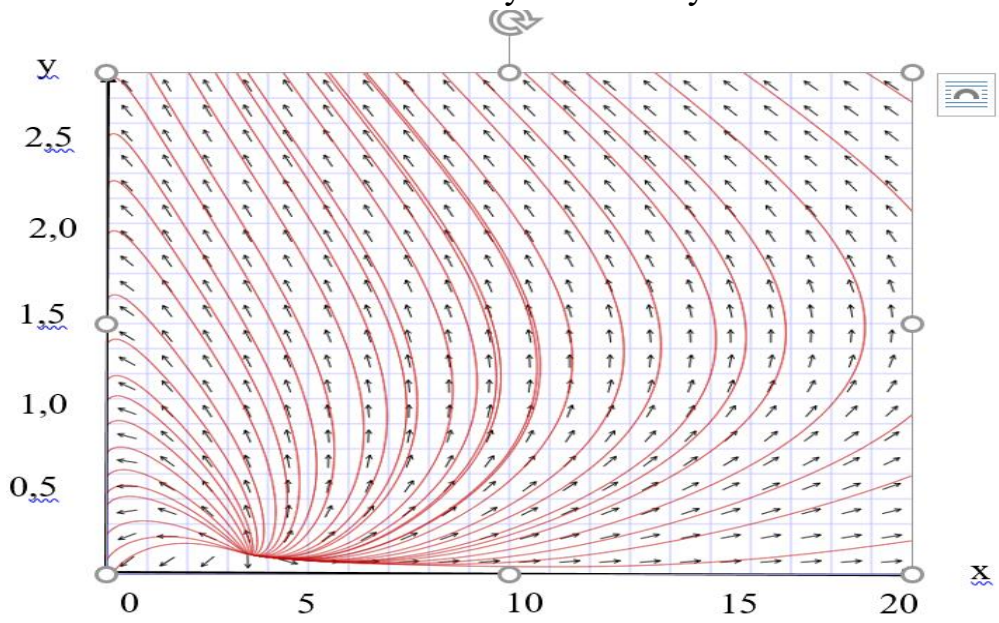

Рис. 4.9. Фазовий портрет системи диференціальних рівнянь з запізненням реагування на атаку, для параметрів наведених у табл. 4.2 з максимальним значенням довіри, розширенням розміру соціальної мережі за логарифмічним законом з максимальним впливом на систему

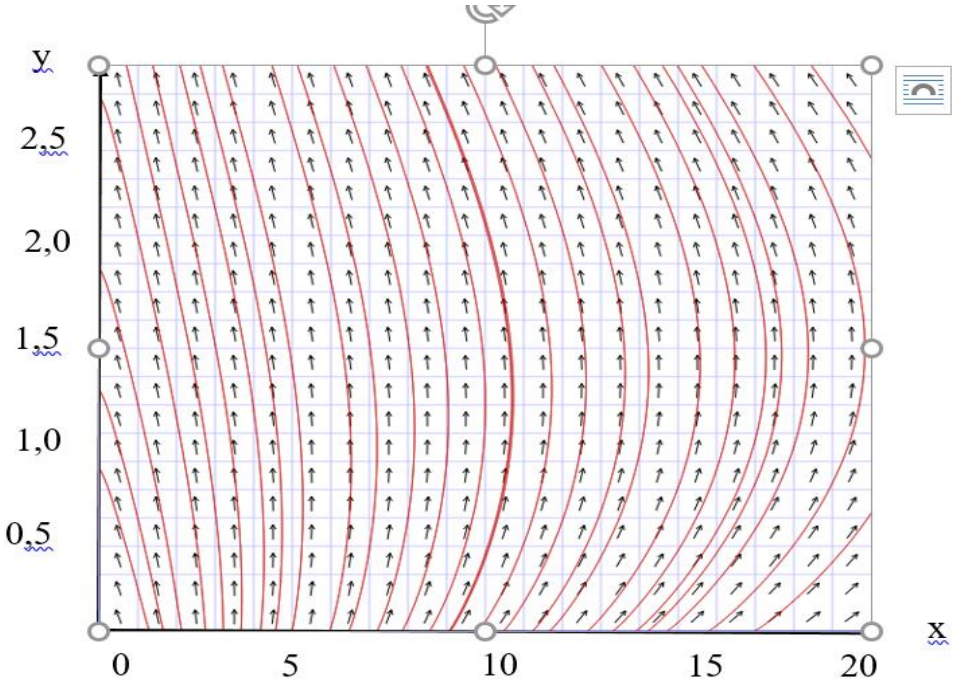

Рис. 4.10. Фазовий портрет системи диференціальних рівнянь із запізненням реагування на атаку, для параметрів наведених у табл. 4.2 з мінімальним значенням довіри, розширенням розміру соціальної мережі за логарифмічним законом з максимальним впливом на систему.

Аналіз графіків фазової площині наведеної на рис. 4.8, 4.9. та 4.10 для моделі, яка описується виразом 4.1 показує, що стійкість системи захисту персональної інформації сильно залежить від параметрів довіри, розширення соціальної мережі та величини зовнішніх впливів.

Використовуючи розроблену модель можна оцінити характер поведінки системи захисту інформації без отримання рішень системи диференційних рівнянь. Це значно скорочує час на отримання результатів реакції системи захисту інформації на: атаки (зовнішні впливи), на розширення загальної соціальної мережі та на ступень комплексної довіри у соціальної мережі.

4.2. Оцінка ефективності методу деперсоналізації для захисту персональних даних

Дослідження соціальних мереж виконується багатьма методами і важливим є математичне моделювання як об'єктів мережі так і процесів, що відбуваються в мережі. Нерідко моделі соціальних мереж представляються математичними співвідношеннями: алгебраїчними структурами, диференціальними, лінійними і нелінійними матричними рівняннями чи нерівностями, іншими засобами. Частіш за все вирішується матричне квадратне рівняння, коли воно виникає в математичній моделі. Розмірність матриць свідомо обрана малою, щоб мати можливість візуально простежити перебіг обчислень. Цей відносно простий приклад показує, наскільки об'ємним і трудомістким процесом є пошук рішення, здавалося б елементарного завдання. З іншого боку, зростання розмірності матриць збереже логіку обчислень, але, при цьому, час зросте багаторазово.

Байєсівські методи були розроблені внаслідок систематичних спроб формулювати та вирішувати проблеми статистичного аналізу. Використання цієї теореми базується на певних співвідношеннях між ймовірностями подій різного характеру та специфікації будь-якої події на необхідному рівні [103]. Більшість статистичних задач, незалежно від методів їх вирішення, мають спільні властивості. Для опису конкретної вибірки розглядаються кілька ймовірнісних моделей, які можуть бути потенційно прийнятними для досліджуваної ситуації. Після отримання даних виникають знання щодо переваг цих моделей, виражені в числовому вигляді. Головною відмінністю байєсівської парадигми від інших статистичних підходів є те, що до отримання даних експерт визначає ступінь своєї довіри до можливих моделей і виражає її у вигляді ймовірностей.

Однією з основних переваг байєсівського підходу є можливість використання початкової (апріорної) інформації щодо параметрів моделі. Така

інформація формується у вигляді апріорної ймовірності або функції густини ймовірності.

Розглянемо випадкову змінну X, яка має розподіл ймовірності, визначений в термінах невідомого параметра θ, який належить певній безлічі можливих значень параметра Θ. Для визначеного значення $X = x$ функція правдоподібності кожного окремого значення θ задається як $P(x|\theta)$. У безперервному випадку апріорні ймовірності для безлічі можливих моделей відповідають, у загальному випадку, розподілу ймовірностей на безлічі можливих значень параметра. Таким чином, апріорні характеристики визначають у вигляді апріорної щільності ймовірності: $P(\theta)$, $\theta \in \Theta$, такий, що

$$\int_{\Theta} P(\theta) d\theta = 1. \tag{4.2}$$

Апріорний розподіл переглядається на основі вибіркових даних $X=x$ для отримання апостеріорної густини ймовірності $P(\theta|x)$, $\theta \in \Theta$. Відповідно до теореми Байєса, яку називають принципом зворотної ймовірності, встановлюється взаємозв'язок між $P(x|\theta)$, $P(\theta|x)$ та $P(\theta)$:

$$P(\theta \mid x) = \frac{P(x \mid \theta) P(\theta)}{P(x)}, \quad \theta \in \Theta, \tag{4.3}$$

де

$$P(x) = \int_{\Theta} P(x \mid \theta) P(\theta)\, d\theta. \tag{4.4}$$

Враховуючи, що в (4.3) знаменник не залежить від θ, досить часто вираз (4.4) представляють у вигляді

$$P(\theta \mid x) \infty P(x \mid \theta) P(\theta), \tag{4.5}$$

де ∞ - означає пропорційність.

Для апостеріорного розподілу має значення тільки правдоподібність. Це досить просто можна показати за допомогою рівності (4.5), якщо його подати таким чином [102]:

$$P(\theta \mid x) \infty P(x \mid \theta) P(\theta) = P(\theta) e^{\ln P(x|\theta)}. \tag{4.6}$$

Якщо припустити, що апріорний розподіл $P(\theta)$ та функція правдоподібності $P(x|\theta)$ невироджені і мають безперервну похідну, і $P(x|\theta)$ має єдиний максимум θ_{max}, який є оцінкою максимальної правдоподібності, то $ln[P(x\ |\theta)]$ має порядок n, а $P(\theta)$ не залежить від обсягу вибірки. Отже, можна інтуїтивно зрозуміти, що при великих значеннях обсягу вибірки багато функцій правдоподібності почнуть переважати над апріорним розподілом.

Частіж за все початкова інформація про значення оцінюваних властивостей невідома, тобто невідомий вид апріорного розповсюдження $P(\theta)$. Інакше кажучи, параметр θ «неінформативний». Для такого випадку запропоновано два правила вибору апріорного розподілу, які охоплюють найпоширеніші випадки [112]. Якщо існує параметр на кінцевому інтервалі або на інтервалі від $-\infty$ до $+\infty$, то його апріорна ймовірність вважається рівномірно розподіленою. Якщо ж можливо обґрунтувати, що параметр набуває значення на інтервалі від 0 до ∞, то ймовірність його логарифму слід вважати рівномірно розподіленою.

Одним з найбільш потужних аналітичних методів дослідження є поділ ("розбиття") даних на групи для порівняння структури підмножин, що вийшли. Ці методи широко застосовуються як у розвідувальному аналізі даних, так і під

час перевірки гіпотез і відомі під різними назвами (класифікація, угруповання, категоризація, розбиття, розшарування та ін.). Продуктивність або гістограми потужності можуть відрізнятися для тимчасових проміжків, коли керування здійснюється різними операторами. Різним експериментальним групам можуть відповідати різні нахили ліній регресії.

Для кількісного опису відмінностей між групами спостережень розроблено численні обчислювальні методи, що ґрунтуються на групуванні даних (наприклад, дисперсійний аналіз). Однак графічні засоби, такі як категоризовані графіки, дають особливі переваги і дозволяють виявити закономірності, які важко піддаються кількісному опису і які дуже складно виявити за допомогою обчислювальних процедур (наприклад, складні взаємозв'язки, винятки або аномалії). У цих випадках графічні методи надають унікальні можливості багатовимірного аналітичного дослідження або "видобування" даних.

Термін "категоризовані графіки" вперше був використаний у програмі STATISTICA компанії StatSoft (крім того, Becker, Cleveland та Clark з Bell Labs називають їх графіками на ґратах). Ці графіки являють собою набори двовимірних, тривимірних, тернарних або *n*-вимірних графіків (таких як гістограми, діаграми розсіювання, лінійні графіки, поверхні, тернарні діаграми розсіювання тощо), графіки розташовуються послідовно в одному графічному вікні, дозволяючи порівнювати структуру даних для кожної із зазначених підгруп.

