

## ДОСЛІДЖЕННЯ ТА АНАЛІЗ МЕТОДІВ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

*В статті запропонований підхід до представлення персональних даних у вигляді неорієнтованого графа, використання графової моделі дозволить застосовувати методи оптимізації на графах для отримання оптимальних параметрів моделі.*

*Дослідження та аналіз методів організації обробки і захисту персональних даних показав, що пропонувані методи і створювані на їх основі системи захисту вимагають значних ресурсів для їх реалізації, мають сильну залежність від типу даних і високу надмірність при практичному застосуванні для роботи з масивами даних невеликої розмірності. Тому в ряді випадків доцільно застосовувати методи, що знімають вимоги до конфіденційності персональних даних, що значно скорочує витрати на захист. Одним з ефективних і перспективних підходів до захисту персональних даних в інформаційних системах є знеособлення персональних даних. У зв'язку з цим доцільно провести дослідження в наступних напрямках: аналіз основних визначень і підходів до організації обробки персональних даних, створення математичної моделі персональних даних; розробка досить універсальних і мало витратних методів і засобів перетворення персональних даних, що забезпечують зниження вимог до захисту. Серед таких методів можна виділити знеособлення персональних даних; розробка методики застосування знеособлення при організації захисту персональних даних; розробка методів оцінки якості захисту персональних даних при знеособленні; розробка інформаційної системи для реєстрації операторів персональних даних та контролю за їх діяльністю. Для зберігання знеособлених даних можна використовувати бази даних, файлові та інформаційні системи, які не мають спеціальних засобів захисту, які відповідають вимогам, визначених у відповідних документах. У зв'язку з цим, процедури знеособлення можна розглядати як перспективні методи захисту і обробки персональних даних, які мають досить широкі можливості для застосування на практиці.*

*Ключові слова: знеособлення даних, персональні дані, бази даних, засоби захисту, інформаційні системи, конфіденційність.*

**Вступ.** Інформація, яка містить відомості про фізичних осіб (громадян) - персональні дані, використовуються в різних системах обробки інформації все частіше, що обумовлено постійним розширенням сфери застосування інформаційних технологій для обслуговування населення. Специфіка роботи з персональними даними заснована на потенційній можливості їх використання для заподіяння шкоди суб'єктам, до яких відносяться дані - власникам персональних даних. Особлива увага приділяється питанням захисту персональних даних (ПД) в автоматизованих інформаційних системах ПД – (ІСПД). Вимоги до захисту в ІСПД,

відповідно до низки документів, враховують категорію і кількість ПД, специфіку вирішуваних завдань і ряд інших показників. Виконання цих вимог, як правило, пов'язане з істотними матеріальними і фінансовими витратами.

**Постановка задачі.** У зв'язку з цим представляють інтерес дослідження спрямовані на розробку і аналіз методів обробки ПД, що дозволяють знизити витрати на забезпечення безпеки в ІСПД.

Для реалізації цього підходу потрібно розробити методи знеособлення і де-знеособлення ПД, що будуть включати в себе правила роботи з знеособленими даними, теоретичне обґрунтування методів знеособлення і де-знеособлення ПД, що дозволяють забезпечити їх конфіденційність, а також правил організації обробки знеособлених даних.

**Основна частина.** База персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

З огляду на це база персональних даних є упорядкованою сукупністю логічно пов'язаних даних про фізичних осіб: що зберігаються та обробляються відповідним програмним забезпеченням, є базою персональних даних в електронній формі; що зберігаються та обробляються на паперових носіях інформації, є базою персональних даних у формі картотек.

Картотекою персональних даних є будь-який структурований масив персональних даних, що є доступним з визначеними критеріями, незалежно від того, чи є такий масив централізованим, децентралізованим або розділеним на функціональних або географічних засадах. Такі дані мають бути структуровані за визначеними критеріями, що стосуються осіб, щоб забезпечити легкий доступ до відповідних персональних даних. Варто зазначити, персональні дані одночасно можуть бути упорядковані і в електронній формі, і в формі картотек. Фізичні особи-підприємці та самозайняті особи самостійно визначають чи володіють вони базами персональних даних у сенсі Закону.

Законодавець поширив дію Закону на всі види діяльності, пов'язані зі створенням баз персональних даних та обробкою персональних даних у цих базах, за винятком такої діяльності, яка здійснюється: фізичною особою - виключно для непрофесійних особистих чи побутових потреб; журналістом – у зв'язку з виконанням ним службових чи професійних обов'язків; професійним творчим працівником - для здійснення творчої діяльності.

