ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ / PRIVACY & PROTECTION FROM IDENTITY THEFT

DOI: 10.18372/2225-5036.28.17371

УДОСКОНАЛЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ЗАХИЩЕНОСТІ ОСОБИСТИХ ДАНИХ ЗА РАХУНОК ВРАХУВАННЯ ДОВІРИ ТА КІЛЬКІСТІ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Толюпа Сергій, Лаптєв Сергій

Київський національний університет імені Тараса Шевченка

ТОЛЮПА Сергій Васильович, д.т.н., професор
Рік та місце народження: 1961 рік, село Варовичи, Київська область, Україна.
Освіта: КВІРТУ ППО, 1986 рік.
Посада: професор кафедри кібербезпеки та захисту інформації.
Київського національного університету імені Тараса Шевченка.
Наукові інтереси: кібербезпека, протидія інформаційним впливам, комплексні системи захисту інформації.
E-mail: serhii.toliupa@knu.ua.
ORCID ID: 0000-0002-1919-9174.

ЛАПТЄВ Сергій Олександрович, аспірант
*Рік та місце народження:*1985 рік, м. Київ, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, 2018 рік.
Посада: Аспірант Кафедра кібербезпеки та захисту інформації Київський національний університет імені Тараса Шевченка, Факультет інформаційних технологій.
Наукові інтереси: кібербезпека, протидія інформаційним впливам, комплексні системи захисту інформації.
E-mail: salaptiev@gmail.com.
ORCID ID: 0000-0002-7291-1829.

Анотація. *Інформація потребує постійного надійного захисту. Захисту від несанкціонованого доступу і поширення, випадкового видалення або зміни. Всі розвинені країни Європи стурбовані проблемою інформаційної безпеки, а також захистом особистих даних громадян країни. Соціальні мережі є одним з основних методів комунікацій, пошуку зв'язків та обміну як загальнодоступною, так і особистою інформацією. Соціальні мережі, становлять постійно зростаючу частку серед загальних мереж. Сама мережа набуває нових властивостей, діючи як самостійний фактор. Тому постійно потрібно розробляти систему захисту інформації, особливо захист особистих даних у соціальної мережи. У роботі проведено аналіз параметрів соціальних мереж. Параметрами соціальної мережи є передача інформації іншим користувачам, щільність трафіку, ймовірність побудови безпечної мережі та інші. Розроблено математична модель визначення захищеності особистих даних від довіри та кількості інформації в соціальних мережах. Проведено математичне моделювання у середовище MatLab, моделювання довело, що виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненційним загасаючим законом. Тобто захист особистих даних зростає від зростання факторів довіри до інформації. Математичне моделювання запропонованої моделі, моделі яка визначає залежність захисту*

особистих даних від довіри та кількості інформації, підтвердило адекватність розробленій моделі та довело, що захист особистих даних пропорційний довірі. Захист особистих даних зростає із ростом параметрів довіри. Але захист особистих даних незначно зменшується зі зростанням кількості інформації, яку потрібно захищати. Це цілком відповідає реальної ситуації та підтверджує адекватність розробленій моделі.

Ключові слова: *соціальна мережа, довіра, кількість інформації, особисті дані, математична модель.*

Постановка проблеми

У сучасному світі інформація потребує надійного захисту: від несанкціонованого доступу і поширення, випадкового видалення або зміни. Всі розвинені країни Європи стурбовані проблемою інформаційної безпеки, а також захистом персональних даних громадян країни. Це обумовлено тим, що інформатизація і оцифровка інформації набули широкого поширення у всіх сферах діяльності людини, в тому числі і зберіганні особистих і робочих даних. Соціальні мережі є одним з основних методів комунікацій, пошуку зв'язків та обміну як загальнодоступною, так і конфіденційною інформацією. До конфіденційної інформації можливо віднести персональні дані користувачів. Соціальні мережі, становлять постійно зростаючу частку серед загальних мереж. Сама мережа набуває нових властивостей, діючи як самостійний фактор.

Оскільки інформація в глобальній мережі існує постійно, сама мережа стає активним агентом впливу на людину, зберігаючи, насамперед, загальнодоступними великі обсяги інформаційних даних. За останні роки почало суттєво змінюватись бачення проблеми кібербезпеки, оскільки людина дедалі більше перестає бути лише суб'єктом кіберзлочинів, перетворюючись на об'єкт сама по собі, а не тільки її фінансові та економічні інтереси та можливості. Об'єктом нападу стають особисті дані користувачів соціальних мереж.