Існує п'ять основних методів категоризації значень: цілі числа, категорії, межі, коди та складні підгрупи. Треба звернути увагу, що одні й ті самі методи категоризації можна використовувати як для розбиття спостережень за вхідними графіками, так і для категоризації спостережень всередині вхідних графіків (наприклад, на гістограмах або діаграмах розмаху).

Загальний масштаб дозволяє порівнювати діапазони та розподіл значень різних категорій. Однак, якщо ці діапазони сильно різняться (що призводить до дуже великої загальної шкали), дослідження деяких графіків може бути ускладнено. Використання незалежного масштабу може спростити виявлення трендів і певних закономірностей усередині категорій, але водночас ускладнити порівняння діапазонів значень різних підгруп. Виходячи з вищевикладеного для наочного показу переваг запропонованого методу будемо використовувати саме категаризовані графіки.

Але для подальшої оцінка ефективності методу захисту інформації у соціальній мережі проведемо тестування даних на нормальність, це буде етапом первинного аналізу даних, оскільки велика кількість статистичних методів використовує те, що дані розподілені нормально. Якщо вибірка не підпорядковується нормальному закону, тоді припущення про параметричні статистичні тести порушуються і слід використовувати непараметричні методи статистики.

Можна виділити такі етапи перевірки вибіркових значень на нормальність:

– підрахунок основних показників вибірки (вибіркове середнє, медіана, коефіцієнти асиметрії та ексцесу);

– графічний, до цього методу відноситься побудова гістограми та графік квантиль-квантиль або коротко *QQ*;

– статистичні методи, дані методи обчислюють статистику за даними та визначають, яка ймовірність того, що дані отримані з нормального розподілу.

Зробимо припущення, яке полягає у тому, що сума досить великого числа незалежних (або слабо залежних) випадкових величин, у нашому випадку параметрів зовнішніх впливів, буде підпорядковано довільним законам розподілу та наближено підпорядковується нормальному закону.

Для подальший оцінки переваг будемо розраховувати, на те що параметри моделей процесу захисту персональної інформації підпорядковується нормальному закону розподілу.

Нормальний закон розподілу характеризується щільністю ймовірності виду [77]

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp[-\frac{(x - m_x)^2}{2\sigma^2}], \quad (4.7)$$

де: σ – середньоквадратичне відхилення випадкової величини;

m_x – математичне очікування випадкової величини.

Дані припущення неодноразово отримали підтвердження у дослідженнях, наприклад дослідження в якому був розроблений програмний комплекс для визначення закону розподілення атак зловмисників [68].

Для пояснення доцільності цього припущення треба ввести поняття щодо центральної граничної теореми, яку також називають теоремою Ляпунова. Її суть полягає в тому, що якщо випадкова величина є сумою дуже великої кількості взаємно незалежних випадкових величин, вплив кожної з яких на всю суму мізерно малий, то має розподіл, близький до нормального.

Посилаючись на те, що загальні ймовірнісні параметри підпорядковуються нормальному закону розподілу, зробимо графічне представлення проведених розрахунків.

Для цього зробимо припущення: для існуючих методик та розробленої методики середнеквадратичне відхилення однакове та буде складати 0,15.

Тоді згідно нормального закону розподілу побудуємо графіки. Графіки наведені на рис. 4.11

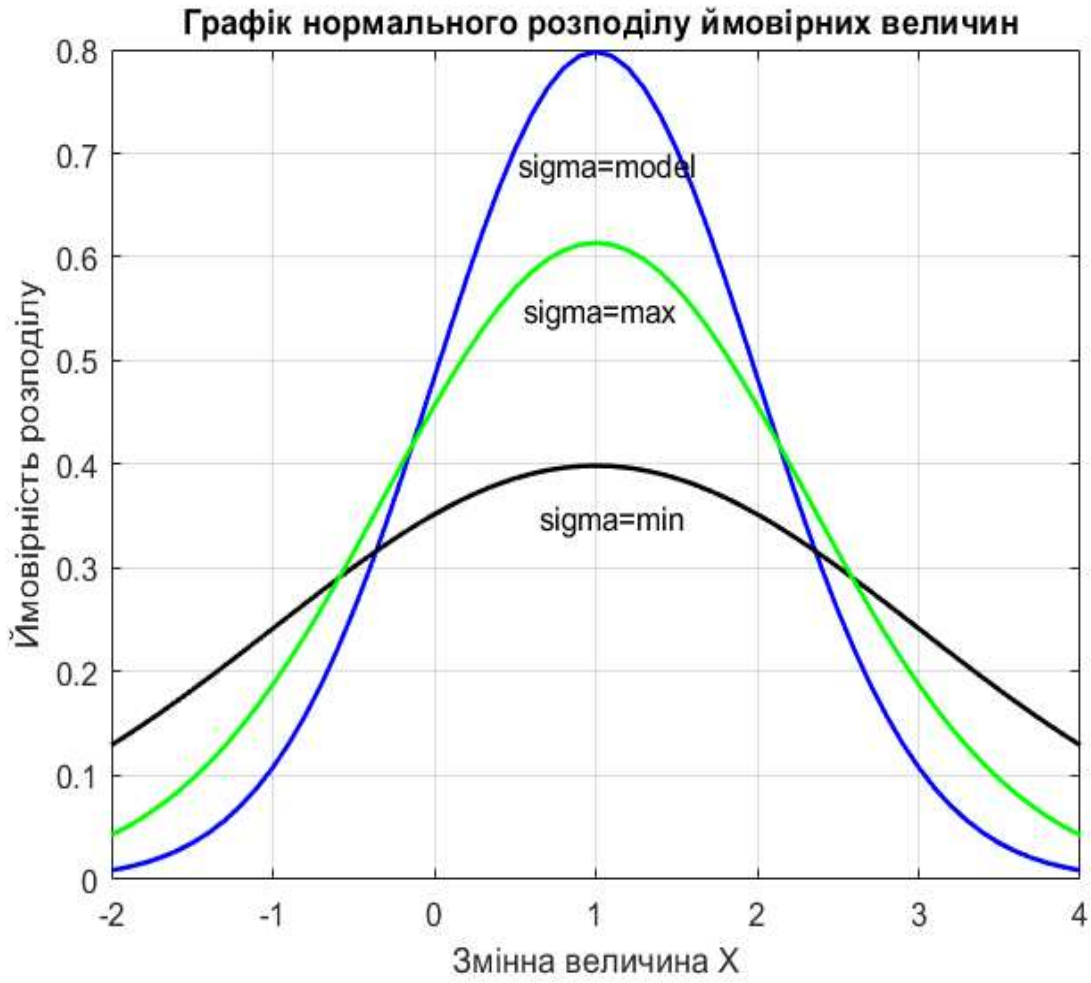

Рис.4.11. Графіки нормального закону розподілу ймовірної величини

Як показує аналіз графіків, при різних значеннях середнеквадратичного відхилення, для існуючих моделей (дані обирались з досліджень наукової літератури) та розробленої моделі, яка склала основу методу захисту персональної інформації, ми отримали перевагу понад 9,5 %. За результатами розрахунків перевага розробленого методу склала 10%, що підтверджує адекватність проведених досліджень, та доводить гарну сходимость результатів моделювання.

Рис. 4.12 показує поведінку системи захисту при зовнішніх впливах.

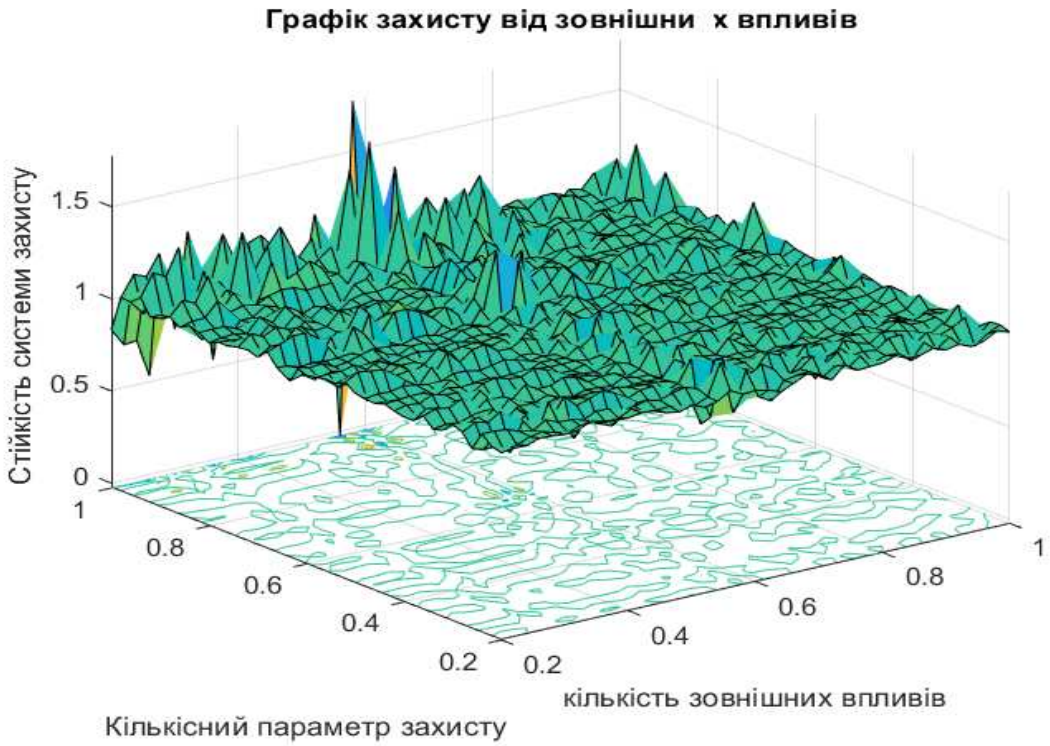

Рис.4.12 Графік результатів моделювання процесу захисту персональних даних при зовнішніх впливах

Як показує аналіз графіка на рис.4.12 система захисту при цих параметрах системи є стійкою. Коливання біля оптимального значення доводять можливість системи реагувати на зовнішні впливи з метою усунення наслідків. Результати моделювання реакції системи захисту персональних даних на зовнішні впливи цілком підтверджують адекватність розроблених наукових положень та відображають фізику процесу.

Числова оцінка системи захищеності персональних даних за розробленим методом.

Надійність сучасних криптографічних алгоритмів ґрунтується на використанні складних математичних алгоритмів з високою обчислювальною стійкість до атак на основі грубої сили та методів криптографічного аналізу.

Однак вони виконують виключно перетворення даних і не включають в себе процедури підготовки інформації. В роботі пропонується додатковий метод підготовки. А саме удосконалений метод попереднього випадкового змішування.

Для оцінки стійкості криптографічних алгоритмів у різних моделях криптосистем пропонується застосовувати швидкий аналіз на основі ентропійного методу, який використовується в пакеті статистичних досліджень випадкових величин NIST STS 822 [37]. Цей метод дозволяє на інтуїтивному рівні порівняти не лише стійкість різних криптографічних алгоритмів та криптосистем, але й ефективність їх програмних реалізацій, при цьому з мінімальними витратами обчислювальних ресурсів, коштів і часу.

При проведенні моделювання оцінки стійкості криптоалгоритмів використовувалися блочно симетричні шифри: 3DES, ГОСТ-28147-2009, Калина-256, AES-256. Для реалізації потокового шифру використовувався генератор псевдовипадкової послідовності криптографично стійкий генератор SecureRandom з криптобібліотеки Java, який позиціонується як придатний для криптографічних застосувань. Для оцінки запропонованого методу використовувався несиметричний криптоалгоритм RSA+ з попереднім випадковим змішуванням.

