УДК 004.056.523:004.6-027.552 DOI: 10.31673/2412-4338.2024.021920

Глухов Сергій Іванович
Київський національний університет імені Тараса Шевченка, Київ
ORCID 0000-0002-4918-3739

Пархоменко Іван Іванович
Київський національний університет імені Тараса Шевченка, Київ
ORCID 0000-0001-6889-9284

Мужанова Тетяна Михайлівна
Державний університет інформаційно-комунікаційних технологій
ORCID 0000-0002-7435-0287

Ровда Володимир Володимирович
Державний університет інформаційно-комунікаційних технологій
ORCID 0009-0001-9987-6787

АЛГОРИТМ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЗА РАХУНОК ПОЄДНАННЯ МОДЕЛЕЙ ЗАГРОЗ І ПОРУШНИКА БЕЗПЕКИ

Анотація. *Статистика порушень інформаційної безпеки свідчить, що компрометація інформації є одним із найчастіших порушень безпеки, а майже половина з них спрямована на заволодіння персональними даними. Оскільки компанії зазнають значних фінансових збитків, втрачають клієнтів і репутацію внаслідок витоку особистих даних, саме вони вимагають особливо надійного й ефективного захисту. Встановлено, що для ефективного захисту персональних даних, які обробляються в ІКС, необхідно впроваджувати комплекс нормативно-правових, організаційних, інженерно-технічних і програмно-апаратних заходів. Розглянуто основні засади нормативно-правового забезпечення захисту персональних даних в Україні, яке зобов'язує підприємства, організації й установи, які володіють або розпоряджаються персональними даними, забезпечити їх належний захист. У роботі проаналізовано існуючі моделі загроз персональним даним і порушника безпеки даних, зокрема вимоги до їх формування, елементи, чинники й характеристики, які мають бути враховані при моделюванні. На основі отриманих результатів запропоновано алгоритм підвищення ефективності захисту персональних даних в ІКС, який завдяки поєднанню моделей загроз і порушника безпеки має синергетичний ефект і призводить до збільшення якісних показників захищеності даних. Саме досягнення синергетичного ефекту щодо підвищення ефективності захисту персональних даних створює переваги представленої моделі у порівнянні з існуючими моделями й алгоритмами. Також представлені рекомендації для організацій і фізичних осіб щодо підвищення ефективності захисту персональних даних в ІКС, постійне дотримання яких сприятиме зменшенню кількості інцидентів, пов'язаних із компрометацією особистої інформації.*

Ключові слова: *захист персональних даних, модель загроз безпеці, модель порушника безпеки, алгоритм підвищення ефективності захисту персональних даних.*

Gluhov Sergiy
Taras Shevchenko National University of Kyiv
ORCID 0000-0002-4918-3739

Parkhomenko Ivan
Taras Shevchenko National University of Kyiv
ORCID 0000-0001-6889-9284

Muzhanova Tetiana
State University of Information and Communication Technologies
ORCID 0000-0002-7435-0287

Rovda Volodymyr
State University of Information and Communication Technologies
ORCID 0009-0001-9987-6787

ALGORITHM FOR INCREASING PERSONAL DATA PROTECTION EFFICIENCY DUE TO COMBINATION OF THREAT AND SECURITY VIOLATOR MODELS

Abstract. *Statistics of information security breaches show that information compromise is one of the most frequent security violations, and almost half of them are aimed at acquiring personal data. Since companies suffer significant financial losses, lose customers and their reputation due to the leakage of personal data, it is this category of data that requires particularly reliable and effective protection. It has been established that for the effective protection of personal data processed in information and communication systems, it is necessary to implement a complex of normative-legal, organizational, engineering-technical and software-hardware measures. The basic principles of the regulatory and legal protection of personal data in Ukraine, which obliges enterprises, organizations and institutions that own or dispose of personal data, to ensure their proper protection, are considered. The paper analyzes the existing models of threats to personal data and data security tools, in particular the requirements for their formation, elements, factors and characteristics that must be considered during modeling. Based on the obtained results, an algorithm for improving the efficiency of personal data protection in ICS is proposed, which, thanks to the combination of threat and security violator models, has a synergistic effect and leads to an increase in the quality of data protection indicators. Achieving a synergistic effect on increasing the efficiency of personal data protection creates advantages of the presented model in comparison with existing models and algorithms. Recommendations for organizations and individuals on improving the efficiency of personal data protection in ICS are also presented, constant compliance with which will help reduce the number of incidents related to the compromise of personal information.*

Keywords: *protection of personal data, security threat model, security violator model, algorithm for increasing the efficiency of personal data protection.*