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

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

Обмін особистими даними потенційно дозволяє використовувати соціальні мережі для вирішення широкого кола інформаційних проблем, але виникає проблема захисту даних. Тому питання розробки нових математичних моделей оцінки залежності захисту персональних даних від довіри та кількості інформації в соціальних мережах є дуже актуальним.

Метою даного дослідження є розробка нової математичної моделі оцінки залежності захисту персональних даних від довіри та кількості інформації в соціальних мережах.

Аналіз останніх досліджень і публікацій

Обмін структурними та тематичними даними потенційно дозволяє використовувати соціальні мережі для вирішення широкого кола проблем інформації для захисту даних.

У статті [1] розглядаються соціальні мережі, які можуть відстежувати дії користувачів та контролювати дані для майбутнього використання. Дослідження 45-ти соціальних мереж, виявило, що приблизно 90% сайтів необґрунтовано вимагають вказувати персональну інформацію для, наприклад, надання дозволу приєднатися до них; 85% сайтів не використовують стандартні протоколи шифрування для захисту даних від атак кіберзлочинців; 72% сайтів здійснюють передачу інформації про користувачів стороннім особам.

У статті [2] розглянуто стандарти, атрибути і характеристики профілю та запропоновано метод виявлення ознак маніпуляцій суспільною думкою у соціальних мережах на основі побудови профілів інформаційної безпеки соціальних інтернет-сервісів, який ґрунтується на градієнтному бустингу бінарних дерев, що дозволило автоматизувати процедури раннього виявлення загроз.

У статтях [3-5] вказується, що поширення персональних даних через соціальні мережі відбувається значно швидше, ніж у реальному житті. Найбільш небезпечно, коли особиста інформація надходить до людей, для яких вона не призначена. Користувачі соціальних мереж часто не знають, що вони можуть змінити персональні параметри конфіденційності, щоб захистити свої дані.

У статті [7] розглянуто механізм застосування кореляції потенційних кризових ситуацій для оцінювання середнього та сумарного рівня критичності поточної ситуації в інформаційній сфері. Механізм заснований на методах експертного оцінювання та нечіткої логіки. Запропонований механізм кореляції з визначенням коефіцієнта кореляції кожної залежної ідентифікації потенційних кризових ситуацій з основним, що визначають взаємозалежності між ними. Отримані коефіцієнти кореляції можуть бути використані для обчислення середнього та сумарного рівнів критичності ситуації, що виникла під впливом декількох взаємопов'язаних і

одночасних потенційних кризових ситуацій. Розглянуто тільки проблеми кореляції інформації.

У статтях [8-9] розроблено структурно-параметричну модель системи оцінювання ризиків інформаційної безпеки яка, за рахунок структурних компонент підсистем, формування первинних і вторинних даних, а також складових їх модулів ініціалізації вхідних даних, формування і перетворення еталонних значень, зважування оціночних параметрів і їх коригування, оцінювання ризиків і генерації звіту, в яких реалізовані запропоновані методи, оцінювання на основі баз даних вразливостей, інкрементування і декрементування порядку лінгвістичних змінних, дозволяє забезпечити високу гнучкість і зручність при оцінювання ризиків інформаційної безпеки без участі експертів відповідної предметної області. Але розглянуто тільки проблеми безпеки інформації, які представлені у локальних базах .

У статті [9] розглянуто якісно-кількісний метод аналізу і оцінювання ризиків інформаційної безпеки за рахунок модифікації процедур визначення безлічі параметрів оцінювання ризику і оцінки поточних значень параметрів з можливістю інтеграції значень показників, які представлені у відповідних базах даних. Для цього пропонується використовувати відповідні бази даних вразливостей, в яких представлені їх кількісні оцінки. У статті [9] розглянуто тільки проблеми безпеки інформації, які представлені в базах значень показників CVSS.

У статтях [10-11] розглянута методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах (АБС), яка ґрунтується на вперше запропонованій трирівневої моделі стратегічного управління безпекою інформаційних технологій. У статтях [10-11] розглянуто тільки проблеми безпеки інформації, без урахування технічних проблем.

Разом з тим, незважаючи на значну кількість публікацій щодо вирішення захисту інформації від різноманітних аспектів атак на особисті дані в умовах цифрового суспільства на сьогоднішній день залишається невирішеною проблема комплексного захисту особистих даних з урахуванням параметрів соціальної мережи.

Тому захист особистих даних з урахуванням параметрів соціальної мережи в умовах інформатизації суспільства є актуальним знаковим завданням.