Моделювання проводилось для тексту довженною 10^8біт, обрано тому що бінарна послідовність, за рекомендаціями NIST вважається достатньою вже з 10^6 біт. Надалі для моделювання скористались готовою програмою яка наведена у [93] та отрималаи результати, які наведені у табл. 4.4

Таблиця 4.4

Результати досліджень стійкості криптоалгоритму експрес-методом

№	Шифр	Ентропія вхідного тексту	Ентропія криптограми. Ймовірність крипто-захисту, *Pc*	Різниця між ентропіями	% ентропії, який додається шифром
1	Криптостійкий генератор SecureRandom з Java	0,5023767	0,7999982	0,2976215	59,242695
2	3DES	0,469276	0,812043	0,342767	73,041664
3	ГОСТ 28147-2009	0,469276	0,811348	0,342767	72,893563
4	Калина-256	0,469276	0,954519	0,485243	103,40247
5	AES-256	0,469276	0,944641	0,475365	101,29753
6	RSA	0,469276	0,954542	0,485266	103,40737
7	RSA+	0,469356	0,999999	0,536439	114,29256

У табл. 4.4 розраховано ентропія вхідного і зашифрованого тексту, різниця, а також відсоток ентропії, що додається до ентропії відкритого тексту самим шифром. Аналіз даних наведених у табл. 4.4 дає можливість оцінити внесок самого шифру в підсумкову ентропію зашифрованого повідомлення. Виходячи з того, що всі вони тестувалися в однакових умовах, можна робити порівняння за відносними показниками.

Таки шифри, як Калина-256 та AES-256 показали, понад 101% ентропії відкритого тексту. Приблизно однакові показники продемонстрували блочно симетричні шифри ГОСТ-28147-2009 – 72,89% та 3DES –73,04%. Для порівняння було проведено моделювання процесу виявлення ентропії криптограми з використанням потокових шифрів на основі криптостійкого генератор

SecureRandom з криптобібліотеки Java. Отримані значення ентропії, набагато менші, ніж у класичних блокових систем шифрування, що не дозволяє говорити про якісне шифруванні за їх допомогою. Запропонований алгоритм RSA+ несиметричної криптографії, за результатами моделювання, забезпечує найвищий досліджений показник понад 114%.

Таким чином, наведені результати моделювання процесу визначення крипостійкості доводять перевагу запропонованого алгоритму RSA+ з попереднім випадковим змішуванням, за показником крипостійкості алгоритму, над іншими алгоритмами шифрування більш ніж на 10%.

Розроблений метод деперсоналізації є перспективним для рішення задач із забезпечення захисту персональних даних саме у оброблюваних системах.

Цей метод має наступні переваги:

- захищає персональні дані від несанкціонованого доступу, включаючи захист від порушень цілісності інформації при її витоку через технічні канали;
- гарантує доступність та забезпечує доступ до персональних даних у разі легітимного запиту;
- персональні дані зберігаються в єдиній таблиці;
- доступ до персональних даних через контекстний аналіз або перебір практично неможливий;
- параметри перестановки генеруються за допомогою випадкових чисел, що підвищує стійкість методу до злому.

Максимальна ефективність цього методу досягається, коли в інформаційних системах зберігається велика кількість персональних даних, що забезпечує найвищий рівень захисту системи.

4.3. Розробка рекомендацій щодо застосування методів захисту персональних даних з урахуванням специфіки соціальних мереж

Для створення безпечної архітектури, пропанується адаптувати технологію Friendsbook. Узагальнена концепція Friendsbook надає концепцію захисту інформації на основі децентралізованої мережі. Тому адаптація цієї технології дозволить створити безпечну архітектуру децентралізованої інформаційної мережі, що саме захищає конфіденційність.

Процес адаптації полягає у наступних кроках:

Огляд

Для забезпечення довірчих відносини з новими віртуальними контактами, технологія Friendsbook обмежує дружбу відносинами які реально існують на сучасний момент. Крім того, перспектива довірчих відносин користувача у Friendsbook завжди обмежується його власною соціальною мережею [70].

На рис. 4.13 зображені взаємодії двох клієнтів. Для яких m – шифровані повідомлення. Перший кліент *u* розміщує свою інформацію у сховище даних. Другій клієнт *v*, також може отримати цю інформацію у будь–який час, використовує при цьому сховище даних. Для приватного зв'язку клієнтів *u* та *v* забезпечують один одного файлообмінником. Перший клієнт *u* посилає свої повідомлення клієнту *v* через обмінник ОБ*v* та отримує інформаційні повідомлення від клієнта *v* через власний файлообмінник ОБ*u*. Загалом кількість файл обмінників та сховищ даних для кожного окремого користувача не обмежені. Але щоб гарантовано отримувати повідомлення або інформацію через свого клієнта, користувач повинен мати тільки одного друга.

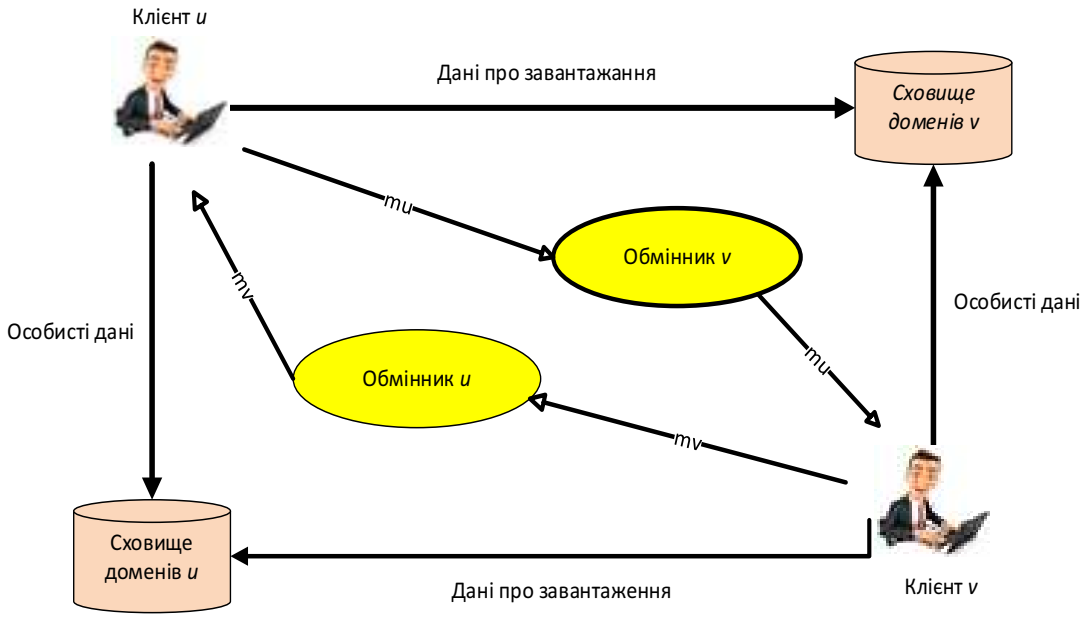

Рис. 4.13 Залежності та взаємодія двох клієнтів, обмінника та доменів сховищ даних [70].

З метою забезпечення власної анонімності, рекомендується використовувати декілька файлообмінників. Також для того, щоб звести до неможливості успішного впливу або атаки, можна використовувати декілька файлообмінників на одного друга. З тих же саме причин рекомендується, також використовувати декілька сховищ даних.

Рекомендована концепція захисту інформації

Для досягнення вимог безпеки інформації та повідомлень, Friendsbook надсилає інформацію та повідомлення, як у тунелі VPN в зашифрованому вигляді. Але на відміну від технології VPN технологія Friendsbook зберігає всі повідомлення та особисту інформацію також у зашифрованому вигляді. Особливістю технології Friendsbook є те, що використовується криптографія, причому двох видів, а саме асиметричне та симетричний шифрування. На першому етапі інформація, яку необхідно передати, або якою треба поділитися, шифрується на основі симетричного шифрування. Тобто для шифрування та

відновлення інформації використовується один і та той же ключ. Однак потім цей самий ключ зашифровується відкритим ключом одержувача інформації. Маємо різновид асиметричного шифрування. Вся інформація та повідомлення зашифровується симетрично-асиметричним засобом.

Раніше так звана «хороша конфіденційность» базувалася на загальній концепції довіри. Автентичність користувача була пов'язана з одноразовим відкритим ключем шифрування, усі довірені відправники використовували один для усіх відкритий ключ. Зрозуміло, що у такому випадку завжди існує великий ризик деанонімізації користувача-передавача та користувача-приймальника.

Для забезпечення максимального захисту конфіденційності пропонується, щоб кожен користувач *u* генерував для кожного з своїх друзів-користувачів $V \in \Gamma(u)$, додатково ще пару ключових слів $K^{-}_{u \to v} K^{+}_{u \to v}$, де $K^{-}_{u \to v}$ буде відноситься до публічного ключа посилання. А кожен друг-користувач додатково генерує, ще пару ключів для спілкування $K^{-}_{u \to v} K^{+}_{u \to v}$, для користувача *u*.

Щоб уникнути деанонімізації, пропонується використовувати три ключа шифрування, але формування довірливих відносин використовуючи три ключа буде пов'язана з підвищеною складністю. Складністю в управлінні ключами шифрування. У цьому випадку, оскільки кожна дружба буде визначатися вже трьома ключами, користувач *u* повинен буде керувати вже 3*n* ключами замість звичайних *n* + 2 ключів для усіх своїх друзів. Тут потрібно вирішувати завдання оптимізації, що більш за доцільно просте керування з ризиком деанонімізації, чи складне керування зі значно меншим ризиком деанонімізації. Для узагальнених рекомендацій, для користувачів які використовують стільниковий зв’язок, як можливість входу у кіберпростір, пропонується обмежиться саме трьома ключами шифрування. Це пов’язано, саме з можливістю стільникової мережи та ПЗ самих гаджетів.

Формат повідомлення

Для стійкого захищеного зв'язку між двома користувачами-друзями використовується Friendsbook-логограма [116]. Логограма складається з ідентифікатора. Логограма, це символьне значення, яке замінює слово. У нашому випадку ідентифікатор логограми складається зі змісту і підпису користувача.

Виходячи із запропонованої структури логограми на рис. 4.14 наведена структура повідомлення за запропонованим алгоритмом.

Ідентифікатор у нашому випадку це хеш–функція відкритого ключа посилання $K^{+}_{u\to v}$. Відповідно ідентифікатор Хеш–значення генерується з використанням відповідної хеш–функції.

Підпис

У загальному випадку підпис використовується для забезпечення захисту інформації, а саме цілісності та автентичності повідомлень користувача v. Це хеш–значення m, закодованого на основі відкритого ключа посилання $K^{-}_{u\to v}$. Структура інформаційного повідомлення

$$H(K_{u\to v}+)\dots K_{u\to v}+(m)\dots K_{u\to v}(H(m))$$

Оскільки тільки повідомлення користувача *u* шифрується на основі відкритого ключа $K^{-}_{u\to v}$ анонімність користувача відправника *v* буде забезпечуватися, тільки коли інформаційне повідомлення передається через захищений канал зв'язку.

Обмін повідомленнями

Обмін інформаційними повідомленнями відбувається за допомогою файлообмінника ОБ*v* або файлообмінника ОБ*u*. За своєю функціональністю файл ообмінник у класичному вигляді зберігає інформаційні повідомлення, поки вони не будуть доставлені користувачу. Причому кожному файлообміннику надається

унікальна адреса. Для підвищення рівня анонімності, користувач повинен надавати кожному зі своїх користувачів друзів різні адреси файлообмінника.

Зберігання інформаційних даних

Для того, щоб захистити особисту інформацію, треба контент зробити доступним тільки для власного кола користувачів друзів.

Схема адресації інформаційного обміну

Для забезпечення доступу до власного профілю та іншого особистого вмісту, кожен користувач друг керує індексом $I_{u \to v}$ для кожного користувача друга v. Ця інформація зберігається у сховищі даних у зашифрованому вигляді, ця інформація шифрується на основі відкритого ключа $K^{+}_{u \to v}$.

Розподілене зберігання особистої інформації

Раніше з’ясовано, що для одного користувача або декількох користувачів друзів можуть бути використані декілька різних файлообмінників, тобто користувачам надана можливість поширювати або вибірково розповсюджувати особисту інформацію за допомогою декількох сховищ інформаційних даних.