1. Постановка проблеми. Як свідчить статистика, компрометація даних є одним із найбільш частих порушень безпеки. Так, у 2022 році від витоку даних із середнім показником 4,8 випадків на день постраждали 422 мільйони людей по всьому світу. Серед особистих даних, які витікають під час цих порушень, в порядку спадання відзначають: імена, номери соціального страхування, домашні адреси, історії хвороби і номери банківських рахунків жертв [1]. Згідно з дослідженням IBM майже половина порушень даних (44%) спрямована на імена клієнтів, адреси електронної пошти та паролі [2]. Дослідження показали, що внаслідок компрометації особистих даних компанії втрачають репутацію і клієнтів. Так, 94% організацій зазначили, що споживачі не будуть користуватися їхніми послугами й купувати їхні продукти, якщо особисті дані клієнтів не будуть належним чином захищені [3]. Отже, саме персональні дані є одним із найцінніших активів організації і вимагають надійного й ефективного захисту.

З огляду на зазначене, дослідження шляхів підвищення ефективності захисту персональних даних, зокрема розробка алгоритму захисту персональних даних, які обробляються в інформаційно-комунікаційних системах (ІКС), за рахунок поєднання моделей загроз і порушника безпеки із забезпеченням синергетичного ефекту, є актуальним науковим завданням.

2. Аналіз останніх досліджень і публікацій. Аналіз наукових публікацій вітчизняних дослідників [4-10] показав, що при побудові захисту особистої інформації використовують два основних підходи, які використовують подання процесу її обробки у вигляді абстрактного

обчислювального середовища з багатьма суб'єктами (користувачі та процеси) і об'єктами (ресурси та набори даних). При цьому побудова системи захисту полягає у створенні захисного середовища як певної сукупності обмежень і процедур, спроможних під управлінням ядра безпеки запобігти несанкціонованому доступу й реалізувати санкціонований доступ суб'єктів до об'єктів, а також забезпечити захист останніх від навмисних і випадкових зовнішніх та внутрішніх загроз.

Водночас, виявлено недоліки, притаманні обом підходам, зокрема формування моделей інформаційної безпеки на основі моделі CIA (конфіденційність, цілісність і доступність), відсутність розмежування понять «інформаційна безпека» й «безпека інформації», формальне комплексування загроз без урахування їх особливостей, які не дозволяє отримати значні переваги при застосуванні моделей загроз персональним даним.

У роботах [11-14] доведено, що однією з важливим елементом моделі загроз є модель порушника, завдяки чому забезпечуються смислові відносини між повним описом загроз і уявленнями про потенційні можливості порушника щодо підготовки і проведення атак як джерела загроз, а також про обмеження щодо цих можливостей. Автори зазначених праць використовують для побудови моделі порушника підходи, що мають спільні класифікаційні ознаки і корелюються в різних джерелах.

Наукові публікації [15-17] представляють моделі порушника, при побудові яких враховують низку чинників, серед яких: цілі й розміщення зловмисника (внутрішній/зовнішній); наявність у порушника доступу до штатних засобів (сукупність програмного, програмно-апаратного й технічного забезпечення); рівень професійної підготовки і знань порушника про об'єкти атак; можливість використання різних засобів для проведення атак; можливість змови зловмисників різних категорій.

Однак, при побудові моделі порушника крім зазначених аспектів доцільно проводити аналіз на відповідність об'єктів доступу суб'єктам атак, каналів атак, обґрунтовувати вилучення суб'єктів атак із числа потенційних порушників, а також враховувати стадії життєвого циклу інформації, на які може впливати порушник.

Вивчення наукових публікацій показало, що для ефективного вирішення завдань захисту особистої інформації необхідно додатково брати до уваги такі рівні впливу: технічних каналів, несанкціонованого доступу, заставних пристроїв, системи захисту інформації, штатних засобів, які можуть бути використані для несанкціонованого доступу до персональних даних, обсягу потенційних збитків. Встановлено, що внаслідок існуючого протиріччя між наявним науковим апаратом і сучасними вимогами щодо протидії загрозам інформаційній безпеці вирішення наукового завдання щодо підвищення ефективності захисту особистої інформації в ІКС через удосконалення моделей загроз і порушника безпеки є на часі.

3. Мета і задачі дослідження. Метою дослідження є підвищення ефективності захисту персональних даних в ІКС шляхом розробки алгоритму підвищення ефективності захисту персональних даних за рахунок поєднання моделей загроз і порушника безпеки.

Для досягнення поставленої мети вирішено такі завдання:

−проведено порівняльний аналіз існуючих моделей захисту персональних даних;

−розроблено алгоритм підвищення ефективності захисту персональних даних в ІКС через поєднання моделей загроз і порушника безпеки;

−надано рекомендації щодо методів підвищення ефективності захисту особистої інформації, яка обробляється в ІКС.

