[7]. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A Method for Decimal Number Recovery from its Residues Based on the Addition of the Product Modules. Proceedings of the 2019 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2019). V.1. 2019. pp. 13-17.
[8]. Kasianchuk M., Yakymenko I., Ivasiev S. High-Productivity Methods of Finding Residues Multidigital Numbers By Modulo, in Inżynier XXI Wieku: VI Międzynarodowa Konferencja studentow oraz doktorantow, 02.12.2016: monografia, 1st ed., Bielsko, Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2016, pp. 123-130. Chapter in monograph.
[9]. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. Cybernetics and Systems Analysis, 2014. Vol. 50, № 5. pp. 649-654.
[10]. Zhengbing Hu., Dychka I., Onai M., Bartkoviak A. The Analysis and Investigation of Multiplicative Inverse Searching Methods in the Ring of Integers Modulo M. International Journal of Intelligent Systems and Applications (IJISA), 2016. Vol. 8, №11. pp. 9-18.

ARITHMETIC OF ASYMMETRIC CRYPTOSYSTEMS IN THE FIELD OF COMPLEX NUMBERS

At the current stage of information technology development, there is a need to improve existing and develop new methods and means of increasing the productivity of asymmetric crypto-algorithms. The article develops the theoretical foundations of modular calculations and asymmetric cryptography in the complex numerical domain. The method of determining the complex and real residues based on the complex module is considered. Euclid's algorithm and its consequence for finding an inverse element in a complex numerical domain are considered. A comparison of the complexity of Euclid's algorithm for finding the inverse of the element when finding the smallest positive and absolutely smallest residues was made. An analogue of Euler's function in the complex numerical domain was searched and this function was used to find the inverse of a complex number. The restoration of a complex number using the Chinese remainder theorem is demonstrated. The considered modular calculations in the field of complex numbers can be used in the construction of new approaches to asymmetric encryption.

Keywords: asymmetric cryptosystem, complex number, Euclid's algorithm, Euler's function, residue number system.

Алілуйко Андрій Миколайович, к.фіз.-мат.н., доцент, доцент кафедри прикладної математики Західноукраїнського національного університету.
Andrii Aliluiko, Ph.D., associate professor, associate professor of the Department of Applied Mathematics, West Ukrainian National University.
E-mail: aliluyko82@gmail.com.
Orcid ID: 0000-0002-4650-9350.

Касянчук Михайло Миколайович, д.т.н., професор, професор кафедри кібербезпеки Західноукраїнського національного університету.
Mykhailo Kasianchuk, doctor of technical science, professor, professor of the Department of Cyber Security, West Ukrainian National University.
E-mail: kasyanchuk@ukr.net.
Orcid ID: 0000-0002-4469-8055.

DOI: 10.18372/2410-7840.26.18824
УДК 336.71:004.056

РОЗРОБКА МОДЕЛІ ЗАХИСТУ ОСОБИСТИХ ДАНИХ У СОЦІАЛЬНИХ МЕРЕЖАХ

Сергій Лаптєв

Десятки мільйонів людей по всьому світу щорічно стають жертвами крадіжок особистих даних. Користувачі мережі втрачають величезні гроші через шахраїв, які використовують їхні дані у незаконний спосіб, і жертвою цього може стати абсолютно будь-яка людина. Крадіжка особистих даних – це будь-який злочин, у якому зловмисник отримує дані іншої особи та використовує особистість жертви для шахрайства. Згідно з дослідженнями, в 2020 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 відомостями у Великобританії. Це найбільша кількість випадків шахрайства за останні 13 років. Тому проблема розробки та дослідження математичних моделей захисту особистих даних є дуже актуальною. Вирішенню завдання розробки моделі та дослідження стійкості системи захисту особистої інформації і присвячена робота. Важливим напрямком є слідкування за поведінкою динамічної системи захисту інформації. В роботі проаналізували, використовуючи методи якісної теорії диференціальних рівнянь, зокрема метод фазової площини, поведінку системи захисту інформації. За допомогою цього методу знаходять характеристики особливих точок, ізольованих замкнутих траєкторій і сепаратриси, що в свою чергу дозволяє оцінити динаміку дослі-

джуваної нелінійної динамічної системи в широкому діапазоні можливих початкових умов. Фазова площина ілюструю повне розмаїття можливих станів системи, й описує картину її динаміки. У роботі наведені результати моделювання, які доводять адекватність розробленої моделі. Підтверджують, що розроблена модель захисту особистих даних з урахуванням часу припинення атаки та призначених параметрах моделювання є стійкою. Використання методу фазової площини є новим методом для дослідження стійкості моделі захисту інформації.