Так, під час здійснення своєї професійної діяльності на адвокатів законодавством не покладено обов'язок ведення баз персональних даних клієнтів. Але, якщо адвокати формують справи на своїх клієнтів, які вони постійно оновлюють та підтримують в актуальному стані, такі справи є базою персональних даних та підлягають державній реєстрації. Нотаріуси можуть обробляти персональні дані своїх найманих працівників, клієнтів у базах персональних даних, однак, документи нотаріального діловодства та архів нотаріуса, визначені у статті 14 Закону України «Про нотаріат» не є базою персональних даних у сенсі Закону України «Про захист персональних даних» та не підлягають державній реєстрації. Крім того, у випадку, якщо фізичні особи – підприємці, укладаються договори виконання робіт або надання послуг з фізичними особами, такі договори також не є базою персональних даних та не підлягають державній реєстрації.

Власником бази персональних даних згідно з абзацом третім статті 2 Закону є фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних та процедуру їх обробки, якщо інше не визначене законом. Так, якщо персональні дані обробляються юридичною особою, то власником бази персональних даних є юридична особа. Розпорядником бази персональних даних згідно з абзацом дев'ятим статті 2 Закону може бути фізична чи юридична особа, якій власником бази персональних даних або законом надано право обробляти ці дані.

Практичним прикладом можуть бути відносини між юридичними особами та їх представництвами, філіями, відділеннями тощо. Так, у сенсі Закону ці представництва, філії, відділення виступатимуть розпорядниками баз персональних даних, власником яких є юридична особа. Згідно зі статтею 4 Закону власником чи розпорядником бази персональних

даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, які обробляють персональні дані відповідно до закону. Але якщо власником бази персональних даних є орган державної влади чи орган місцевого самоврядування, то розпорядником бази персональних даних, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу.

Порядок обробки персональних даних. Обробка персональних даних включає в себе такі дії, як збирання, реєстрацію, накопичення, зберігання, адаптування, зміну, поновлення, використання і поширення (розповсюдження, реалізацію, передачу), знеособлення, знищення персональних даних. Обробка персональних даних може бути здійснена як неавтоматичними засобами з носіїв (у тому числі паперових), що становлять будь-який структурований масив персональних даних, який є доступним за визначеними критеріями, так і з використанням інформаційних (автоматизованих) систем.

До персональних даних можна віднести будь-які відомості, за якими ідентифікується або може бути ідентифікована фізична особа, зокрема: прізвище, ім'я, по батькові, адреса, телефони, паспортні дані, національність, освіта, сімейний стан, релігійні та світоглядні переконання, стан здоров'я, матеріальний стан, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи (за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану із здійсненням функцій держави або органу місцевого самоврядування) тощо. Вказаний перелік не є вичерпним. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може оброблятися в тому числі поширюватись тільки за її згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Саме тому, зважаючи на гарантування Конституцією України права особи на невтручання у її особисте життя, правові відносини пов'язані із захистом і обробкою персональних даних були врегульовані Законом України «Про захист персональних даних». Загальні вимоги щодо обробки та захисту персональних даних суб'єктів персональних даних визначені Типовим порядком обробки персональних даних, затвердженим наказом Уповноваженого Верховної Ради України з прав людини №1/02-14 від 08 січня 2014р.

Власники, розпорядники персональних даних самостійно визначають порядок обробки персональних даних, враховуючи специфіку обробки персональних даних у різних сферах, відповідно до вимог, визначених Законом України «Про захист персональних даних» (далі – Закон) та цим Порядком. Вимоги цього Порядку враховуються під час розробки кодексів поведінки щодо обробки персональних даних професійними, самоврядними та іншими громадськими об'єднаннями чи юридичними особами відповідно до статті 27 Закону.

Вимоги до обробки персональних даних. Власник визначає: мету та підстави обробки персональних даних; категорії суб'єктів персональних даних; склад персональних даних; порядок обробки персональних даних (спосіб збору, накопичення персональних даних; строк та умови зберігання персональних даних; умови та процедуру зміни, видалення або знищення персональних даних; умови та процедуру передачі персональних даних та перелік третіх осіб, яким можуть передаватися персональні дані; порядок доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних; заходи забезпечення захисту персональних даних; процедуру збереження інформації про операції, пов'язані з обробкою персональних даних та доступом до них). Також, у деяких випадках, власник визначає обов'язки та права осіб, відповідальних за організацію роботи, пов'язаної із захистом персональних даних під час їх обробки. Обробка даних повинна здійснюватися тільки за згодою суб'єкта. Якщо за результатами розгляду такої вимоги виявлено, що персональні дані суб'єкта (їх частина) обробляються незаконно власник повинен припинити обробку персональних даних суб'єкта (їх частини) та проінформувати про це.