Навчання дружбі користувачів

Вимога міцних відносин довіри між користувачами друзями не надає широкої можливості пошуку інших користувачів, які можуть бути у подальшому користувачами - друзями. Можливість надіслати запит на дружбу іншим користувачам мережі дуже обмежений. Це відноситься до недоліків запропонованих рекомендацій забезпечення захисту інформації, але додає певних переваг для безпеки особистої або персональної інформації.

Обмін інформаційними повідомленнями

Безпечний канал зв'язку між двома користувачами друзями надає право власності та використання інформації. Слід відмітити, що цілісність повідомлень та автентичності користувача забезпечується використанням пари ключів, що генерують два користувача при спілкуванні. Це додатково забезпечує авторизований доступ до файлообмінника для обміну інформацією.

Таким чином, безпечний канал зв'язку буде існувати тільки тоді, коли двоє користувачів мережі є друзями. Треба відмітити, що для заведення нових

користувачів - друзів, буде потрібно обмінюватися через небезпечний канал зв’язку. Але ці канали є роздільними та не перетинаються між собою. Закритий канал створюється тільки при встановлені дружніх відносин.

Протокол дружби користувачів

Для укладення дружби існує дружній протокол. Надалі обмін інформацією завжди стосується тільки обміну інформаційними повідомленнями. Слід відмітити, що протокол не визначає спосіб, або канал обміну інформацією між двома користувачами. Процес дружби наведено на рис. 4.15.

Протокол взаємодії. Запропоновані рекомендації виключають можливості перегляду інформації інших користувачів. Збільшення можливості при налагодженні процесу дружби, надається незалежний протокол зв'язку. У соціальних мережах нові дружні відносини, частіше за все, з’являються у результаті знайомства з друзями друзів. Підхід ґрунтується на припущенні, що два друга *v* та w користувача *u*, можливо, погодяться на дружні відносини, коли *u* наддасть позитивну рекомендацію *w* та *v*. Імовірність прийняття позитивної рекомендації залежить від ступеня довіри між *u* та *v* або між *u* та *w*.

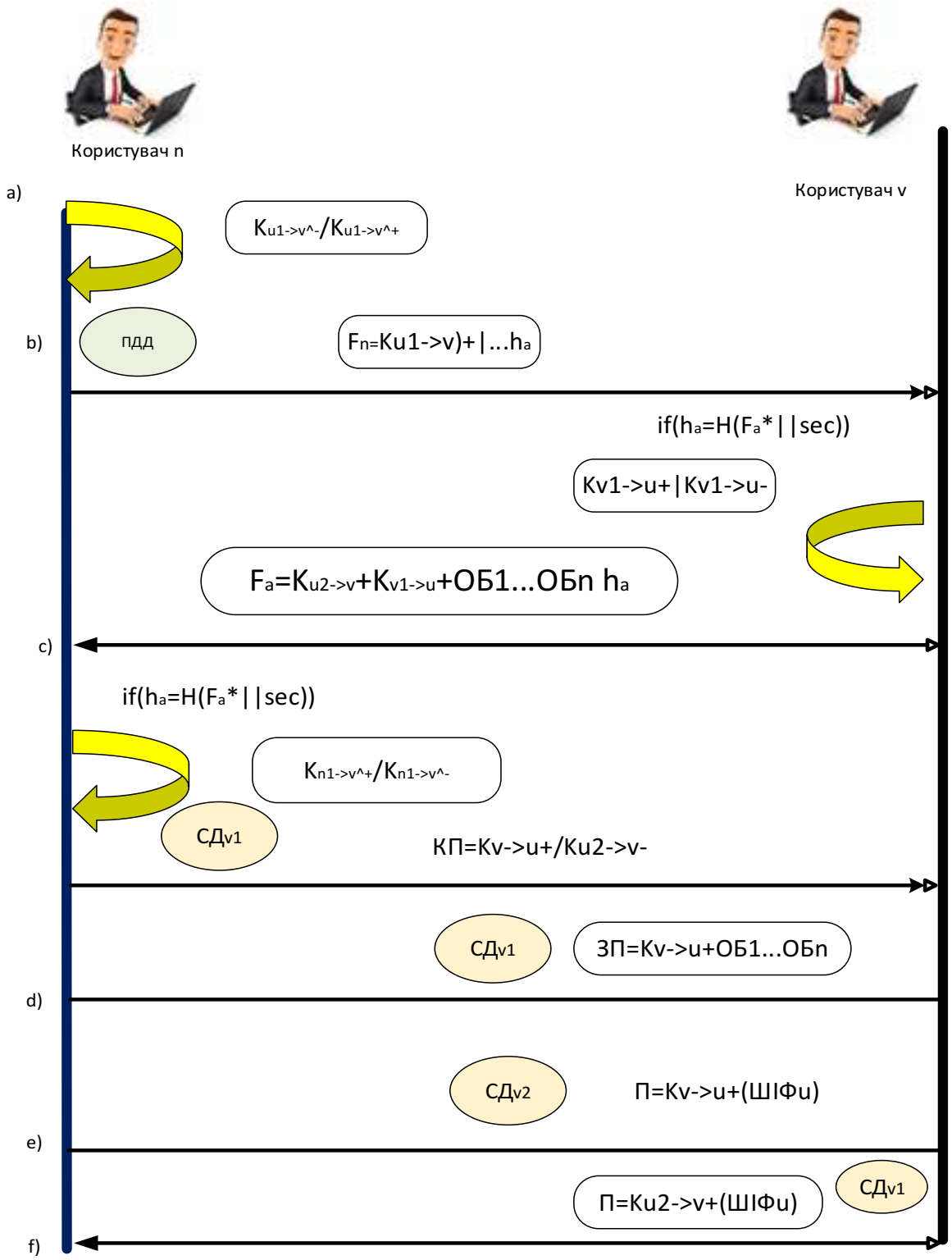

Рис. 4.15 Формування дружби користувачів з використанням протоколу довіри- дружби.

Таким чином розроблено та запропоновано рекомендації створення безпечної архітектури децентралізованої соціальної мережі для стільникового зв'язку, що захищає доступність, конфіденційність та цілісність особистої інформації та інформаційних повідомлень загалом.

Ці рекомендації особливо актуальні на сучасний момент у зв'язку з практично необмеженим використанням стільникового зв'язку користувачами соціальних мереж. Але слід відмітити, що ці рекомендації цілком можуть бути адаптовані для інших каналів зв'язку між користувачами.

4.4. Розробка рекомендацій щодо застосування методів захисту персональних даних з урахуванням специфіки функціонування інформаційних мереж

Рекомендації щодо захисту інформації на інтернет сайтах та веб додатках

Мета злому та зараження сайту вірусами - завжди отримання матеріальної вигоди або через маніпуляції з даними або через використання ресурсів хостингу. Щоб досягти мети збереження персональної інформації користувачів або конфіденційної інформації від несанкціонованого доступу, та захистити сам сайт від несанкціонованого доступу сторонніми особами, необхідно надійно захистити свій інформаційний інтернет ресурс.

Для захисту власного інформаційного інтернет ресурсу, можливо виділити декілька рекомендацій:

- забезпечити захист свого ресурсу від DDoS-атак;
- рекомендовано підключити SSL-сертифікат;
- обрати та використовувати надійний хостинг;
- використовувати тільки безпечні «сторонні модулі» плагіни/бібліотеки/фреймворки/CMS;

– застосовувати сучасні техніки захисту від SQL-ін'єкцій та XSS-атак;

– забезпечити ведення документування, а саме ведення журналу інтернет ресурсу;

– проводити регулярне резервне копіювання усіх даних своїх інтенет ресурсів;

– використовувати складні паролі;

– у разі наявності адміністративної панелі треба обов’язково забезпечити контроль конфіденційності та автентифікації.

Треба розуміти, що це тільки основні методи та засоби захисту інформації інтернет ресурсів. Але нажаль не повний список рекомендацій, бо методи несанкціонованого доступу зловмисників постійно удосконалюються. Основна рекомендація це потрібно обирати надійний сервер або віртуальний хостінг та обов’язково підключення SSL-сертифіката. Додаткові рекомендації, які пропонуються:

*Зберігати лише потрібні для бізнесу дані клієнтів***.**

Зловмисники не можуть вкрасти те, чого не маєте. Тому зберігайте лише ті особисті дані клієнта, які справді необхідні для ведення бізнесу. Коли необхідно обробити дані банківських карток, використовуйте зашифрований канал для їх обробки, щоб унеможливити зчитування даних картки серверами. Це може зайняти більше часу при проведенні платежу клієнтами, але убезпечать від ризиків, пов'язаних із збереженням даних банківських карток клієнтів.

Безпека облікових даних

Необхідно зберігати поза доступом для інших логін та пароль від хостингу. Адже отримавши доступ до управління сайтом, хакер може зробити все, що завгодно – від зміни вмісту сторінок до поширення вірусів та переадресації на інший сайт.

Це стосується і даних для входу в панель адміністрування. Маючи доступ до неї, зловмисник також може змінювати сайт та отримує доступ до всіх файлів. Іноді відновити доступ до ресурсу буває дуже складно, тому що для цього часто потрібний візит до власника хостингу. Подібна ситуація стає ще неприємнішою, якщо хостинг, на якому розміщено сайт, в іншій країні.

Не можна зберігати паролі в браузері, а також в окремому файлі в пам'яті комп'ютера. Найкраще зберігати облікові дані на окремому знімному носії.

Зрозуміло, не варто забувати і про надійність самих паролів, очевидно, що пароль типу Qwerty не забезпечить необхідний рівень безпеки. Найкращим рішенням стане використання спеціальних програм-генераторів, здатних створити надійні паролі, які дуже важко підібрати.

Оновлення SSL

Під час передачі конфіденційної інформації необхідно зашифрувати з'єднання між сайтом та браузером. Для того, щоб убезпечити сайт від злому хакерами, постійно оновлюйте версії поточних шифрувальних алгоритмів, наприклад, для SSL (Secure Sockets Layer - рівень захищених сокетів). Для забезпечення безпеки важливо використовувати оновлені версії бібліотеки шифрування. Так була виявлена серйозна вразливість у коді версій SSL 3.0 та 2.0. Саме тому оновлення потрібні.

Тестуйте сайт на наявність уразливостей

Компанії, що випускають банківські картки, зобов'язують продавців тестувати їхні ресурси на відповідність до певних стандартів безпеки. Однак цього часом недостатньо. Найнадійніший шлях запобігання непередбаченим зламам - проведення регулярного тестування ресурсів.

Вони регулярно сканують веб-сайти (включаючи перевірку всіх посилань), щоб переконатися, що хакери не впровадили зловмисне програмне забезпечення

в оголошення, графіку чи будь-який інший вміст, розміщений на сайті третіми сторонами.

Тестування на проникнення.

Добірка інструментів сканування, які допомагають виявити різні вразливості в коді під час тестування програми, щоб знайти вразливі місця у коді.

Шифруйте комунікації

Шифруйте комунікації зі своїми бізнес-партнерами, особливо коли це стосується даних платіжних карток. При необхідності можна навіть замислитись про шифрування електронних повідомлень.

Треба довіряти, але обов'язково перевіряти

Треба довіряти своїм клієнтам. Однак у наші дні найкраще перевірити двічі. Тому підключіть систему підтвердження адреси та запитуйте клієнтів вводити код автентифікації картки для всіх транзакцій.

Вибирайте надійного хостинг-провайдера

Вибираючи хостинг-провайдера, переконайтеся, що ви інвестуєте у якісні послуги. Багато хостерів, наприклад, Timeweb, пропонують набір послуг, що сприяють стабільній та надійній роботі сайту. Найбільшу безпеку можуть гарантувати провайдери, які:

- проводять регулярне резервне копіювання;
- проводять регулярний моніторинг мережі;
- надають підтримку.

Треба бути впевнені, у хостинг-провайдері.