***Ключові слова**: фазовий портрет, інформаційні технології нелінійна система, стійкість, конфіденційність, доступність , прогнозування, алгоритм.*

ВСТУП

Великий ринок для крадіжки особистих даних – це соціальні мережі. У соціальних мережах зберігається величезна кількість персональних та особистих даних користувачів, за якими полюють зловмисники. На даний момент соціальні мережі являють собою величезну базу даних з найрізноманітнішою інформацією про величезну кількість людей по всьому світу. Чим більше людина спілкується в соціальних мережах, тим більше інформації про нього можна зібрати без особливих зусиль [1].

Соціальна мережа (СМ) – соціальна структура, утворена індивідами або організаціями в якій підтримуються соціальні відносини. Вона відображає різноманітні зв'язки між ними через різноманітні соціальні взаємовідносини, починаючи з випадкових знайомств і закінчуючи тісними родинними зв'язками [2]. Соціальні мережі є одним із основних способів спілкування, пошуку зв'язків та обміну як загальнодоступною, так і конфіденційною інформацією. Соціальні мережі становлять дедалі більшу частку спільних мереж. Сама мережа набуває нових властивостей, виступаючи як самостійний фактор.

ПОСТАНОВКА ПРОБЛЕМИ

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 особливо загострюється через посилення цифрового гуманістичного характеру освіти, зростання ролі соціальних мереж у житті людини загалом.

Захист особистих (персональних) даних у сучасному інформаційному житті є чи не найважливішим аспектом у забезпеченні безпечного використання всіх можливостей сучасних технологій. Тому проблема дослідження параметрів соціальних мереж для подальшого їх використання у вирішенні завдань захисту інформації та особистих (персональних) даних є дуже актуальною.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Обмін структурними та тематичними даними потенційно дозволяє використовувати соціальні мережі для вирішення широкого кола питань інформаційної безпеки.

У роботах [3, 4] розглядаються соціальні мережі, які можуть відстежувати дії користувачів і контролювати дані для подальшого використання. Дослідження 45 соціальних мереж показало, що приблизно 90% сайтів необґрунтовано вимагають особисту інформацію, наприклад, щоб отримати дозвіл на приєднання до них; 85 % сайтів не використовують стандартні протоколи шифрування для захисту даних від атак кіберзлочинців; 72% сайтів передають інформацію про користувачів третім особам.

У роботах [5, 6] розглянуто стандарти, атрибути та характеристики профілю та запропоновано метод виявлення ознак маніпулювання громадською думкою в соціальних мережах на основі побудови профілів інформаційної безпеки соціальних Інтернет-сервісів на основі градієнтного підвищення бінарних дерев, які автоматизує процедури раннього виявлення.

У роботі [7] вказується, що поширення персональних даних через соціальні мережі відбувається набагато швидше, ніж у реальному житті. Найбільш небезпечно, коли особиста інформація потрапляє до людей, для яких вона не призначена. Користувачі соціальних мереж часто не знають, що вони можуть змінити особисті налаштування конфіденційності, щоб захистити свої дані.

У роботі [8] розглянуто механізм застосування кореляції потенційних кризових ситуацій для оцінки середнього та сумарного рівня критичності поточної ситуації в інформаційній сфері. Механізм базується на методах експертної оцінки та нечіткої логіки. Запропоновано кореляційний механізм визначення коефіцієнта кореляції кожної залежної ідентифікації потенційних кризових ситуацій з основною, що визначає взаємозалежності між ними. Отримані коефіцієнти кореляції можуть бути використані для розрахунку середнього та сумарного рівнів критичності ситуації,

що виникла під впливом кількох взаємопов'язаних та одночасних потенційних кризових ситуацій. Розглянуто лише задачі кореляції інформації.