Видалення та знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних. Також власник, розпорядник персональних даних повинен вжити заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

Автоматизовані системи обробки персональних даних. Автоматизована система обробки ПД – це організаційно-технічна система, що являє собою сукупність наступних взаємопов'язаних компонентів: технічних засобів обробки і передачі даних (засобів обчислювальної техніки і зв'язку); методів і алгоритмів обробки у вигляді відповідного програмного забезпечення; інформації (масивів, наборів, баз даних) на різних носіях; персоналу і користувачів системи, об'єднаного за організаційно-структурними, тематичними, технологічними або іншими ознаками для виконання автоматизованої обробки інформації (даних) з метою задоволення інформаційних потреб суб'єктів інформаційних відносин.

Загальноприйнятої класифікації АС взагалі не існує, тому їх можна класифікувати за різними ознаками: за рівнем або сферою діяльності – державні, територіальні (регіональні), галузеві, об'єднань, підприємств або установ, технологічних процесів; за рівнем автоматизації процесів управління – інформаційно-пошукові, інформаційно-довідкові, інформаційно-керівні, системи підтримки прийняття рішень, інтелектуальні АС; За ступенем централізації обробки інформації – централізовані АС, децентралізовані АС, інформаційні системи колективного використання; за ступенем інтеграції функцій – багаторівневі АС з інтеграцією за рівнями управління (підприємство – об'єднання, об'єднання – галузь і т. ін.), багаторівневі АС з інтеграцією за рівнями планування і т. ін.

Державні АС призначені для вирішення найважливіших проблем країни. Центральне місце в мережі державних АС належить автоматизованій системі державної статистики (АСДС). Відомі й інші державні АС, система обробки інформації з цін (АСОІ цін), система управління національним банком (АСУ банк), система обробки науково-технічної інформації (АСО НТІ) і т. ін.

Територіальні (регіональні) АС призначені для управління адміністративно-територіальним регіоном - АС області, міста, району.

Галузеві інформаційні системи управління призначені для управління підвідомчими підприємствами та організаціями.

Залежно від мети функціонування та завдань, які покладені на АС на етапах збору та змістової обробки даних, розрізняють такі типи АС: інформаційно-пошукові; інформаційно-довідкові; інформаційно-управлінські; інтелектуальні інформаційні системи та системи підтримки прийняття рішень.

Інформаційно-пошукові системи (ІСП) орієнтовані на розв'язування завдань пошуку інформації. Змістова обробка інформації в таких системах відсутня. В інформаційно-довідкових системах (ІДС) за результатами пошуку обчислюють значення арифметичних функцій. Інформаційно-управляючі, або управлінські, системи (відомі у вітчизняній літературі під назвою "автоматизовані системи організаційного управління") являють собою організаційно-технічні системи, які забезпечують вироблення рішення на основі автоматизації інформаційних процесів у сфері управління. Отже, ці системи призначені для автоматизованого розв'язування широкого кола завдань управління.

До інформаційних систем нового покоління належать системи підтримки прийняття рішень (СППР) та інформаційні системи, побудовані на штучному інтелекті (інтелектуальні АС).

Для задоволення законних прав необхідно постійно підтримувати наступні властивості інформації і систем її обробки: доступність інформації; цілісність інформації; конфіденційність інформації.

Захист персональних даних. Відповідно до закону суб'єкти підприємницької діяльності притягуються до адміністративної відповідальності за вчинення таких правопорушень: неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних; неповідомлення

або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних; ухилення від державної реєстрації бази персональних даних; недодержання встановленого законодавством про захист персональних даних порядку; невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних щодо усунення порушень законодавства про захист персональних даних.

За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності.

Організація контролю за виконанням правил обробки ПД. Контроль за забезпеченням захисту інформації в системі полягає у перевірці виконання вимог з технічного та криптографічного захисту інформації та здійснюється у порядку визначеному Адміністрацією. У системі, яка складається з кількох інформаційних та телекомунікаційних систем, ці правила можуть застосовуватись до кожної складової частини окремо.

**Опис персональних даних.** Загальний опис персональних даних представимо наступним чином. Нехай  $\epsilon$  множина суб'єктів, кількість яких  $C (0 < C < \infty)$ , всі суб'єкти пронумеровані і кожен має унікальний номер. Кожному суб'єкту відповідає своя множина елементів персональних даних. Формально множина персональних даних  $i$ -го суб'єкта визначимо як множину –  $ПД_i (i = 1, 2, \dots, C)$ . Для кожного елемента множини  $ПД_i$ ,  $\epsilon$  аналогічний

(відповідний) елемент  $C$  персональних даних. Вважаємо, що  $\bigcap_{i=1}^C ПД_i = \emptyset$ , тобто множина

персональних даних різних суб'єктів не перетинаються. Кожна множина  $ПД_i$ , відповідно до визначення персональних даних, складається з двох непересічних підмножин -

$ПД_i = ПД_{i1} \cup ПД_{i2}$ .  $ПД_{i1} = (nd_{i11}, nd_{i12}, \dots, nd_{i1M}) = \bigcup_{j=1}^{M_i} nd_{i1j}$  – підмножина первинних даних,

однозначно визначають номер  $i$  суб'єкта персональних даних (підмножина ідентифікаційних даних) (прізвище, ім'я, по батькові, дата народження, місце народження і т.д.). Тут  $nd_{i1j} = (nd_{i1j1}, nd_{i1j2}, \dots, nd_{i1jR_{i1j}})$  – підмножина даних типу  $j (j = 1, 2, \dots, M_i)$ , де  $R_{i1j}$  – розмірність цієї підмножини  $1 < R_{i1j} < \infty$ ;  $M_i$  - число типів даних, що однозначно визначають  $i$ -й суб'єкт.