4. Результати дослідження. З розвитком інформаційних технологій зростають і загрози безпеці інформації, в тому числі й персональних даних. Відповідно, виникає нагальна потребі забезпечення їх надійного й ефективного захисту.

Важливу роль у забезпеченні безпеки персональних даних відіграє нормативно-правова база, яка встановлює вимоги, зобов’язання, обмеження, а також санкції за їх невиконання. Так, Закон України «Про захист персональних даних» зобов’язує організації, підприємства й установи, які володіють або розпоряджаються персональними даними, забезпечити захист цих

даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних [18].

Зазначений Закон визначає суб'єктів відносин, пов'язаних із персональними даними, та їх права, встановлює підстави, загальні й особливі вимоги до обробки персональних даних, порядок доступу до них, окреслює засади збирання, використання, накопичення та зберігання, поширення, видалення або знищення персональних даних тощо. Також у Законі встановлено повноваження Уповноваженого Верховної Ради України з прав людини, який разом із судовими інстанціями здійснює контроль за дотриманням законодавства про захист персональних даних.

У 2010 році у Україна ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [19] спільно з Додатковим протоколом щодо органів нагляду та транскордонних потоків даних. Метою Конвенції задекларовано забезпечення всім людям незалежно від громадянства або місця проживання, дотримання їхнього права на недоторканість приватного життя, у зв'язку з автоматизованою обробкою персональних даних. Усі підписанти зобов’язуються дотримуватися встановлених принципів захисту даних, які піддаються автоматизованій обробці.

Відповідно до Конвенції й Закону України «Про захист персональних даних» персональні дані є будь-якою інформацією, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною.

Не можна не згадати прийняття у 2016 році Загального регламенту захисту даних ЄС (General Data Protection Regulation, GDPR) [20], який є зразком кращих практик у галузі захисту персональних даних для усіх європейських держав, у тому числі й України.

Відповідно до GDPR *основними принципами обробки персональних даних* є**:**

1. Законність, справедливість і прозорість. Персональні дані мають оброблятися відповідно до норм діючого законодавства, неупереджено та прозоро. Будь-яка інформація про цілі, методи й обсяги обробки таких даних має бути подана у простій і доступній для сприйняття формі.

2. Обмеження мети. Персональні дані підлягають збиранню й використанню виключно для цілей, які заявлені організацією (онлайн-сервісом).

3. Мінімізація даних. Особисті дані можуть збиратися й оброблятися лише в обсягах, передбачених для досягнення цілей обробки. Перевищення обсягів є протизаконним.

4. Точність. У випадку обробки неточних персональних даних особи, такі дані мають бути негайно видалені або виправлені на її вимогу.

5. Обмеження термінів зберігання. Особисті дані мають зберігатися у формі, яка дозволяє ідентифікувати суб'єкта даних упродовж незначно більшого терміну, ніж це необхідно з метою обробки.

6. Цілісність і конфіденційність. У процесі обробки персональних даних користувачів компанії зобов'язані забезпечити їх захист від несанкціонованої чи незаконної обробки, знищення або пошкодження [20].

Слід відзначити, що вітчизняний Закон про захист персональних даних також декларує вимоги щодо дотримання зазначених принципів (статті 6-7, 24).

Водночас, для комплексного захисту особистої інформації необхідно поєднання нормативно-правових, організаційних, інженерно-технічних і програмно-апаратних заходів. Цю класифікацію слід враховувати також при моделюванні загроз безпеці персональних даних для забезпечення достатнього рівня захищеності.

Модель загроз безпеці персональних даних ґрунтується на загальних класифікаціях [5-8,13-16], які охоплюють перехоплення персональних даних технічними каналами і несанкціонований доступ до ІКС, в яких вони обробляються.

Потоки несанкціонованого доступу до ІКС з персональними даними можуть бути як випадковими [25], так і цілеспрямованими з використанням програмних і програмно-апаратних засобів. Під порушником безпеки персональних даних будемо розуміти фізичну

особу, яка випадково чи навмисно вчиняє дії, наслідком яких є порушення безпеки персональних даних у процесі їх обробки технічними засобами в ІКС персональних даних [24].

Модель надає можливість виявляти і запобігати діям порушників безпеки персональних даних [26].

Формування моделі порушника є складним процесом, який вимагає врахування багатьох, нерідко суперечливих чинників. Така модель, як і модель загроз безпеці персональних даних, має бути адаптивною, щоб забезпечити належний рівень їх захищеності. За неможливості формування моделі порушника можна замінити її моделлю загроз. Модель загроз, яка детально описана у міжнародних стандартах, є похідною від рівня захищеності та ймовірності реалізації загрози і досить точно видає вербальні інтерпретації [7]. Опис може відповідати формальному опису систем безпеки.