У роботі [9] розроблено структурно-параметричну модель системи оцінки ризиків інформаційної безпеки, яка за рахунок структурних складових підсистем формування первинних і вторинних даних, а також їх складових модулів ініціалізації вхідних даних, формування та перетворення еталонних значень, зважування параметрів оцінки та їх коригування, оцінка ризиків та формування звітів, які реалізують запропоновані методи, оцінка на основі баз даних уразливостей, збільшення та зменшення порядку лінгвістичних змінних, забезпечує високу гнучкість та зручність оцінювання інформаційної безпеки ризики без участі фахівців у предметній області. Але розглядаються лише ті проблеми інформаційної безпеки, які представлені в локальних базах даних.

У роботі [10] запропоновано якісно-кількісний метод аналізу та оцінки ризиків інформаційної безпеки шляхом модифікації процедур визначення багатьох параметрів оцінки ризиків та оцінки поточних значень параметрів з можливістю інтеграції значень показників, представлених у відповідних базах даних. Для цього пропонується використовувати відповідні бази даних вразливостей, в яких представлені їх кількісні оцінки. У роботі [11] розглядаються лише питання інформаційної безпеки, які представлені в базах даних показників CVSS.

У роботі [12] розглянуто методологію побудови системи інформаційної безпеки банківської інформації в автоматизованих банківських системах (АБС), яка базується на запропонованій вперше трирівневій моделі стратегічного управління безпекою інформаційних технологій.

У роботі [13] розглядаються лише проблеми інформаційної безпеки без урахування технічних проблем.

Разом з тим, незважаючи на значну кількість публікацій щодо вирішення різних аспектів підвищення захищеності особистих даних, стає очевидним що процес захисту особистих даних потребує удосконалення. Тому актуальним науковим завданням є дослідження всієї сукупності параметрів загроз у соціальних мережах для вирішення завдань захисту особистих даних користувачів.

МЕТА РОБОТИ

Для вирішення наукового завдання з дослідження параметрів загроз даним що зберігаються у соціальних мережах для вирішення завдань захисту особистих даних користувачів треба вирішити наступні часткові завдання:

-розробити модель захисту особистих даних у соціальних мережах зі урахуванням параметру запізнення реагування на атаку з метою подолання її наслідків;

-дослідити розроблену модель методом фазової площині на предмет стійкості до атак.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Послуги соціальних мереж кардинально еволюціонують у взаємодії між людьми, стаючи сьогодні фактично переважним сервісом в Інтернеті [14].

Основна інформація, що зберігається в Інтернет–соціальних мережах (ІСМ), це самостійно генеровані та підтримувані дані користувачів та їхніх відвідувачів можна класифікувати на наступні типи [15]:

- особисті контактні дані, що описують особу користувача;
- підключення, що представляє з'єднання в трафіку соціальної мережі;
- інтереси користувача;
- інформація про автобіографію користувача;
- спілкування, включаючи всі взаємодії з іншими користувачами ІСМ через сервіс посилки повідомлень (СПП).

СПП – сервіс посилки повідомлень між мережевими компонентами Web Services і зовнішніми компонентами. Забезпечує масову доставку повідомлень в складній мережі. Користувачам ІСМ зазвичай дозволено визначати власні налаштування конфіденційності через деякі функції контролю доступу. Зокрема, користувач ІСМ може контролювати видимість присутності іншого користувача в мережі в межах ІСМ; видимість контактів із його списку контактів; видимість та доступ до його власної професійної інформації; доступ до власного завантаженого вмісту та розміщених повідомлень. Усі ці функції зазвичай беруть за вхід інформацію, що підлягає захисту, і список постачальників, які мають права на доступ до неї. Відвідувачі можуть бути об'єднані в загальні групи, такі як "друзі", "друзі друзів", "всі" або групи, визначені користувачем, такі як "члени сім'ї", "колеги" [15].

Проблему конфіденційності даних користувачів можна визначити як проблему контролю використання: контроль використання забезпечує контроль доступу разом з додатковим контролем щодо подальшого використання даних, навіть коли інформація вже доступна. Доступ до вмісту

користувальницької програми може бути наданий тільки користувачем безпосередньо, і це управління доступом повинно бути таким же надійним, як і сама програма.

Але вказаного недостатньо для забезпечення конфіденційності приватної особи. Наприклад, якщо програма містить кілька інформаційних блоків, то доступ до кожного блоку повинен управлятися окремо. Крім того, конфіденційність зв'язку вимагає методів, спрямованих на отримання будь-якого типу інформації стосовно:

- анонімності, тобто користувачі повинні отримувати доступ до ресурсів чи послуг, не розкриваючи власну особу;
- незабезпеченість, тобто вимога, 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 або тим самим одержувачем;
- непростежуваність, яка вимагає, що жодна третя сторона не може мати історію дій, що виконуються довільними користувачами в системі; Іншими словами, вона вимагає як анонімності, так і непов'язаності.