Треба маскування адреси доступу до панелі адміністрування

Багато стандартних CMS мають стандартні адреси для входу в розділ керування. На щастя, практично завжди можна поміняти ці адреси менш очевидними, щоб ніхто сторонній не зміг увійти в панель адміністрування сайту.

Не варто встановлювати невідомі доповнення. Не всі програми можуть виявитися корисними. Часто подібні неперевірені доповнення служать не для розширення функціональних можливостей сайту, а для впровадження шкідливого коду, що дозволяє хакеру отримати доступ до сайту. Перед встановленням підозрілого скрипта правильним рішенням буде проконсультуватися з досвідченим веб-програмістом.

Таким чином надано рекомендації, спрямовані на підвищення рівня захищеності власних інтернет ресурсів. Але треба враховувати, що кожна окрема рекомендація потребує окремого ретельного розгляду. Треба враховувати, що підхід до забезпечення захисту інформації має бути системним та комплексним. Необхідно постійно та ретельно виконувати надані рекомендації та удосконалювати ці рекомендації в разі появи нових вразливостей та загроз персональним даним які збираєте.

Розробка рекомендацій що до захисту даних та перспектив розвитку інформаційних мереж

Історія та перспективи розвитку інтернету, централізованих та децентралізованих мереж та як результат - можливої архітектури децентралізованої мережі наступного покоління.

Web 2.0 концепції. Сформульована в 2005 році Тімом О'Рейлі — передбачає активне залучення користувачів до колективного створення та редагування контенту мережі. Без перебільшення, вершиною та тріумфом цієї концепції стали соціальні мережі. Гігантські платформи, що об'єднують мільярди користувачів та зберігають сотні петабайт даних.

Для соціальних мереж ця концепція надала:

– уніфікацію інтерфейсу; виявилося, що всі можливості по створенню різноманітного дизайну користувачам не потрібні; всі сторінки користувачів

мають однаковий дизайн і це всіх влаштовує та навіть зручно; відрізняється лише контент.

– уніфікацію функціоналу; все різноманіття скриптів виявилося також непотрібним. «стрічка», друзі, альбоми… за час існування соцмереж їх функціонал більш-менш стабілізувався і навряд чи зміниться: адже функціонал визначається видами активності людей, а люди практично не змінюються.

– єдину базу даних (БД); працювати з такою БД виявилося набагато зручніше, ніж із безліччю розрізнених сайтів; пошук став набагато простіше. Замість безперервного сканування різноманітних слабко пов'язаних сторінок, кешування всього цього, ранжирування за найскладнішими евристичними алгоритмами – відносно простий уніфікований запит до єдиної бази із відомою структурою.

– інтерфейс зворотного зв'язку - подобайки та репости; у звичайному Інтернеті той же Google ніяк не міг отримати зворотний зв'язок від користувачів після переходу за посиланням у пошуковій видачі. У соцмережах цей зв'язок виявився простим і природним.

Але була втрачена децентралізація, а отже, свобода. Вважається, що тепер наші дані нам не належать. Якщо раніше ми могли розмістити домашню сторінку хоч на власному комп'ютері, то тепер ми віддаємо всі наші дані інтернет-гігантам. Крім того, у міру розвитку Інтернету їм зацікавилися уряди та корпорації, у зв'язку з чим виникли проблеми політичної цензури та копірайтних обмежень. Наші сторінки в соцмережах можуть забанити та видалити, якщо контент не відповідає якимось правилам соцмережі; за необережне висловлювання — притягнути до адміністративної та навіть кримінальної відповідальності.

OcialFi - нова концепція взаємодії в криптоіндустрії. Ця концепція симбіоз децентралізованих фінансів (DeFi) та соціальних мереж, заснованих на блокчейні.

У централізованих ресурсах – жорсткий диктат серверного коду. У децентралізованих - необхідність домовлятися між безліччю рівних учасників. Зрозуміло, тут не обійтися без криптографії, блокчейнів та інших досягнень, відпрацьованих головним чином криптовалютах. Недоліки: децентралізована архітектура завжди складніше централізованою. Звідси і ряд недоліків: вартість, уніфікація, підключення до роздачі існуючих файлосховищ та інше.

Таким чином перспективним напрямком розвитку інформаційних мереж збереження персональних даних є використання децентралізації, по-перше, платформи соціальних мереж Web3 підвищують конфіденційність, оскільки вони дозволяють користувачам контролювати свої дані та володіти ними, що ускладнює доступ великих компаній чи урядів до їхньої інформації або її неправомірне використання.

Крім того, децентралізовані інформаційні мережі менш схильні до витоку даних, оскільки дані користувача зберігаються в децентралізованій мережі вузлів, а не на центральному сервері. Користувачі можуть створювати облікові записи без зв'язку з реальними особами, такими як адреси електронної пошти або номери телефонів. Ці мережі часто покладаються на криптографію з відкритим ключем для захисту облікового запису, а не на одну організацію для захисту даних користувача.

Висновки до 4 розділу

1. Таким чином удосконалено метод оцінки поведінки системи захисту персональної інформації, який відрізняється від існуючих застосуванням запропонованої моделі та оцінювання стійкості системи за допомогою методу фазової площини. Метод дозволяє знайти характеристики особливих точок, ізольованих замкнутих траєкторій, що, в свою чергу, дозволяє оцінити динаміку досліджуваної нелінійної динамічної системи в широкому діапазоні можливих початкових умов без отримання остаточних рішень диференціальних рівнянь.

2. Набув подальшого розвитоку метод деперсоналізації даних для захисту персональної інформації в мережах, який, на відміну від існуючих, враховує специфіку соціальної мережі: запізнення реагування на атаку, параметр комплексної довіри та параметр розширення інформаційної мережі. Запропонований метод дозволяє забезпечити ефективний захист персональної інформації у системах обробки даних інформаційної мережи.

3. Проведена оцінка ефективності методу захисту інформації у соціальній мережі. Оцінка ефективності проводилась за допомогою моделювання стійкості криптоалгоритмів експрес-аналізом на основі ентропійного методу. Отримані результати моделювання процесу визначення крипостійкості доводять перевагу запропонованого алгоритму з попереднім випадковим змішуванням, за показником крипостійкості алгоритму, над іншими сучасними алгоритмами шифрування більш ніж на 10%. Таким чином результати моделювання підтвердили, що у результаті розробки математичних моделей та застосування узагальненого методу захисту персональних даних дозволено підвищити ефектівність їх захисту загалом на 10-12%.

4. Розроблено рекомендації щодо створення безпечної архітектури децентралізованої інформаційної мережі, що захищає конфіденційність, цілісність особистої інформації та інформаційних повідомлень загалом. Ці рекомендації особливо актуальні на сучасний момент у зв’язку з практично необмеженим використанням інформаційних мереж користувачами.

ВИСНОВКИ

В результаті дисертаційних досліджень вирішено актуальне наукове завдання щодо розробки науково-методичного апарату захисту персональних даних з урахуванням специфіки соціальних мереж.

Реалізація зазначеного науково-методичного апарату наддасть можливість підвищити захищеность персональних даних в інформаційних мережах за рахунок врахування специфіки соціальних мереж: запізнення реагування на атаку; комплексної довіри; урахування параметра розширення мереж; урахування сильних та слабких зв'язків між користувачами та оцінки економічних витрат на захист персональної інформації в інформаційних мережах.

Відсутність аналогічних рішень у нашій країні та за кордоном робить результати досліджень пріоритетними.

В дисертації одержані такі основні результати:

1. На підставі проведеного аналізу, результатів вивчення наукових публікацій за темою досліджень, дисертацій, патентів, монографій та практичних доробок було визначено, що у повної мірі не вирішені питання щодо захисту персональних даних. Було виявлено існування протиріччя між загальним характером існуючих математичних моделей захисту персональних даних та необхідністю підвищення захищеності персональних даних у соціальних мережах. Відсутність дієвих методик ефективного та надійного захисту персональних даних у інформаційних мережах доводять актуальність обраного наукового завдання.

2. Вперше розроблено математичну модель захисту персональних даних у соціальних мережах, яка базується на моделі Лотки-Вольттери та враховує такі

параметри функціонування мережі: запізнення реагування на атаку, параметр загальної довіри та параметр розширення соціальної мережі. Модель дозволяє провести об'єктивну оцінку балансу між загрозами безпеки інформації та специфічними параметрами мережі, оцінити економічні витрати на захист персональної інформації у інформаційній мережі.

3. Удосконалено метод оцінки поведінки системи захисту персональних даних, який відрізняється від існуючих застосуванням запропонованої моделі та оцінювання стійкості системи за допомогою методу фазової площини. Метод дозволяє знайти характеристики особливих точок, ізольованих замкнутих траєкторій, що, в свою чергу, дозволяє оцінити динаміку досліджуваної нелінійної динамічної системи в широкому діапазоні можливих початкових умов без отримання остаточних рішень диференціальних рівнянь.

4. Набув подальшого розвитку метод деперсоналізації даних для захисту персональної інформації в мережах, який, на відміну від існуючих, базується на розробленій моделі захисту. Запропонований метод дозволяє забезпечити ефективний захист персональної інформації в системах обробки даних інформаційної мережі.

5. Проведена оцінка ефективності методу захисту інформації у соціальній мережі. Отримані результати моделювання процесу захисту персональних даних у соціальних мережах довели, що впровадження запропонованих наукових результатів дозволить підвищити ефективность захисту персональних даних загалом на 10-12%.

6. Розроблено практичні рекомендації щодо захисту персональних даних. Розроблена методика дозволяє захищати персональні дані з ефективністю, що на 10-12% відсотків більша чим ефективність захисту за існуючими методами та

методиками. Розроблено рекомендації створення безпечної архітектури децентралізованої інформаційної мережі, що захищає конфіденційність персональних даних.

7. Результати досліджень прийняті до впровадження в Інституті програмних систем Національної академії наук України (акт від 07.02.2023 року); Науково методичному центрі кадрової політики Міністерства оборони України (акт від 19.10.2023 року).

8. Мета досліджень щодо підвищення захищеності персональних даних у інформаційних мережах за рахунок врахування специфіки соціальних мереж: запізнення реагування на атаку; комплексної довіри, урахування параметра розширення соціальних мереж, урахування сильних та слабких зв’язків між користувачами на захист персональної інформації у інформаційних мережах досягнута та всі часткові завдання вирішені повністю. Наукові результати досліджень є внеском в розвиток наукових теоретичних, методологічних, технічних, технологічних й організаційних основ створення комплексних систем захисту інформації, зокрема інформації, що зберігається, оброблюється і передається в комп’ютерних системах і мережах.

9. Напрямками подальших досліджень може бути питання щодо розробки нових та удосконалення існуючих методів виявлення зовнішніх впливів на середовища збереження персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лаптєв О.А., Лаптєв С.О. Забезпечення інформаційної безпеки на підприємствах за допомогою сучасних інформаційних систем. Тези доповідей: Міжнародної науково-практична конференція студентів, аспірантів та молодих вчених «Комп'ютери. Програми. Інтернер.2003». м. Київ. НТСА НТУУ КПІ 21-23 квітня 2003 р. С.100 – 101.

2. Лаптєв О., Собчук В., Собчук А., Лаптєв С., Лаптєва Т. Застосування періодичних розв'язків нелілейних диференціальних рівнянь з імпульсною дією в моделях систем захисту інформаційних мереж. Збірник наукових матеріалів «I International scientific and theoretical conference» (Internet). 23.04.2021. Краків, Poland. С.138–141.

3. Лаптєв О.А., Гребенніков А.Б., Лаптєв С.О., Загиней А.Ю. Модель захисту інформації при нелінійних параметрах зовнішніх впливів з урахуванням взаємодії користувачів. Тези доповідей «Актуальні проблеми управління інформаційною безпекою держави», XII Всеукраїнська науково-практична конференція. Київ, 26 березня 2021 р. С.64 – 66

4. Svynchuk O., Barabash A., Laptiev S. and Laptieva T. Modification of query processing methods in distributed databases using fractal trees. International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv – Odesa, Ukraine. P.32 – 37, ISBN 978-966-676-818-9. Scopus

5. Laptiev O., Lukova-Chuiko N., Laptiev S., Laptieva T., Savchenko V., Yevseiev S. Development of a method for detecting deviations in the nature of traffic from the elements of the communication network. International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv – Odesa, Ukraine. P.1–9, ISBN 978-966-676-818-9. Scopus

6. 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. P.15-21.