Нехай U_1, U_2,…, U_n – дискретні стани безпеки персональних даних, на які впливають загрози, тоді враховуючи вимоги до системи захисту персональних даних, можна оцінити вербальну інтерпретацію результатів. Дискретний стан може бути визначений шляхом виконання такого логічного виразу:

$$\forall U_i, U_n \le U_o, \quad i = [1, n]. \tag{1.1}$$

де Ui - стан безпеки персональних даних, що обробляються оператором; U_0 - граничний стан безпеки персональних даних, який відповідає вимогам законодавства; n – кількість потенційно можливих станів безпеки персональних даних.

Моделюючи загрози безпеці персональних даних для забезпечення прийнятного рівня захищеності, не слід забувати про технічні канали, вразливі до витоків інформації. Під технічним каналом витоку інформації розумітимемо сукупність носія інформації (засобу обробки), фізичного середовища поширення інформаційного сигналу та засобів, якими видобувається інформація, яка підлягає захисту [21].

Найчастіше основним засобом передавання персональних даних є глобальна мережа Інтернет. Причому актуальною є тенденція використання Інтернету для передачі персональних даних навіть усередині організації, оскільки керівники все рідше прагнуть розгортати внутрішню локальну мережу і все частіше використовують хмарні технології [4-8]. У таких випадках моделювання загроз безпеці персональних даних дозволяє швидко виявити проблему.

Модель загроз безпеки персональних даних для забезпечення прийнятного рівня захищеності дозволяє вирішити такі завдання:

–виявлення загроз безпеці персональних даних в ІКС організації, де вони обробляються;

–пошук особливостей функціонування ІКС;

–розрахунок показників захищеності персональних даних від внутрішніх і зовнішніх загроз;

–розробка системи захисту персональних даних, що забезпечує прийнятний рівень захищеності, передбачений для певного класу ІКС, де обробляються персональні дані організації;

–впровадження заходів для запобігання несанкціонованому доступу до персональних даних;

–моделювання впливу на технічні засоби ІКС;

–визначення ІКС, в яких може бути порушено безпеку персональних даних організації;

–постійний моніторинг рівня захищеності персональних даних.

Слід відзначити, що моделі загроз безпеці персональних даних для конкретної організації будуть притаманні як загальні, так і унікальні характеристики.

До загальних відносять, зокрема обсяг персональних даних, що обробляються в ІКС. Цей важливий показник, на відміну від обсягу цифрової інформації, який зазвичай вимірюють у байтах (кілобайтах, гігабайтах), доцільно вимірювати за кількістю суб'єктів персональних даних. У звичайній класифікації прийнято такі обсяги ділити на такі категорії:

–до 1 000 суб'єктів персональних даних;

–1 000 - 100 000 суб'єктів персональних даних;

–понад 100 000 суб'єктів персональних даних.

Іншою вагомою характеристикою є наявність під'єднання до мережі Інтернет [11-15]. Вимоги до під'єднаної до Інтернету ІКС, в якій обробляються персональні дані, є значно вищими.

Не менш важливими є показники розмежування прав доступу [16-17, 21-23], оскільки користувачі ІКС, де обробляються персональні дані, можуть мати різні права доступу в залежності від ролі й повноважень.

Також при моделюванні загроз безпеці персональних даних доцільно враховувати можливість реалізації так званого ефекту Сноудена, коли основний витік даних походить від системного адміністратора, обов'язки якого охоплюють забезпечення інформаційної безпеки.

Крім переліченого, модель загроз безпеці персональних даних повинна враховувати чинник наявності ліцензії на інформаційні технології, які використовуються для зберігання й обробки персональних даних. Так, при формуванні підсистеми антивірусного захисту модель передбачає застосування ліцензованих антивірусних програм.

З урахуванням викладеного вище запропоновано алгоритм підвищення ефективності захисту персональних даних за рахунок поєднання моделей загроз і порушника безпеки (Рис.1).

Представлений алгоритм завдяки поєднанню (накладанню) моделей загроз і порушника безпеки має синергетичний ефект, який є результатом спільної дії зазначених моделей і призводить до збільшення якісних показників функціонування без збільшення кількісних. Саме досягнення синергетичного ефекту щодо підвищення ефективності захисту персональних даних створює переваги представленої моделі у порівнянні з існуючими моделями й алгоритмами.

Водночас, для підвищення ефективності захисту персональних даних, які обробляються в ІКС, як для окремої особи, так і для працівників організації слід дотримуватися таких рекомендацій.

Двофакторна аутентифікація, яка передбачає використання двох різних методів перевірки ідентичності користувача при вході до системи, є ефективним способом значно підвищити безпеку особистої інформації. Зазвичай перший метод - це звичайний пароль, а другий - згенерований код або секретні питання. Навіть у випадку, якщо зловмиснику вдасться отримати облікові дані користувача для входу в систему, і він намагатиметься отримати доступ до даних, йому все ще потрібно буде використовувати додатковий метод автентифікації.