Щоб передбачити охоплення та тривалість нападу на персональні дані, треба звернутись до моделювання передачі вірусу – шкідливого коду у мережи суспільстві. Моделі можуть бути різною мірою детальними. Деякі з них описують лише зараження та відбій атаки на базу зберігання особистих даних. Інші моделі враховують додаткові фактори, такі як наявність бази шкідливих кодів, яка накопичується зі часом. Тому детальність моделі залежить від атаки на базу особистих даних, атаку поширення якої треба припинити системою захисту даних.

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 розповсюджується (E), після де якого 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:

•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 розробляють 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 (вірус) у момент часу t, y(t) – функція яка описує поведінку об'єкта також у момент часу t.

Визначимо функцію для нападника:

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

Функція (1) відповідає за успішний напад на об'єкт. Для пояснення рівняння розкладемо функцію на складові:

$$f(t)=\frac{c\cdot x(t)\cdot y(t)}{(1+dx(t))}=\frac{c\cdot y(t)}{d(1+x(t))}+\frac{c\cdot y(t)}{dt}. \quad (2)$$

Перша складова виразу (2) $\frac{c\cdot y(t)}{dt}$ буде відповідати за кількість нападників (вірусів), друга складова $\frac{c\cdot y(t)}{d(1+x(t))}$ буде відповідати за ліквідування нападників (вірусів). Обидві складові описують взаємодію Нападник (Вірус) – Об'єкт.

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

$$\begin{cases}\frac{dx(t)}{dt}=-k_1\cdot x(t)-b\cdot x(t)y(t)+a_1\cdot(t-\Delta t_1)\\ \frac{dy(t)}{dt}=-k_2\cdot y(t)-\frac{c\cdot y(t)}{d(1+x(t))}+\frac{c\cdot y(t-\Delta t_2)}{dt}\end{cases}, \quad (3)$$

де Δt_1 – час необхідний для підготовки нападу (створення вірусу); Δt_2 – час необхідний для підготовки систем захисту; $(t-\Delta t_1)$ –кількість можливих варіантів нападу (вірусів) 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, тоб то щоб любе збурення, любий напад не міг вивести систему з рівноваги (робочого стану). Інакше кажучи що система була стійкою. З цей метою проаналізуємо систему рівнянь (3) на стійкість. Для цього розкладемо $x(t-\Delta t_1)$ та $y(t-\Delta t_2)$ у ряд Тейлора з зберіганням тільки лілейних членів за Δt_1 та Δt_2, підставимо ряди які ми отримали у систему рівнянь, отримуємо:

$$\begin{cases}\frac{dx(t)}{dt}(1+a_1\Delta t_1)=-k_1\cdot x(t)-b\cdot x(t)y(t)+a_1\cdot x(t)\\ \frac{dy(t)}{dt}(1+\frac{c}{d}\Delta t_2)=-k_2\cdot y(t)-\frac{c\cdot y(t)}{d\cdot(1+x(t))}+\frac{c\cdot y(t)}{dt}\end{cases}. \quad (4)$$

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

$$\begin{cases}\frac{dx(t)}{dt}K_1=-k_1\cdot(\tilde{x}+x_0)-b\cdot(\tilde{x}+x_0)\times\\ \times(\tilde{y}+y_0)+a_1\cdot(\tilde{x}+x_0)\\ \frac{dy(t)}{dt}K_2=-k_2\cdot(\tilde{y}+y_0)-\frac{c\cdot(\tilde{y}+y_0)}{d\cdot(1+d\cdot(\tilde{x}+x_0))}+\\ +\frac{c\cdot(\tilde{y}+y_0)}{dt}\end{cases}, \quad (5)$$

де $K_1=(1+a_1\Delta t_1)$, $K_2=(1+\frac{c}{d}\Delta t_2)$-постійні коефіцієнти.