7. Лаптев О.А., Собчук В.В., Саланда И.П., Сачук Ю.В. Математична модель структури інформаційної сеті на основі нестационарної ієрархічної та стаціонарної гиперсети. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, Вип. 64, 2019. С. 124 – 132.

8. Laptev A., Sobchuk V., Barabash O., Musienko A., Analysis of the main Approaches and Stages for Providing the Properties of the Functional Stability of the Information Systems of the Enterprise .Sciences of Europe. Praha, Czech Republic. 2019. Vol. 1. No 42. P. 41 – 44.

9. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., ...Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, С. 67–70. Scopus

10. Vlasyk, H., Zamrii, I., Shkapa, V., ...Kalyniuk, A., LaptievA, T. The method of solving problems of optimal restoration of telecommunication signals. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, С. 71–75. Scopus

11. Andrii Sobchuk, Halyna Haidur, Serhii Laptiev, Tetiana Laptieva, Farhod Asrorov, Oleh Perehuda. Modified Fourier transform for improving spectral analysis of radio signals. “Modern information, measurement and control systems: problems, applications and perspectives’2022” (MIMCS’2022). November 4-5, 2022, Antalya, Turkey. Scopus

12. Yevseiev, S., Trakaliuk, O., Kuzmenko, M., Laptieva T., Laptiev, S., Polovinkin, I. An Improved Method of Detection and Localization of Signals the Digital Range 2022 IEEE 4th International Conference on Advanced Trends in nformation Theory (ATIT), 15-17 December 2022, Kyiv, Ukraine, 2022. P.129 – 132. Scopus. DOI: 10.1109/ATIT58178.2022.10024242

13. Закон України "Про інформацію" [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

14. Закон України "Про захист персональних даних" [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

15. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В.. Інформаційна та Кібербезпека: Соціотехнічний Аспект. Київ: ДУТ, 2015-315с.

16. Ахрамович В.М. Модель сильних та слабких зв’язків користувачів у соціальних. Зв'язок, 2019, №3, С.1-5.

17. Базарний С. Класифікація методів аналізу та моделей соціальних мереж в інтересах інформаційної операції. Ukrainian Scientific Journal of Information Security. 2023, vol. 29, issue 2, P. 61-66

18. S.Yevseiev, O. Laptiev, O.Korol, S.Pohasii, S.Milevskyi, R. Khmelevsky. Analysis of information security threat assessment of the objects of information activity. International independent scientific journal. Poland. Vol. 1, №34, 2021, P.33 – 39. ISSN 3547-2340

19. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. 220 с

20. Черняк А. М., Прозоров А. Ю. Аспекти запобігання правопорушенням у сфері використання банківських платіжних карток під час

проведення безконтактних й інтернет-платежів та їх кваліфікація. Naukovij visnik Nacional'noi akademii vnutrisnih sprav. №4 (113).c.8-14. 2019. ISSN 2410-3594.

21. Що таке фішинг? [Електронний ресурс] – Режим доступу до ресурсу: http://help.sslatcost.com/article/346?locale=uk.

22. Безмалий В.Ф. Фішинг (Phishing), Вішинг (vishing), Фармінг – шахрайство в Інтернеті [Електронний ресурс] / В.Ф. Безмалий. – Режим доступу до ресурсу: http://vse-prosto.весьтоп.рф/fishing-phishing-vishing-vishing-farming.html.

23. Szafranski R. Theory of Information Warfare: Preparing For 2020. Official Site of "Airpower Journal". URL:http://www.airpower.au.af.mil/airchronicles/apj/apj95/spr95_files/szfran.htm

24. Sobchuk V., Zamrii I., Sobchuk A., Laptiev S., Laptieva T. Periodic solutions of nonlinear differential equation of models information network. Sciences of Europe. Praha, Czech Republic, Vol. 1. No 67. 2021. ISSN 3162-2364. P. 31 – 35

25. Sobchuk V., Sobchuk A., Laptiev S., Laptieva T., Hrebennikov A., Bobrov S. Investingation of dynamic processes in information networks with the application neural networks. International independent scientific journal. Poland. Vol.1,№26, 2021. pp.36–42

26. Sobchuk V., Breslavsky V., Laptiev S., Laptieva T., Zahynei A., Kovalenko O. Development of routing algoritm for self-organizing information networks. German International Journal of Modern Science №7, Vol. 2, 2021. P.32–35, ISSN (Print) 2701-8369, ISSN (Online) 2701-8377

27. Valentin Sobchuk, Iryna Zamrii, Andrii Sobchuk, Serhii Laptiev, Tetyana Laptieva, Vladimir Samosyuk. Method of Data Processing in Information Systems Using Solutions of Differential Equations with Impulse Effect. International Journal of Science and Engineering Investigations. (IJSEI) Denmark. April.2021. Vol. 10, Issue 11. P. 1–6

28. S. Laptiev, T. Laptieva, A. Hrebennikov, O.Kitura, V. Marchenko, M. Lutsenko Advanced model of the protection system of insider informations. Journal of science. Lyon Vol.1. №20. 2021. P.39–44

29. Oleksandr Laptiev, Valentyn Sobchuk, Andrii Sobchuk, Serhii Laptiev, Tetiana Laptieva. Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Кібербезпека: освіта, наука, техніка. Том 4 № 12, 2021. P19–28. DOI: https://doi.org/10.28925/2663-4023.2021.12.1928

30. Valentin Sobchuk, Iryna Zamrii,Yuliya Olimpiyeva, Serhii Laptiev. Functional stability of technological processes based on nonlinear dynamics with the application of neural networks. Advanced information systems. Kharkiv.Vol.5. №2. 2021 P.49–57.

31. Rostislav Khmelevskoy, Serhii Laptiev, Tetiana Laptieva. Improving the Method of Assessing the Information Security of Computer Systems from Malicious Software. International Journal of Science and Engineering Investigations. (IJSEI) Denmark. Juli. 2021. Vol. 10, Issue 113. P. 43–48

32. Asadi Hrebennikov, Serhii Laptiev, Tetiana Laptieva, Mykhailo Lutsenko, Anton Naumenko, German Shuklin. Development of a model for detecting means of covert information retrieval using topological threat identification. International Journal of Science and Engineering Investigations. (IJSEI) Denmark. Juli. 2021. Vol. 10, Issue 113. P. 1–5.

33. Лукова-Чуйко Н.В., Толюпа С.В., Погасій С.С., Лаптєва Т.О., Лаптєв С.О. Удосконалення моделі захисту інформації в соціальних мережах. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, Вип. 73, 2021. С. 88 – 103. DOI: https://doi.org/10.17721/2519-481X/2021/73

34. Inna Kal’chuka, Serhii Laptiev, Tetiana Laptieva. Analysis of Data Transmission using one modified neural networks. International Journal Artificial Intelligent and Informatics. Vol.3, No.2, December2021, P. 73–79. ISSN 2622-626X. https://doi.org/10.33292/ijarlit.v3i2.49

35. Serhii Laptiev. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 4(16), 2022. С. 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562

36. S. Laptiev, S. Tolupa. The methodology for evaluating the functional stability of the protection system of special networks. Наукоємні технології. Інформаційні технології, кібербезпека. Том 55 № 3 (2022) С.178 – 183. https://doi.org/10.18372/2310-5461.55.16900

37. Замрій І.В., Собчук А.В., Лаптєв С.О., Лаптєва Т.О., Копитко С.Б. Алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем. Телекомунікаційні та інформаційні технології. № 1 (74). 2022. С.4 - 15.

38. Корольков Роман Юрійович, Лаптєв Сергій Олександрович. Натурне моделювання атаки «war driving» на бездротову мережу. Кібербезпека: освіта, наука, техніка. No 2 (18), 2022, С. 99-107.

39. Толюпа Сергій, Лаптєв Сергій. Удосконалення математичної моделі захищеності особистих даних за рахунок врахування довіри та кількісті інформації в соціальних мережах. Безпека інформації. Безпека інформації. НАУ. Том 28 № 3 (2022): Безпека інформації. 2022, С.143-148.

40. Лаптєв О.А., Лаптєв С.О. Забезпечення інформаційної безпеки на підприємствах за допомогою сучасних інформаційних систем. Тези доповідей: Міжнародної науково-практична конференція студентів, аспірантів та молодих

вчених «Комп'ютери. Програми. Інтернер.2003». м. Київ. НТСА НТУУ КПІ 21-23 квітня 2003 р. С.100 – 101.

41. Лаптєв О., Собчук В., Собчук А., Лаптєв С., Лаптєва Т. Застосування періодичних розв'язків нелілейних диференціальних рівнянь з імпульсною дією в моделях систем захисту інформаційних мереж. Збірник наукових матеріалів «I International scientific and theoretical conference» (Internet). 23.04.2021. Краків, Poland. С.138–141.

42. Лаптєв О.А., Гребенніков А.Б., Лаптєв С.О., Загиней А.Ю. Модель захисту інформації при нелінійних параметрах зовнішніх впливів з урахуванням взаємодії користувачів. XII Всеукраїнська науково-практична конференція. Київ, 26 березня 2021 р. С.64–66

43. Богдан Анастасія Сергіївна, Лаптєв Сергій Олександрович, Лаптєва Тетяна Олександрівна, Кітура Олег Володимирович. Ідентифікація та верифікація особистостей, як складова комплексної системи захисту об'єкта. XXVII Міжнародна науково-практична конференція, 25-28 мая 2021, Амстердам, Нидерланды 2021р. С . 674 – 680.

44. Крупенко С.В., Лаптєв С.О., Лаптєва Т.О., Кітура О.В. Побудова системи контролю та управління доступом за допомогою акустичного методу автентифікації та авторизації. «Science of post-industrial society: globalization and transformation processes» 04.06.2021 Вінниця, UKR - Відень, AUT. https://ojs.ukrlogos.in.ua/index.php/grail-of-science/issue/archive

45. Собчук В.В., Барабаш О.В., Мусієнко А.П. Лаптєв С.О. Організація інформаційної системи підприємства із застосування методології адаптивного накопичення діагностичної інформації. X Міжнар. наук.–практ. конф.», 4–6 червня 2021 р. Луцьк–Світязь: СНУ імені Лесі Українки, 2019. С. 58 – 59.

46. Oleksandr Laptiev, Sergii Laptiev. The method detection of radio signals based to use on the differential transformation. «IV Міжнародна науково-практична

конференція. Проблеми кібербезпеки інформаційно-телекомунікаційних систем».(PCSITS). Київ. 15-16 квітня 2021 року С.33-35.

47. С.О. Лаптєв. Удосконалення моделі виявлення загроз несанкціонованого витоку персональних даних з соціальних мереж. Науково-технічна конференція молодих вчених «Актуальні проблеми інформаційних технологій» (АРЈТ-2021)19-20 жовтня 2021р. Київ. С.58 –60.

48. Sergii Laptiev, Tetiana Laptieva .An improved method of detecting signals of unauthorized information leakage. VIII Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» 11 - 12 листопада 2021р. Львів, Україна. С.115–117.