Надійні паролі. При створенні пароля необхідно уникати використання простих цифр чи букв, особистих даних, які буде легко вирахувати хакеру. Надійний пароль повинен містити комбінації малих і великих літер, цифр і символів, і періодично змінюватися. Збільшує шанси злому використання одного й того ж пароля для кількох облікових записів. Слід використовувати унікальний і надійний пароль для кожного облікового запису. Використання менеджера паролів дозволить тримати їх у безпеці завдяки шифруванню.

Використання захищених мереж. У більшості загальнодоступних і безкоштовних мереж Wi-Fi рівень безпеки є неприйнятно низьким. Тому інші користувачі тієї ж мережі можуть легко отримати доступ до чужих особистих даних, «злити» їх або використати для фінансового шахрайства. Прийнятним рішенням є використання VPN-мережі, яка шифрує з'єднання, а, отже, краще захищає від загроз.

Захищені з'єднання. Перш ніж ввійти до онлайн-банку, електронної пошти чи іншого сервісу

шляхом введення особистої інформації, варто перевірити, чи з'єднання є захищеним (адреса сайту має починатися з https, а не http). Щоб перевірити надійність веб-сайту є кілька інших способів, наприклад, політика конфіденційності веб-сайту, контактна інформація або друк «перевірено». Також варто встановити на свій комп'ютер антивірусне ПЗ і регулярно його оновлювати.

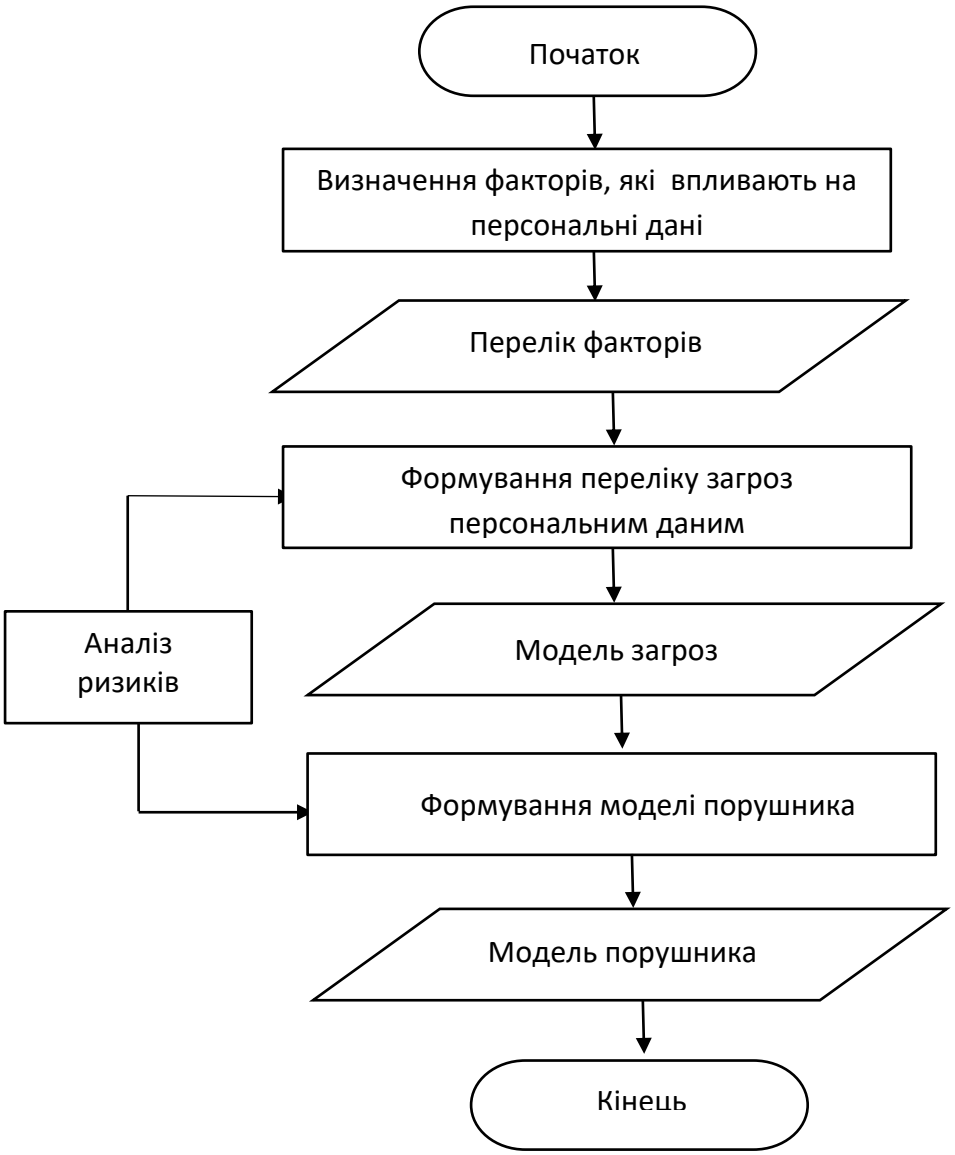

Рис. 1. Алгоритм підвищення ефективності захисту персональних даних в ІКС шляхом поєднання моделей загроз і порушника безпеки.