Після перетворень отримуємо систему:

$$\begin{cases}\frac{d\tilde{x}(t)}{dt}K_1=\tilde{x}\cdot(-k_1\cdot-b\cdot y_0+a_1)-b\cdot x_0\cdot\tilde{y}\\ \frac{d\tilde{y}(t)}{dt}K_2=\tilde{y}\cdot(\frac{c}{d}-k_2-\frac{c}{d\cdot(1+d\cdot x_0)})+\\ +\tilde{x}\cdot\frac{c\cdot y_0}{(1+d\cdot x_0)^2}\end{cases}. \quad (6)$$

Система диференціальних рівнянь є розробленою моделлю захисту персональних даних у соціальних мережах. Вона є системою диференціальних рівнянь з запізненням.

Диференціальне рівняння, що описує поведінку динамічної системи, звичайно залежить від одного або декількох параметрів. Зміна цих параметрів буде, взагалі кажучи, призводити до зміни фазового портрету.

Побудуємо фазові портрети системи (6) при різних значеннях постійних коефіцієнтів K1, K2, k1, k2, b, c, a1, d, та визначим стійкість системи. (рис. 1) для даних (табл. 1).

Таблиця 1

Значення постійних коефіцієнтів

KK1	KK2	kk1	kk2	bb	cc	aa1	dd
11	11	11	22	11	55	33	22

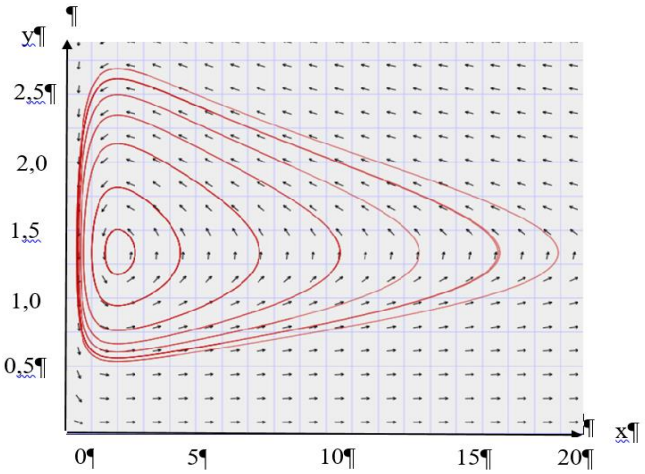

Рис.1. Фазовий портрет системи диференціальних рівнянь з запізненням, для параметрів наведених у табл.1

Аналогічно, приведемо рисунок (рис. 2) для наведених даних (табл. 2).

Таблиця 2

Значення постійних коефіцієнтів

KK1	KK2	kk1	kk2	bb	cc	aa1	dd
11	11	11	11	33.5	22.5	33	11.5

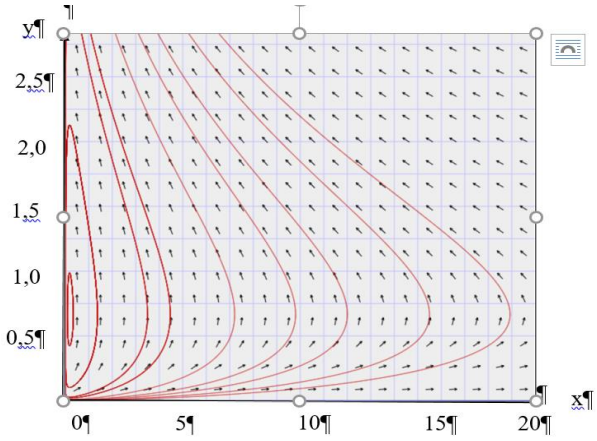

Рис.2. Фазовий портрет системи диференціальних рівнянь з запізненням, для параметрів наведених у табл.2

Аналіз фазових портретів системи диференціальних рівнянь з запізненням, дозволяє зробити висновок, що система стійка.

Варто зазначити, що поведінку динамічної системи зручно аналізувати використовуючи методи якісної теорії диференціальних рівнянь, зокрема званий метод фазової площини. Зазвичай метод фазової площини застосовують для дослідження нелінійних систем, у випадках, коли лінеаризація призводить до незадовільних помилок, або коли лінеаризація значно обмежена в застосовності за часом.

За допомогою цього методу знаходять характеристики особливих точок, ізольованих замкнутих траєкторій і сепаратриси, що в свою чергу дозволяє оцінити динаміку досліджуваної нелінійної динамічної системи в широкому діапазоні можливих початкових умов.