Виклад основного матеріалу дослідження

У класичному підході до проблеми захисту особистих даних розрізняють множину загроз від втрати довіри між користувачами, яку можна представити у вигляді функції:

$$T_i = F(\left[D_j, D_n, D_m, D_k \right]), \quad (1)$$

де: T_i – множина загроз від втрати довіри між користувачами; D_j – довіра до надання послуг (людина довіряє стороні в наданні провайдером якісних послуг або ресурсів); D_n – довіра делегування (delegation trust) описує довіру в користувача (представника), що діє і виносить рішення від імені сторони, якій довіряє; D_m – довіра доступу (access trust) описує довіру зі сторони (провайдера) до користувача, якому надається доступ до ресурсів. Це – контроль доступу. Використовується в системах автентифікації; D_k – контекстна довіра визначає міру віри учасника в необхідні системи та інституційні механізми, що підтримують транзакції і забезпечують безпеку мережі.

Втрата такої якості, як довіра – процес, який має часовий інтервал. Втрата довіри це процес повного блокування обміну інформації.

Позначимо кількість інформації в системі – I. Потік інформації за межі інформаційної системи через *dI* –, швидкість зміни цього потоку – $\frac{dI}{dt}$. Логічне, що якщо потік і швидкість зміни потоку дорівнюють нулю, то витоку інформації немає:

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

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

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_v + C_k) I - L_2 (I_0^2 \sin^2 \omega t) - \\ - L_3 (I_0^3 \sin^3 \omega t) - \dots \\ \frac{dZ}{dt} = D_i - I (C_{d1} + C_{d2}) - K_2 (Z_0^2 \sin^2 \omega t) - \\ - K_3 (Z_0^3 \sin^3 \omega t) - \dots . \end{cases} \quad (3)$$

Для рішення системи рівнянь (3) представимо систему (3) у вигляді:

$$\begin{cases} \frac{dI}{dt} = \alpha Z + \beta_1 I - \sum_{k=2}^{\infty} L_k I_0^k \sin^k \omega t \\ \frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \end{cases}, \quad (4)$$

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

Далі використовуємо метод виключення:

$$\frac{dZ}{dt} = \beta_2 I + \gamma - \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \Rightarrow$$

$$I = \frac{1}{\beta_2} \left(\frac{dZ}{dt} - \gamma + \sum_{k=2}^{\infty} K_k Z_0^k \sin^k \omega t \right) \Rightarrow$$

$$\frac{dI}{dt} = \frac{1}{\beta_2} \left(\frac{d^2 Z}{dt^2} + \frac{1}{\omega} \sum_{k=2}^{\infty} \left(k K_k Z_0^k \sin^{k-1} \omega t \cos \omega t \right) \right). \quad (5)$$

Підставляємо у перше рівняння системи:

$$\frac{1}{\beta_2}\left(\frac{d^2Z}{dt^2}+\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)\right)=$$
$$=\alpha Z+\frac{\beta_1}{\beta_2}\left(\frac{dZ}{dt}-\gamma+\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t\right)- \quad (6)$$
$$-\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t \quad \text{або}$$
$$\frac{d^2Z}{dt^2}-\beta_1\frac{dZ}{dt}-\alpha\beta_2Z=$$
$$-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1\gamma+ \quad (7)$$
$$+\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t.$$

Знайдемо рішення відповідного рівняння:

$$Z''-\beta_1Z'-\alpha\beta_2Z=0. \quad (8)$$

Характеристичне рівняння має вигляд: $\lambda^2-\beta_1\lambda-\alpha\beta_2=0$.

Будемо розглядати тільки випадок для позитивного дискримінанта цього рівняння:

$$D=\beta_1^2+4\alpha\beta_2>0\Rightarrow\lambda_{1,2}=\frac{\beta_1\pm\sqrt{\beta_1^2+4\alpha\beta_2}}{2}$$

та

$Z_{оди}(t)=c_1e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+c_2e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}$ – загальне рішення рівняння (8).

Для знаходження загального рішення неоднорідного рівняння скористаємось методом варіації призвільних постоялих:

$$Z_{оди}(t)=c_1(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+c_2(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}, \quad (9)$$

де $c_1'(t),c_2'(t)$ будуть знайдені з системи:

$$\begin{cases}c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=0,\\ c_1'(t)\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}+\\ +c_2'(t)\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=N(t),\end{cases} \quad (10)$$

де

$$N(t)=-\frac{1}{\omega}\sum_{k=2}^{\infty}\left(kK_kZ_0^k\sin^{k-1}\omega t\cos\omega t\right)-\beta_1\gamma+$$
$$\beta_1\sum_{k=2}^{\infty}K_kZ_0^k\sin^k\omega t-\beta_2\sum_{k=2}^{\infty}L_kI_0^k\sin^k\omega t. \quad (11)$$