Налаштування конфіденційності. Кожен повинен знати, що комп'ютер, смартфон, обліковий запис і програма мають налаштування конфіденційності. Відповідно користувач може обмежити категорії й обсяг даних, які їм дозволено збирати. Особливо увагу варто звернути на налаштування щодо засобів оплати онлайн, геолокації, зображень, номеру телефону.

Дотримання вимог приватності. Слід бути обережним, поширюючи особисту інформацію в соціальних мережах або на інших загальнодоступних ресурсах. Персональні дані, оприлюднені в соціальних мережах, можуть легко бути використані зловмисниками, щоб зламати чужий обліковий запис, ідентифікувати й шантажувати особу тощо. Навіть, видаливши особисті дані, особа не може бути впевнена, що вони не були збережені іншими особами або ресурсами.

Ознайомлення з політиками конфіденційності. Завжди треба пам'ятати, що часто лише одне натискання на кнопку або чек-бокс прирівнюється до надання згоди на обробку персональних даних. Важливо знайти час на ознайомлення з угодами користувача, політиками конфіденційності сайтів або додатків. Принаймні не лишнім буде визначити, які дані запитує

сайт або додаток, чи необхідна така інформація для мети, з якою особа користується сайтом або додатком.

Увага до посилань і вкладень. Перед тим, як відкрити електронного листа, вкладення чи натиснути на посилання, обов'язково звертати увагу на адресу електронної пошти, орфографічні помилки, неперсоніфіковане звертання, наявність підозрілих прикріплених файлів, маніпулятивний зміст (погрози, термінові прохання) тощо. Адже фішингові схеми мають на меті спонукати користувача зробити необдуманий клік, щоб надати зловмисникам можливість викрасти особисті дані чи завантажити шкідливий код.

Виправлення операційної системи й інших програм. Оскільки завданням зловмисника є знайти прогалини у системному або іншому програмному забезпеченні, щоб у подальшому проникнути в нього, обов'язком користувача є регулярне оновлення й застосування виправлень операційної системи й іншого ПЗ.

Резервне копіювання даних. Щоб запобігти небажаній втраті цінних даних, потрібно робити регулярне резервне копіювання. Тому що, яким би надійним не був захист, порушення безпеки все одно можуть статися. Не можна зберігати створені резервні копії на тому ж носієві, що й основні. Доцільно зберігати скопійовані файли в безпечному місці, наприклад, у хмарах.

Надійна утилізація. Перш ніж утилізувати комп'ютер або смартфон варто переконатися, що всі персональні дані на ньому надійно знищено. Надійніше видаляти конфіденційну інформацію відповідно до рекомендацій виробника або використовувати спеціальні програми.

5. Висновки. У результаті порівняльного аналізу існуючих моделей захисту персональних даних встановлено, що внаслідок існуючого протиріччя між наявним науковим апаратом і зростаючими вимогами щодо протидії загрозам інформаційній безпеці проблема підвищення ефективності захисту особистої інформації залишається актуальною.

Наголошено, що для ефективного захисту персональних даних, які обробляються в ІКС, необхідно поєднання нормативно-правових, організаційних, інженерно-технічних і програмно-апаратних заходів. Цю класифікацію слід також враховувати при моделюванні загроз безпеці персональних даних для забезпечення достатнього рівня захищеності.

У роботі розроблено алгоритм підвищення ефективності захисту персональних даних в ІКС, який завдяки поєднанню моделей загроз і порушника безпеки має синергетичний ефект і призводить до збільшення якісних показників захищеності даних. Саме досягнення синергетичного ефекту щодо підвищення ефективності захисту персональних даних створює переваги представленої моделі у порівнянні з існуючими моделями й алгоритмами.

Відповідно до представлених рекомендацій для підвищення ефективності захисту персональних даних, які обробляються в ІКС, як для окремої особи, так і в межах організації доцільно: використовувати двофакторну автентифікацію; створювати надійні паролі; використовувати захищені мережі і з'єднання; налаштовувати параметри конфіденційності; дотримуватися вимог приватності в мережі Інтернет; знайомитися з угодами користувача, політиками конфіденційності сайтів або додатків; звертати увагу на підозрілі листи, посилання і вкладення; регулярно оновлювати й виправляти операційну систему й інше ПЗ; здійснювати резервне копіювання особистої інформації; забезпечувати надійну утилізацію носіїв персональних даних.