49. Т.О. Лаптєва, С.О. Лаптєв. Удосконалення методу захисту інформації за рахунок топологічної ідентифікації загроз. VIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень» 17-19 листопада 2021 р. Київ. Україна. С.92–95

50. Svynchuk O., Barabash A., Laptiev S. and Laptieva T. Modification of query processing methods in distributed databases using fractal trees. International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv – Odesa, Ukraine. pp.32–37, ISBN 978-966-676-818-9. Scopus

51. Laptiev O., Lukova-Chuiko N., Laptiev S., Laptieva T., Savchenko V., Yevseiev S. Development of a method for detecting deviations in the nature of traffic from the elements of the communication network. International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv – Odesa, Ukraine. pp.1–9, ISBN 978-966-676-818-9. Scopus

52. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., ...Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, С. 67–70.Scopus

53. Vlasyk, H., Zamrii, I., Shkapa, V., ...Kalyniuk, A., LaptievA, T. The method of solving problems of optimal restoration of telecommunication signals. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, С. 71–75. Scopus

54. Savchenko V., Akhramovych V., Dzyuba T., ...Lukova-Chuiko N., LaptievA T. Methodology for calculating information protection from parameters of its distribution in social networks. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, С. 99–105. Scopus

55. Лаптєв С.О., Толюпа С.В., Барабаш О.В. Модель виявлення витоку інформації за допомогою топологічної ідентифікації загроз. Математика. Інформаційні технології. Освіта. 2022 рік: збірка тез допов. учасник. XI Міжнар. наук.–практ. конф., 3–5 червня 2022 р. Луцьк–Світязь: СНУ імені Лесі Українки, 2022. С. 96 – 101.

56. Сергій Лаптєв, Сергій Толюпа, Іван Опірський. Дослідження моделей захисту інформації у кіберфізичних системах. V Міжнародна науково-практична конференція. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)”27-28 жовтня 2022 р. Київ, Україна. Збірник матеріалів доповідей та тез. С 11-12.

57. Andrii Sobchuk, Halyna Haidur, Serhii Laptiev, Tetiana Laptieva, Farhod Asrorov, Oleh Perehuda. Modified Fourier transform for improving spectral analysis of radio signals. “Modern information, measurement and control systems: problems,

applications and perspectives’2022” (MIMCS’2022). November 4-5, 2022, Antalya, Turkey. Scopus

58. Yevseiev, S., Trakaliuk, O., Kuzmenko, M., Laptieva T., Laptiev, S., Polovinkin, I. An Improved Method of Detection and Localization of Signals the Digital Range 2022 IEEE 4th International Conference on Advanced Trends in nformation Theory (ATIT), 15-17 December 2022, Kyiv, Ukraine, 2022. P.129 – 132.

59. Ахрамович В.М., Чегренець В.М. Дослідження науково–методичного апарату захисту даних особистості в соціальний мережах. Sciences of Europe. Praha, Czech Republic. 2019. № 46. P. 36–39. www.european–science.org

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

61. Голубенко О. Л. Петров А. С., Петров А. О. Соціальні мережі як загроза безпеки [Електронний ресурс] 2018. Режим доступу до ресурсу. http://www.nbuv.gov.ua/old_ jrn/Soc_Gum/VSUNU/2011_7/title/1.pdf.

62. Грищук Р. В. Диференціально–ігрова розгалужена спектральна модель процесу нападу на інформацію. Вісник Житомирського державного технологічного університету. 2019. № I (48). С. 152–159.

63. Грищук Р. В. Р–моделювання процесів нападу на інформацію при нестаціонарній природі потоків захисних дій та інформаційних атак. Р.В. Грищук. Системи обробки інформації. Х. ХУПС ім. І. Кожедуба. № 7 (79). 2019. С. 98–101.

64. Грищук Р.В. Диференціально–ігрова модель системи захисту інформації при нестаціонарній природі потоків захисних дій та інформаційних атак. Р. В. Грищук. Інформаційна безпека. № 2 (4). 2019.С. 23–29.

65. Грищук Р.В. Диференціально–тейлорівська модель перебування технічного об’єкта під впливом методів несанкціонованого доступу. Р.В. Грищук. Захист інформації. 2019. №1 (42). С. 19–27.

66. Грищук Р.В. Концепція побудови диференціально–ігрових гарантовано захищених розподілених систем захисту інформації. Сучасний захист інформації. № 1 (6). 2017. С. 4–9.

67. Грищук Р.В. Метод диференціально–ігрового Р–моделювання процесів нападу на інформацію. Інформаційна безпека. 2019. № 2. С. 128–132.

68. Грищук Р.В. Спектральна модель процесу нападу на інформацію. Р.В. Грищук. Захист інформації. 2019. № 2 (43). С. 71–81.

69. Дудикевич В.Б., Опірський І.Р. Аналіз моделей захисту інформації в інформаційних мережах держави. Системи обробки інформації. 2016. № 4 (141).

70. Лаптєв О.А. Модель інформаційної безпеки на основі марковських випадкових процесів. Науково–практичний журнал «Зв'язок». К. ДУТ. 2018. № 6 (136). С. 45 – 49.

71. Лаптєв О.А., Степаненко В.І., Тихонов Ю.О. Формальні математичні моделі для забезпечення безпеки інформації. Сучасний захист інформації: науково–технічний журнал. К ДУТ. 2019. № 1. С. 59 – 64.

72. Петров А.А., Хорошко В.А. Збірник наукових праць Київського національного університету імені Тараса Шевченка. К. ВІКНУ. 2019. № 21. С. 128–131. www.isa.ru.

73. Про захист осіб у зв’язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.81. № 108. Офіційний вісник України. 2011. № 1. 701 с.

74. Про захист осіб у зв’язку з обробкою даних у інформаційних магістралях: Рекомендації Ради Європи R(99)5 від 09.11.99. Режим доступу. //www.medialaw.kiev.ua /laws/laws_international/105/

75. Про захист персональних даних. Закон України від 01.06.10 р. № 2297–VI. Офіційний вісник України. 2010. № 49. 199 с.

76. Про захист фізичних осіб при обробці персональних даних і вільним обігом цих даних: Директива Європейського парламенту та Ради 95/46/ЄС від 24.10.85. Режим доступу. //www.zakon.rada.gov.ua /laws/show/994_242

77. Стефурак О.Р.,Тихонов Ю.О., Лаптєв О.А., Зозуля С.А. Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. Сучасний захист інформації. №2 (42). 2020.С. 19-26.

78. Хорошко В.О., Хохлачова Ю.Є. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Т. 22. Частина 1: Безпека інформації. 2016. DOI: 10.18372/2225-5036.22.11104

79. A Satsiou. and L. Tassiulas. Reputation–based resource allocation in p2p systems of rational users. IEEE Transactions on Parallel and Distributed Systems. 2018. 21 (4). P. 466 –479.

80. A.–L. Barabási, R. Albert, and H. Jeong, “Mean–field theory for scale–free random networks,” Physica A: Statistical Mechanics and its Applications, 2019. vol. 272, №. 1–2. P. 173 – 187.

81. Ballester C., Zenou Y. Key Player Po licies When Contextual Effects Matter. Jour nal of Mathematical Sociology. 2018. №. 38. P. 233–248. Available at: https://pdfs. semanticscholar.org.

82. Barabási A.–L., Albert R. Emergence of scaling in random networks. Science. 2019. V.286. P.509–512.

83. Barabási A.–L., Albert R., Jeong H. Scale–free characteristics of random networks. The topology of the world–wide web. Physica A. 2019. V.281. P.69–77.

84. Barabasi A.L., Bonabeau E. Scale Free Networks. Scientific American. 2019. P. 50–59.

85. Basilisa Mvungi, Mizuho Iwaihara. Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. Computers in Human Behavior. Dec. 2019. P. 20–34.

86. Bondar I. V. Construction method for information security threat models of automated systems. Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta imeni akademika M. F. Reshetneva. 2019. P. 7 – 10.

87. Callaway D. S. Network Robustness and Fragility: Percolation on Random Graphs. Duncan S. Callaway, M. E. J. Newman, Steven H. Strogatz, Duncan J. Watts. Physical Review Letters. 2019. Vol. 85. №25. P. 5468–5471.

88. Carl Timm, Richard Perez. Seven Deadliest Social Network Attacks. Syngress Publishing. 2019. L.A.Cutillo,R.Molva,andT.Strufe, Safebook:Aprivacy–preservingonline social network leveraging on real–life trust. Communications Magazine, IEEE. Dec. 2019. vol. 47. P. 94–101,

89. Chen, P.A Study on Advanced Persistent Threats. Communications and Multimedia Security. Chen, P., Desmet, L., Huygens, C. Springer Berlin Heidelberg. 2019. P. 63—72.

90. Dushkin A.V., Demchenkov A.V. Analytical model for estimation the effectiveness of efficiency data protection from threats of violations integrity in information systems. «Vestnik Voronezhskogo instituta MVD Rossii». 2016. № 1. P. 87–95.

91. Freeman L.C. Centrality in social networks: Conceptual clarification. Social Networks. 2018. №1. P. 215–239.

92. Friedkin N. E. Theoretical foundations for centrality measures. Amer. J. Sociol. 2019. V. 96. P. 1478–1504.

93. S. Yevseiev, H. Kots, S. Minukhin, O. Korol, and A. Kholodkova, “The development of the method of multifactor authentication based on hybrid crypto-code

constructions on defective codes". Eastern-European journal of enterprise technologies. 2017. 5/9(89). P. 19 – 35,.

94. Kosko B. Fuzzy cognitive maps. International Journal of Man–Machine Studies, 2019. Vol.1. P. 65–75.

95. Kotenko I. V., Chechulin A. A., Shorov A. V., Komashinsky D. V. Analysis and evaluation of web pages classification techniques for inappropriate content blocking. 14th Industrial Conference on Data Mining, LNAI. New York e. a.: Springer–Verlag. 2019. Vol. 8557. P. 39–54.

96. L.A.Cutillo,R.Molva,andT.Strufe. Privacy preser ving social network ingthrough decentralization. in 2019 Sixth International Conference on Wireless On–Demand Network Systems and Services (WONS). 2019. P. 145–152, IEEE, Feb. 2019.

97. Meila M., Shi J. A. Random Walks View of spectral segmentation. Proceedings of AISTATS. 2019. P. 1–6.

98. Melman S., Bobkov V., Cherkashin A. Technology and system visualization of large amounts of synoptic data. Journal Information Science and Control Systems. 2019. Vol. 3(45). P. 63–71.

99. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation. System Sciences. 2019. P. 2431–2439.

100. Newman M. E., Girvan M. Finding and evaluating community structure in networks. Physical Review E., vol. 69(2), 2019. P. 26–53.

101. Opsahl T., Agneessens F., Skvoretz J. Node centrality in weighted networks: Generalizing degree and shortest paths. Social Networks Journal. Vol. 32(3). 2019.P. 245–251.

102. P. Dewan and P. Dasgupta. P2p reputation management using distributed identities and decentralized recommendation chains. IEEE Transactions on Knowledge and Data Engineering, July. 2019. №22(7) P. 1000 –1013.

103. P. Michiardi and R. Molva. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Proceedings of IFIP Communication and Multimedia Security Conference. CMS 2019. Portoroz, SLOVENIA. 2019.

104. Patrick Van Eecke, Maarten Truyens. Privacy and social networks. Computer Law & Security Review. 2018. №26(5). P. 535–546.

105. Pavlo Shchypanskyi, Vitalii Savchenko, Volodymyr Akhramovych, Tetiana Muzshanova, Svitlana Lehominova, Volodymyr Chegrenets.The Model of Secure Social Networks Activity Based on Graph Theory/ International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278–3075,Volume–9 Issue–4, February 2020 Pp 1803–1810. https://www.ijitee.org/download/volume–9–issue–4.

106. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: an online social network with user–defined privacy. SIGCOMM Comput. Commun. Rev. 2018.vol. 39. P. 135–146.

107. Raymond D. Privacy–preserving social network analysis. A dissertation for the science degree of doctor philosophy in University of Texas at Dallas University of Texas at Dallas in Partial Fulfillment of the Requirements for the Degree of, USA. 2019. P. 134 –158.

108. Reid Fergal, McDaid Aaron, Hurley Neil. Partitioning breaks communities. Mining Social Networks and Security Informatics. Springer. 2019. P. 79–105.