Отримаємо:

$$c_1'(t)e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}=-c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\Rightarrow$$
$$\Rightarrow c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\times$$
$$\times\left(-\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}+\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}\right)=N(t), \quad (12)$$

або

$$c_2'(t)e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}\sqrt{\beta_1^2+4\alpha\beta_2}=-N(t). \quad (13)$$

Тоді отримаємо:

$$c_2(t)=-\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt \quad (14)$$

та

$$c_1(t)=\frac{1}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt. \quad (15)$$

Математична модель у кінцевому вигляді буде мати вигляд:

$$Z(t)=\frac{e^{\frac{\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt-$$
$$-\frac{e^{\frac{\beta_1-\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}}{\sqrt{\beta_1^2+4\alpha\beta_2}}\int N(t)e^{\frac{-\beta_1+\sqrt{\beta_1^2+4\alpha\beta_2}}{2}t}dt. \quad (16)$$

У цілому ми отримали результати, у загальному вигляді: залежність захисту особистих даних від довіри пропорційна при постійних параметрах захисту інформаційної мережі.

З метою підтвердження отриманих результатів проведемо моделювання у середовище MatLab.

На рис. 1. наведено залежність захисту персональних даних (у відносних одиницях) від кількості інформації у системи – основний параметр, та параметра довіри до інформації

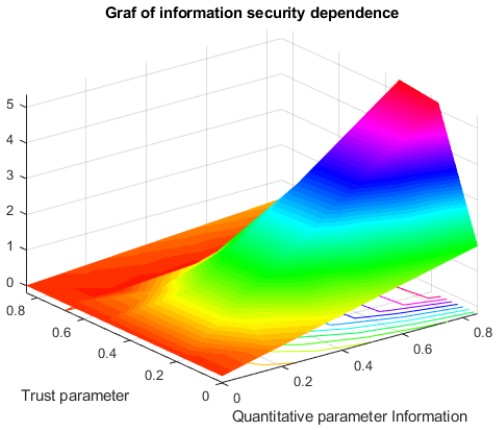

Рис. 1. Залежність захисту особистих даних від зростання кількості інформації в системі

На рис. 2 наведено залежність захисту особистих даних (у відносних одиницях) від параметра довіри до інформації – основний параметр, та кількості інформації у системи.

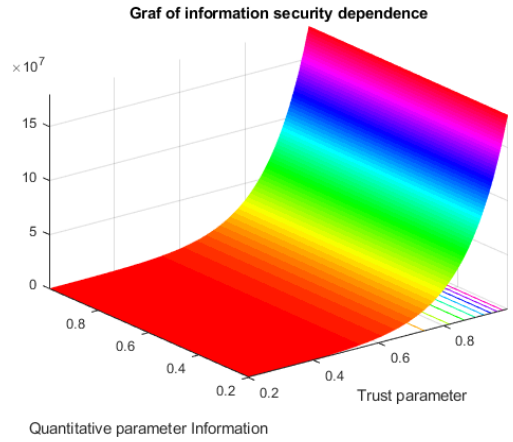

Рис. 2. Залежність захисту особистих даних від довіри між користувачами

Як бачимо з результатів моделювання. Захист персональних даних, напряму залежить від кількості інформації та параметрів довіри до цій інформації. Захист особистих даних зростає зі зростанням кількості достовірної інформації та кількості загальної інформації. Що цілком підтверджує адекватність запропонованого методу оцінки захищеності особистих даних.

Висновки. Запропоновано метод оцінки залежності захисту особистих даних від кількість інформації в системі та довіри в соціальних мережах.

Проведено моделювання для різних значень параметрів довіри та кількісті інформації в системі. Усі варіанти рішення рівняння близько стаціонарного стану системи, довели, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини довіри, та загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненційним загасаючим законом. Отримані графічні матеріали довели, що захист особистих даних зростає від зростання факторів довіри до інформації. Залежність захисту особистих даних від довіри пропорційна при постійних інших параметрах захисту. Зі зростанням кількісті інформації в системі та довіри до інформації сумарний показник захисту інформації, при моделюванні за запропонованої методикою, зростає зі швидкістю на 9% більше ніж за моделюванням за старими методами, що є цілком сприятним результатом.

ЛІТЕРАТУРА

[1] 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.

[2] Inna Kal'chuka, Serhii Laptiev, Tetiana Laptieva. Analysis of Data Transmission using one modified neural network. International Journal Artificial Intelligent and Informatics. Vol.3, No.2, December2021, pp. 73–79.