Планується зосередити увагу подальших досліджень на розробці програмної реалізації запропонованого алгоритму підвищення ефективності захисту персональних даних.

Список використаної літератури

1. ITRC Annual Data Breach Report (2020). *ITRC*. https://www.idtheftcenter.org/publication/2022-data-breach-report/

2. IBM Report: Cost of a Data Breach Hits Record High During Pandemic (2021). *IBM*. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

3. Cisco 2024 Data Privacy Benchmark Study. *Cisco*. https://www.cisco.com/c/en/us/about/

trust-center/data-privacy-benchmark-study.html#~about-the-study

4. Собчук В. В., Замрій І. В., Собчук А. В., Лаптєв С. О., Лаптєва Т. О. Періодичні рішення нелінійних диференційних рівнянь моделей інформаційної мережі. *Sciences of Europe*. Praha, Czech Republic. 2021.Vol. 1. No 67. С. 31-35.

5. Лаптєв О. А., Собчук В. В., Собчук А. В., Лаптєв С. О., Лаптєва Т. О. 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

6. 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.

7. Лаптєв С. О. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. *Кібербезпека: освіта, наука, техніка*. 2022. 4(16). С. 45–62.

8. 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.

9. 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.

10. 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).* 2021.Vol. 13, No. 1. pp.15-21. https://www.ijcnis.org/index.php/ijcnis/article/view/4882

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

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

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

14. 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*, Volume 8. No. 2, February 2020, pp. 271-276. http://www.warse.org/ IJETER/static/pdf/file/ijeter05822020.pdf

15. Yang Jaewon, Leskovec Jure. Defining and evaluating network communities based on ground–truth. *Knowledge and Information Systems*. 2015. Т. 42, № 1. pp. 181–213.

16. 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.

17. 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.

18. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Офіційний вісник України* від 09.07.2010, 2010 р., № 49, стор. 199, стаття 1604. https://zakon.rada.gov.ua/laws/card/2297-17

19. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. *Офіційний вісник України* від 14.01.2011, 2011 р., № 1, / № 58, 2010, ст. 1994 /, стор. 701, стаття 85

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2016/679/oj

21. Лаптєв О., Гришанович Т. Комплексна методика оцінювання ефективності функціонування системи дистанційного навчання. *Прикладні проблеми комп'ютерних наук, безпеки та математики*. Волинський національний університет імені Лесі Українки, Луцьк. 2023. 2023. С. 63–75.

22. Лаптєв О. А., Бучик С. С., Савченко В. А., Наконечний В. С., Михальчук І. І., Шестак Я. В. Виявлення та блокування повільних DDOS-атак за допомогою прогнозування поведінки користувача. *Наукоємні технології. Інформаційні технології, кібербезпека*. 2022. Том 55. № 3. С. 184-192.

23. Беркман Л. Н., Барабаш О. В., Ткаченко О. М., Мусієнко А. П., Лаптєв О. А., Свинчук О. В. Інтелектуальна система управління для інфокомунікаційних мереж. *Системи управління навігації і зв'язку*. 2022. Том 3. № 69. С. 54–59.

24. Наконечний В., Лаптєв О., Погасій С., Лазаренко С., Мартинюк Г. Відбір джерел з неправдивою інформацію методом бджолиної колонії. *Наукоємні технології. Інформаційні технології, кібербезпека*. 2021. Том 52. № 4. С.330-337.

25. Кальчук І., Лаптєва Т., Лукова-Чуйко Н., Харкевич Ю. Метод побудови захищених каналів передачі даних з використанням модифікованої нейронної мережі. *Information Technology and Security*. 2021. Vol. 9, Iss. 2, July – December. pp. 232–243.

26. Лаптєва Т. О. Спрощений алгоритм аналізу розповсюдження недостовірної інформації в умовах інформаційного протиборства. *Науково-технічна конференція молодих вчених «Актуальні проблеми інформаційних технологій» (АРЈТ-2021)* 19-20 жовтня 2021р. Київ. С. 56–58.

References

1. ITRC Annual Data Breach Report (2020). *ITRC*. https://www.idtheftcenter.org/publication/2022-data-breach-report/

2. IBM Report: Cost of a Data Breach Hits Record High During Pandemic (2021). *IBM*. https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

3. Cisco 2024 Data Privacy Benchmark Study. *Cisco*. https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html#~about-the-study

4. 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. pp. 31-35.