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 значеннями: координати і швидкості; воно може бути представлено у плоскій декартовій системі координат відповідною точкою. Таку точку називають зображуючою точкою, а площину – фазовою площиною.

При рухи системи величини змінюються, а отже, зображуюча точка буде змінювати своє положення на фазовій площині. Геометричне місце зображуючих точок для заданого руху називається фазовою траєкторією. Сукупність усіх можливих фазових траєкторій системи називають її фазовим портретом.

Взагалі, структура фазових траєкторій дає тільки якісні особливості можливих рухів системи, але показує ряд найбільш характерних її властивостей.

У якісної теорії диференціальних рівнянь встановлюється, що через кожну точку фазової площини проходить одна і лише одна фазова траєкторія, за винятком тих точок, в яких похідна не визначена. Тобто фазова площина ілюструю повне розмаїття можливих станів системи, й описує картину її динаміки.

ВИСНОВКИ

Удосконалено метод виявлення неправдивої інформації на основі методу експертної оцінки. Запропонований метод експертних оцінок має безсумнівні переваги в порівнянні з методами, заснованими на звичайній статистичній обробці результатів індивідуальних опитувань. На відміну від існуючого підходу, удосконалений метод дозволяє проводити ретельний відбір експертів. За допомогою двох критеріїв: самооцінки експерта та оцінки експерта робочою групою. Це дозволяє значно зменшити похибку оцінки експерта.

Отримання об'єктивної правдивої інформації досягається можливістю встановлювати інтервал довіри до оцінки інформації.

Проте удосконалений метод має і ряд недоліків. Серед них, вирішення проблеми оптимізації завдання, якщо інтервал довіри буде загально великим, тоді часу на завершення оцінки треба менше, але при цьому точність буде значно мен-

ше і навпаки коли інтервал довіри до оцінки буде малим, треба багато часу, що теж не є сприятливим. Тобто напрямком подальших досліджень є завдання оптимізації критеріїв оцінки.

ЛІТЕРАТУРА

[1]. 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. pp. 31-35.

[2]. 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): pp. 19-28. DOI: https://doi.org/10.28925/2663-4023.2021.12.1928.

[3]. 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.

[4]. 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.

[5]. 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.

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

[7]. O.Laptiev, V.Savchenko, A. Kotenko, V.Akhramovych, V.Samosyuk, G.Shuklin, A.Biehun. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp. 15-21. https://www.ijcnis.org/index.php/ijcnis/article/view/4882.

[8]. S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. Synergy of building cybersecurity systems: monograph / Edited by– Kharkiv: PC TECHNOLOGY CENTER, 2021. 188 p. http://monograph.com.ua/pctc/catalog/book/64.

[9]. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. К.: Інтертехнологія, 2009. 164 с.

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

[11]. 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.No. 2, February2020, pp. 271-276. http://www.warse.org/IJETER/static/pdf/file/ijeter05822020.pdf.

[12]. Yang Jaewon, Leskovec Jure. Defining and evaluating network communities based on ground–truth // Knowledge and Information Systems. 2015. Т. 42, № 1. pp. 181-213.

[13]. Thomas Paul, Sonja Buchegger, and Thorsten Strufe. Decentralizing social networking services. In International Tyrrhenian Workshop on Digital Communications, ITWDC 2015, pp. 1-10, Island of Ponza, Italy, September 2015.

[14]. Лукова-Чуйко Н.В., Лаптєв О.А., Барабаш О.В., Мусієнко А.П., Ахрамович В.М. Метод розрахунку захисту персональних даних з урахуванням комплексу специфічних параметрів соціальних мереж. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ, 2022. № 76. С. 54-68. https: // doi.org / 10.17721 / 2519-481X/2022/76-05.

[15]. Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, Вип. 64, 2019. С. 124-132.