[3] М.М. Браіловський, І.С. Іванченко, І.Р. Опірський, В.О. Хорошко. Інформаційно-психологічне протиборство в Україні. НАУ: Науковий журнал «Безпека інформації», – том 25 №3, - Київ, 2019. С. 144-149.

[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.

[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.

[6] 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,

[7] Lukova-Chuiko, N., Herasymenko, O., Tolupa, 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, pp. 67–70.

[8] 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, pp. 71–75.

[9] 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, pp. 99–105.

[10] 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.

[11] 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.

[12] Yoshihara T. Chinese Information Warfare: A Phantom Menace or Emerging Threat? Strategic Studies Institute, U.S. Army War College. 43 p.

[13] Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства. Збірник наукових праць ВІТІ НТУУ «КПІ». 2013. № 1. С. 31–39.

[14] O.R. Laponina, V.A. Suhomlin, "Networks transformation methods to SDN-Architecture", International Journal of Open Information Technologies. Vol. 3, No. 4, 2015. pp. 8-17.

[15] N. Pashynska, V. Snytyuk, V. Putrenko, A. Musienko "A decision tree in a classification of fire hazard factors ", Eastern-European Journal of Enterprise Technologies. – Kharkov, 2016. – № 5/10(83). – pp. 32–37.

[16] Davydenko V.A., Romashkina G.F., Chukanov S.N. Modelirovanie sotsial'nkh setei [Modeling social networks]. Vestnik Tyumenskogo gosudarstvennogo universiteta – Vesntik TSU, No. 1, 2005. pp. 68–79.

[17] Gatti M. Large-Scale Multi-Agent-Based Modeling and Simulation of Microblogging-Based Online Social Network. Multi-Agent-Based Simulation XIV. MABS. 2014. pp. 17−33.

[18] Gubanov D., Chkhartishvili A. A conceptual approach to the analysis of online social networks. Upravlenie bol'shimi sistemami – Large-Scale Systems Control, No. 45, 2013. pp. 222−236.

[19] Akhramovich V.M. Communication and influence of users in social networks. Colloquium–journal. Warszawa, Polska. 2020. №3 (55). pp. 21–25.

УДК 336.71:004.056

Toliupa S., Laptiev S. Improvement of the mathematical model of personal data protection considering trust and quantity of information in social networks

Abstract. *Information needs constant reliable protection. Protection against unauthorized access and distribution, accidental deletion or modification. All developed European countries are concerned about the problem of information security, as well as the protection of personal data of the country's citizens. Social networks are one of the main methods of communication, finding connections and sharing both public and personal information. Social networks make up a constantly growing share among general networks. The network itself acquires new properties, acting as an independent factor. Therefore, it is constantly necessary to develop an information protection system, especially the protection of personal data in social networks. The paper analyzes the parameters of social networks. The parameters of the social network are the transfer of information to other users, traffic density, the probability of building a secure network, and others. A mathematical model for determining the security of personal data from trust and the amount of information in social networks has been developed. Mathematical modeling was carried out in the MatLab environment, the simulation proved that, based on the conditions of the dissipation ratio and the natural frequency of fluctuations of the quantity, the decay of the latter to a certain value is carried out periodically, with a decaying amplitude, or according to an exponential decay law. That is, the protection of personal data increases due to the growth of information trust factors. Mathematical modeling of the proposed model, a model that determines the dependence of personal data protection on trust and the amount of information, confirmed the adequacy of the developed model and proved that personal data protection is proportional to trust. The protection of personal data increases with the growth of trust parameters. But the protection of personal data diminishes slightly as the amount of information to be protected grows. This fully corresponds to the real situation and confirms the adequacy of the developed model.*

Keywords*: social network, trust, amount of information, personal data, mathematical model.*

Толюпа Сергій Васильович, доктор технічних наук, професор**,** профессор кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Serhii Toliupa, Doctor of Technical Sciences, Professor, Professor of the Department of Cyber Security and Information Protection, Faculty of Information technology of Taras Shevchenko National University of Kyiv.

Лаптєв Сергій Олександрович, аспірант кафедри кібербезпеки та захисту інформації, факультет інформаційних технологій**,** Київський національний університет імені Тараса Шевченка.

Serhii Laptiev, PhD-student of the Department of Cyber Security and Information Protection, Faculty of information technology of Taras Shevchenko National University of Kyiv.

Отримано *14 жовтня 2022 року,* затверджено редколегією *14 листопада 2022 року*