5. Oleksandr Laptiev, Valentyn Sobchuk, Andrii Sobchuk, Serhii Laptiev, Tetiana Laptieva. An improved model for estimating the economic costs of the information protection system in social networks. *Cyber security: education, science, technology*. Volume 4 No. 12 (2021). pp. 19–28. https://doi.org/10.28925/2663-4023.2021.12.1928

6. Lukova-Chuiko N.V., Tolyupa S.V., Pogasii S.S., Lapteva T.O., Laptev S.O. Improving the model of information protection in social networks. *Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University*. K.: VIKNU, Vol. 73, 2021. pp. 88-103.

7. Sergey Laptiev. An improved method of protecting personal data from attacks using social engineering algorithms. *Cybersecurity: education, science, technology*. 4(16), 2022. pp. 45–62.

8. S. Laptiev, S. Tolupa. The methodology for evaluating the functional stability of the protection system of special networks. *Scientific technologies. Information technologies, cyber security*. Volume 55 No. 3 (2022) C.178 – 183. https://doi.org/10.18372/2310-5461.55.16900

9. 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. https://doi.org/10.21303/2461-4262.2021.001615

10. 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

11. S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. Synergy of building cybersecurity systems: monograph. Kharkiv: PC Technology Center, 2021. 188 p. http://monograph.com.ua/pctc/catalog/book/64

12. Horbulin V.P. Information operations and social security: threats, countermeasures, modeling: monograph / V.P. Horbulin, O.G. Dodonov, D.V. Lande. K.: Intertekhnologiya, 2009. 164 p.

13. Akhramovych V.M. Models of trust and reputation of users in social networks. *Modern information protection*. K. DUT. 2019, No. 4, pp. 45–51.

14. Vitalii Savchenko, VolodymyrAkhramovych, Alina Tusych, Irina Sribna, Ihor Vlasov. Analysis of Social Network Parameters and the Likelihood of its Construction. *International Journal of Emerging Trends in Engineering Research.* Volume 8.No. 2, February 2020, pp. 271–276. http://www.warse.org/IJETER/static/pdf/file/ijeter05822020.pdf

15. Yang Jaewon, Leskovec Jure. Defining and evaluating network communities based on ground-truth. *Knowledge and Information Systems*. 2015. Vol. 42, No. 1. pp. 181–213.

16. 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.

17. Lukova-Chuiko N.V., Laptev O.A., Barabash O.V., Musienko A.P., Ahramovich V.M. The method of calculating the protection of personal data taking into account the set of specific parameters of social networks. *Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University*. Kyiv: VIKNU, 2022. No. 76. pp. 54–68.

18. On the protection of personal data: Law of Ukraine dated 01.06.2010 No. 2297-VI. *Official Gazette of Ukraine* dated 09.07.2010, 2010, No. 49, p. 199, Article 1604. https://zakon.rada.gov.ua/laws/card/2297-17

19. Convention on the Protection of Individuals in Connection with Automated Processing of Personal Data. *Official Gazette of Ukraine* dated 14.01.2011, 2011, No. 1, / No. 58, 2010, Art. 1994 /, p. 701, Article 85.

20. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2016/679/oj

21. Laptev, O., Gryshanovych, T. Complex methodology for evaluating the effectiveness of the distance learning system. *Applied problems of computer science, security and mathematics*. Lesya Ukrainka Volyn National University, Lutsk. 1 (May 2023). 2023. pp.63–75.

22. Laptev O.A., Buchyk S.S., Savchenko V.A., Nakonechnyi V.S. , Mykhalchuk I.I., Shestak Ya.V., Detection and blocking of slow DDOS attacks using user behavior prediction. *Scientific technologies. Information technologies, cyber security*. Volume 55 No. 3 (2022) pp. 184-192.

23. Berkman L.N., Barabash O.V., Tkachenko O.M., Musienko A.P., Laptev O.A., Svynchuk O.V. Intelligent control system for information communication networks. *Navigation and communication control systems.* Volume 3. No. 69. 2022. pp. 54–59.

24. Volodymyr Nakonechny, Oleksandr Laptev, Serhii Pogasii, Serhii Lazarenko, Hanna Martyniuk. Selection of sources with false information using the bee colony method. *Scientific technologies. Information technologies, cyber security*. Volume 52 No. 4 (2021) pp. 330-337.

25. Kalchuk I., Lapteva T., Lukova-Chuiko N., Kharkevich Yu. The method of constructing protected data transmission channels using a modified neural network. *Information Technology and Security*. Vol. 9, Iss. 2, pp. 232–243. July - December 2021.

26. T.O. Lapteva A simplified algorithm for the analysis of the spread of unreliable information in the conditions of information conflict. *Scientific and technical conference of young scientists "Actual problems of information technologies" (ARJT-2021).* October 19-20, 2021. Kyiv. pp.56–58.