109. S. Buchegger and A. Datta. A case for P2P infrastructure for social networks – opportunities & challenges. in WONS'19 IEEE. Feb. 2019. P. 161 – 168,

110. S. Buchegger, D. Schiöberg, L.–H. Vu, and A. Dattaю Peerson: P2p social networking: early experiences and insights. in Proceedings of the Second ACM

EuroSys Workshop on Social Network Systems. SNS ’19, (New York, NY, USA), ACM. 2019. P. 46–52,

111. S.E. Smaha. Haystack: an intrusion detection system. Aerospace Computer Security Applications Conference. 2019. P. 37–44.

112. Vitalii Savchenko, Volodymyr Akhramovych, Alina Tushych, Irina Sribna, Ihor Vlasov. Analysis of Social Network Parameters and the Likelihood of its Construction. International Journal of Emerging Trends in Engineering Research ISSN 2347 –3983, Volume 8.№. 2. February 2020. P. 271–276.

113. Watts D.J., Strogatz S.H. Collective dynamics of “small–world” networks. Nature. 2018. Vol. 393. P. 440–442. gs.statcounter.com/social–media – stats.

114. Williamson, Matthew M.; Laeveillae, Jasmin, Epidemiological model of virus spread and cleanup. Hewlett–Packard Laboratories Bristol. February 27th. 2019. URL: http://www.hpl.hp.com/techreports/2019/HPL–2003–39.pdf.

115. X. Yin, W. Yurcik, A. Slagell, The design of VisFlowConnect–IP: a link analysis system for IP security situational awareness[A]. IEEE International Workshop on Information Assurance[C]. IEEE. 2018. P. 141–153.

116. Zadeh L., Abbasov A., Shahbazova S. Fuzzy based techniques in human like processing of social network data. Intern. Journal of Uncertainty, Fuzziness and Knowledge–Based Systems. Singapore: World Scientific. 2019. Vol. 23 (Suppl. 1). P. 1–14.

117. Lukova–Chuiko N., Barabash O., Musiyenko A. Methods of self–diagnosis of telecommunication networks based on flexible structures of test connections. Collection of materials of International Scientific Conference «Complex Systems Security Management – 2015». Liptovský Mikuláš, Slovakiya. 2015. P. 215 – 220.

Додаток А

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Лаптєв С. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка. 2022. Том 4, №16. С. 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562

2. Лаптєв С., Собчук В., Собчук А., Лаптєва Т. Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Кібербезпека: освіта, наука, техніка. 2021. Том 4, № 12. С.19 – 28. https://doi.org/10.28925/2663-4023.2021.12.1928, ISSN 2663-4023

3. Laptiev S., Tolupa S. The methodology for evaluating the functional stability of the protection system of special networks. Наукоємні технології. Vol. 55, № 3. 2022. P.178 – 183. https://doi.org/10.18372/2310-5461.55.16900

4. Корольков Р., Лаптєв С. Натурне моделювання атаки «war driving» на бездротову мережу. Кібербезпека: освіта, наука, техніка. Том 2, №18. 2022. С. 99-107. https://doi.org/10.28925/2663-4023.2022. 18.99107, ISSN 2663-4023.

5. Толюпа С., Лаптєв С. Удосконалення математичної моделі захищеності особистих даних за рахунок врахування довіри та кількісті інформації в соціальних мережах. Безпека інформації. 2022.Том 28, № 3. С.143–148. https://doi.org/10.18372/2225-5036.28.17371

6. Замрій І.В., Собчук А.В., Лаптєв С.О., Лаптєва Т.О., Копитко С.Б. Алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем. Телекомунікаційні та інформаційні технології. 2022.№ 1 (74). С.4 - 15. https://doi.org/10.31673/2412-4338.2022.010414

7. Sobchuk V., Laptiev S., Laptieva T., Barabash O., Drobyk O., Sobchuk A. A modified method of spectral analysis of radio signals using the operator approach for

the fourier transform. 2024. IT, Automation, Measurements in Economy and Environmental Protection. Vol. 14, No 2, P.56–61. https://doi.org/10.35784/iapgos.5783 **Scopus**

8. Лаптєв С. Розробка моделі захисту особистих даних у соціальних мережах. Захист інформації. Том 26, №1. 2024. С.43-50 https://jrnl.nau.edu.ua/index.php/ZI/article/view/18824

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Лаптєв С.О. Удосконалення моделі виявлення загроз несанкціонованого витоку персональних даних з соціальних мереж. Науково-технічна конференція молодих вчених *«Актуальні проблеми інформаційних технологій» (APJT-2021)*19-20 жовтня 2021р. Київ. С.58 –60.

2. Laptiev S., Laptieva T. An improved method of detecting signals of unauthorized information leakage. *VIII Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем»* 11 – 12 листопада 2021р. Львів, Україна. С.115–117.

3. Лаптєв С.О., Лаптєва Т.О. Удосконалення методу захисту інформації за рахунок топологічної ідентифікації загроз. *VIII Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень»* 17-19 листопада 2021 р. Київ. Україна. С.92–95.

4. Savchenko V., Akhramovych V., Dzyuba T., ...Lukova-Chuiko N., LaptievA T. Methodology for calculating information protection from parameters of its distribution in social networks. *2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 – Proceedings*. 2021. С. 99 – 105. **Scopus**

5. Лаптєв С.О., Толюпа С.В., Барабаш О.В. Модель виявлення витоку інформації за допомогою топологічної ідентифікації загроз. *Математика. Інформаційні технології. Освіта.* 2022 рік: збірка тез допов. учасник. XI Міжнар.

наук.–практ. конф., 3–5 червня 2022 р. Луцьк–Світязь: СНУ імені Лесі Українки, 2022. С. 96 – 101.

6. Sobchuk V., Zamrii I., Laptiev S. Ensuring Functional Stability of Technological Processes as Cyber-physical Systems Using Neural Networks. *At the international conference on smart technologies in urban engineeringheld in Kharkiv*, Ukraine, 9-11 June 2022. Springer. https://link.springer.com/chapter/10.1007/978-3-031-20141-7_53

7. Лаптєв С., Толюпа С., Опірський І. Дослідження моделей захисту інформації у кіберфізичних системах. *V Міжнародна науково-практична конференція. «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS)* 27-28 жовтня 2022 р. Київ, Україна. Збірник матеріалів доповідей та тез. С 11-12.

8. Лаптєв С.О. Моделі та методи захисту персональних даних з урахуванням специфіки соціальних мереж. *X Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених. «Об'єднані наукою: перспективи міждисциплінарних досліджень».* 23–24 листопада 2023 р. Київ. Збірник праць конференції. С.129-130.

9. Лаптєв С. Модель захисту персональних даних з урахуванням специфіки функціонування інформаційних мереж. *1st international scientific and practical conference «Information Systems and Technology: Results and Prospects» (IST 2024)",* March 6, 2024. Kyiv. C. 350-352.

Відомості про апробацію результатів дисертації

1. Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених «Комп'ютери. Програми. Інтернер.2003». НТСА НТУУ КПІ 21-23 квітня 2003 р. м. Київ: форма участі – очна.

2. XII Всеукраїнська науково-практична конференція. Київ, 26 березня 2021 р. Київ: форма участі – очна.

3. Всеукраїнська науково-практична конференція «Актуальні проблеми інформаційних технологій» (АРЈТ-2021)19-20 жовтня 2021р. Київ: форма участі – очна.

4. VIII Всеукраїнськf науково-практичнf конференціz студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень» 17-19 листопада 2021 р. Київ: форма участі – очна.

5. International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv – Odesa. Odesa**. Scopus**: форма участі – очна.

6. International Scientific And Practical Conference "Information Security And Information Technologies": Conference Proceedings. 13-19 September 2021. Kharkiv – Odesa, Odesa. **Scopus:** форма участі – очна.

7. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, Kyiv. **Scopus** : форма участі – очна.

8. V Міжнародна науково-практична конференція. "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)"27-28 жовтня 2022 р. Київ :форма участі – онлайн.

9. 2022 IEEE Third International Conference on system analysis & intelligent computing (SAIC), 04-07 Oktober, Kyiv, Ukraine. p. 148-153. **Scopus** : форма участі – онлайн.

10. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), 15-17 December 2022, Kyiv, Ukraine: форма участі – онлайн.

11. VI міжнародна науково-практична конференція. «Проблеми кібербезпеки інформаційно-телекомунікаційних систем». 26 квітня 2024 р. м. Київ: форма участі – онлайн.

Додакток Б

Акти реалізації результатів досліджень

ЗАТВЕРДЖУЮ
Начальник Науково-методичного центру
кадрової політики Міністерства оборони України
кандидат військ.наук
старший науковий співробітник
полковник Ігор ПОЛОВІНКІН
«19» 10 2023 року

АКТ
про реалізацію результатів наукових досліджень
Лаптєва Сергія Олександровича

Комісія у складі: голови комісії – заступника начальника Центру з наукової роботи кандидата педагогічних наук полковника Тракалюка О.Л. та членів комісії: начальника науково-дослідного відділу (проблем психологічного вивчення особового складу) кандидата психологічних наук полковника Кузьменка М.Д., начальника науково-дослідного відділу (кадрової політики) полковника Федоровича В.В., наукового співробітника науково-дослідного відділу (проблем психологічного вивчення особового складу) кандидата історичних наук полковника Малюги В.М. склала зазначений акт в тому, що результати наукових досліджень Лаптєва Сергія Олександровича були застосовані в ході проведення досліджень з використанням поліграфа з персоналом Міністерства оборони України при розробці методу захисту персональної інформації з урахуванням специфіки соціальних мереж. Цей метод враховує визначення шкідливих впливів на параметри захисту інформації в соціальних мережах, який, на відміну від існуючих, відрізняється застосуванням системи диференційних рівнянь, які враховують комплексні параметри нападу,

що є певною перевагою розроблених математичних моделей забезпечення безпеки інформації в соціальних мережах. Зокрема, ефективність розробленої методики забезпечення захисту інформації в соціальних мережах полягає у визначенні стійкості системи захисту завдяки побудові фазових портретів системи захисту та ретельного аналізу перехідних процесів з метою виявлення впливів на систему захисту.

Голова комісії:
заступник начальника Центру
з наукової роботи
кандидат пед. наук
полковник Олег ТРАКАЛЮК

Члени комісії:
начальник науково-дослідного відділу
(проблем психологічного вивчення особового складу)
кандидат психол.наук
полковник Максим КУЗЬМЕНКО

начальник науково-дослідного відділу
(кадрової політики)
полковник Володимир ФЕДОРОВИЧ

науковий співробітник науково-дослідного відділу
(проблем психологічного вивчення особового складу)
кандидат іст. наук
полковник Валерій МАЛЮГА

ЗАТВЕРДЖУЮ

Заступник директора з наукової роботи
Інституту програмних систем НАН України
доктор технічних наук, професор

Віктор ШЕВЧЕНКО

АКТ
Впровадження результатів дисертаційної роботи
Лаптєва Сергія Олександровича

Комісія у складі:
заступник директора з загальних питань Гребенніков А.Б. (голова),
учений секретар к.т.н., с.н.с. Дергильова О.В.,
завідувач НДВ 23 к.е.н. Федоренко Р.М.

склала даний акт про те, що результати отримані у дисертаційному дослідженні аспіранта Лаптєва Сергія Олександровича реалізовані при розробці методу захисту персональної інформації у соціальній мережі, яка, на відміну від існуючих моделей враховує специфіку соціальних мереж. Дозволяє провести об'єктивну оцінку балансу між загрозами безпеки інформації та специфічними параметрами соціальної мережі, такими як параметр комплексної довіри, параметр розширення соціальних мереж, сильних та слабких зв'язків між користувачами та оцінки економічних витрат на захист персональної інформації у соціальної мережи.

Даний акт не є підставою для фінансових взаєморозрахунків.

Голова комісії: Гребенніков А.Б.

Члени комісії: Дергильова О.В.

Федоренко Р.М.

07.02.2023