DEVELOPMENT OF A MODEL FOR THE PROTECTION OF PERSONAL DATA IN SOCIAL NETWORKS

Tens of millions of people around the world become victims of identity 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. Identity theft is any crime in which an attacker obtains another person's data and uses the victim's identity to commit fraud. According to research, data theft caused $16 billion in losses to 15.4 million consumers in the United States in 2020. In the same year, the British fraud prevention organization Cifas recorded almost 173,000 cases of identity fraud in the UK. This is the largest number of fraud cases in the last 13 years. Therefore, the problem of developing and researching mathematical models of personal data protection is very relevant. The work is devoted to solving the task of developing a model and researching the stability of the personal information protection system. Monitoring the behavior of the dynamic information protection system is an important direction. The paper analyzed the behavior of the information protection system using the methods of the qualitative theory of differential equations, in particular the

phase plane method. With the help of this method, the characteristics of special points, isolated closed trajectories and separatrices are found, which in turn allows to evaluate the dynamics of the studied nonlinear dynamic system in a wide range of possible initial conditions. The phase plane illustrates the full variety of possible states of the system, and describes the picture of its dynamics. The paper presents simulation results that prove the adequacy of the developed model. It is confirmed that the developed model of personal data protection is stable, taking into account the attack termination time and the assigned modeling parameters. Using the phase plane method is a new method for researching the stability of the information protection model.

Keywords: phase portrait, information technologies, nonlinear system, stability, confidentiality, availability, forecasting, algorithm.

Лаптєв Сергій Олександрович, аспірант кафедри кібербезпеки та захисту інформації, Факультет інформаційних технологій, Київський національний університет імені Тараса Шевченка, Київ, Україна

Serhii Laptiev, PhD student of the department of cyber security and information protection, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
E-mail: salaptiev@gmail.com.
Orcid ID: 0000-0002-7291-1829.

DOI: 10.18372/2410-7840.26.18826
УДК 004.056(477)

МЕТОДИЧИЙ ПІДХІД ДЛЯ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТРУРИ В УМОВАХ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Володимир Шиповський

В ході широкомасштабного вторгнення російської федерації на територію України, вагоме місце займають деструктивні кібервпливи з боку російських кібервійськ на критичну інфраструктуру держави. Цілями Кібератак є не лише військові об'єкти, а й цивільні об'єкти критичної інфраструктури України. Такі дії мають на меті підрив морального духу населення країни та нанесення значної шкоди економіці країни. Відповіддю на це є необхідність розробки ефективних методів кіберзахисту об'єктів критичної інфраструктури (далі – ОКІ) та удосконалення інструментів оцінювання кіберстійкості цих об'єктів, з метою забезпечення їх захисту та оперативного відновлення після можливих атак. Представлена стаття фокусується на розробці методики оцінювання кіберстійкості ОКІ в умовах загроз національній безпеці держави з метою створення сприятливих умов для запобігання та своєчасного реагування на деструктивні кібервпливи з боку ворога та містить рекомендації щодо оцінювання кіберстійкості інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури. Методика включає в себе розрахунки з використанням теорії ймовірності та методичних рекомендацій, затверджених державними органами України, для категоризації об'єктів критичної інфраструктури з метою оцінювання їх критичності. Методика призначена для оперативного виявлення потенційних цілей ворога та удосконалення рівня кіберзахисту ОКІ у визначеному регіоні країни.

***Ключові слова**: кіберзахист, кіберстійкість, кібероборона, інформаційні системи, кіберзахищеність, інформаційно-телекомунікаційні системи, стійкість, об'єкти критичної інфраструктури, оцінювання, технологія, безпека мереж, національна безпека, гібридні загрози, оцінка, методичний підхід, методика, система, загрози національній безпеці, моделювання, математична модель.*

ВСТУП.

З моменту початку повномасштабного вторгнення Росії у лютому 2022 року ми стали свідками декількох інновацій у веденні війни, коли безпілотні засоби в повітрі, на землі та на морі змінили підходи до розвідки та тактичних і оперативних бойових дій. Проте, російсько-українська війна не перетворилася на науково-фантастичне протистояння між автоматизованими роботизованими системами. Однак, інформаційні технології трансформували природу війни і продовжують це робити. Військові доктрини та правила ведення бойових дій, що були розроблені раніше, потребують оновлення відповідно до сьогоднішніх і майбутніх викликів.

Інтеграція інформаційних технологій зі збройною боротьбою не лише змінила арсенал наявної зброї, але й розмила межі між фізичним та кіберпростором. Традиційні військові арсенали, що раніше складалися з танків, літаків та піхоти, тепер доповнені потужними кіберзасобами. Сучасні ландшафти кібератак дозволяють проникати в інформаційні системи як військових об'єктів, так і критичної інфраструктури держави, значно розширюючи можливості впливу. Урядовою командою реагування на комп'ютерні надзвичай-