Тип даних, як зазначалося, відповідає конкретній характеристиці суб'єкта даних, наприклад: прізвище, ім'я, дата народження і т.д. Число елементів кожної підмножини  $nd_{i1j} - R_{i1j}$ ,

визначається числом даних типу  $j$  по суб'єкту  $i$ . Число даних деяких типів може бути більше одиниці, наприклад, підмножина даних типу «Прізвище» може містити кілька елементів. У загальному випадку розмірності підмножин  $nd_{i1j}$  і  $nd_{i1k} (k, j = 1, 2, \dots, M_i; k \neq j)$  можуть бути

неоднаковими тобто  $R_{i1j} \neq R_{i1k}$ .

$ПД_{i2} = (nd_{i21}, nd_{i22}, \dots, nd_{i2N_i}) = \bigcup_{j=1}^{N_i} nd_{i2j}$  підмножина вторинних персональних даних про

$i$ -й суб'єкт (номер паспорта, ПІН, стан здоров'я, релігійна приналежність, адреса і т.д.), які не дозволяють конкретно визначити суб'єкт. Тут  $nd_{i2j} = (nd_{i2j1}, nd_{i2j2}, \dots, nd_{i2jR_{i2j}})$  - підмножина

даних типу  $j (j = 1, 2, \dots, N_i)$  де  $R_{i2j}$  - розмірність підмножини  $1 < R_{i2j} < \infty$ ;  $N_i$  - загальне число

типів даних про  $i$ -й суб'єкт. Тип даних тут також відповідає характеристиці суб'єкта, наприклад: номер паспорта, ПІН, адреса реєстрації, вартість власної нерухомості і т.і. Число елементів кожної підмножини  $nd_{i2j} - R_{i2j}$ , визначається числом даних типу  $j$  по  $i$ -му суб'єкту.

Можливі випадки, коли  $R_{i2j} > 1$ , ( $j = 1, 2, \dots, N_i$ ), наприклад, для даних типу «Номер паспорта». У загальному випадку, розмірності підмножин  $pd_{i2j}$  і  $pd_{i2k}$  ( $k, j = 1, 2, \dots, N_i; k \neq j$ ) також можуть бути неоднаковими тобто  $R_{i2j} \neq R_{i2k}$ . Вважаємо, що між елементами підмножин  $PD_{i1}$  і  $PD_{i2}$  (між елементами множини  $PD_i$ ) встановлені зв'язки, що дозволяють формувати персональні дані для і-го суб'єкта.

Зв'язки між елементами підмножин відповідають зв'язкам між аналогічними елементами персональних даних. Наявність зв'язків дозволяє проводити пошук потрібного елемента шляхом перегляду його зв'язків з іншими елементами. Зв'язки встановлюються, наприклад, в документах, виданих на певний набір персональних даних. Так, наприклад, елементи типу «Прізвище», «Ім'я», «По батькові» можуть бути пов'язані з елементами типу «ІПН», «Медична карта» і т.д. Множина всіх персональних даних, що відносяться до і-го суб'єкта, незалежно від їх фізичного розміщення, будемо називати повною множиною персональних даних.

Зв'язки між елементами повної множини персональних даних  $PD_i$  зручно представити у вигляді неорієнтованого графа, де вершинами є елементи підмножин  $PD_{i1}$  і  $PD_{i2}$ , а ребра показують зв'язки між вершинами (елементами множини персональних даних). Такий граф будемо називати графом повної множини персональних даних. Використання графової моделі дозволяє, наприклад, застосовувати методи оптимізації на графах для отримання оптимальних параметрів моделі.

**Висновки.** Результати проведеного дослідження та аналізу стану законодавчої бази по роботі з персональними даними, правил створення ІСПД і організації захисту персональних даних в таких системах, дозволяють зробити наступні висновки: законодавча база повинна постійно вдосконалюватися в режимі уточнення і доповнення, що обумовлено появою нових напрямків і застосуванням нових інформаційних технологій роботи з персональними даними; вирішення питань класифікації та, відповідно, захисту при створенні ІСПД в кожному конкретному випадку носить досить суб'єктивний характер, оскільки об'єктивна оцінка загроз, що завдається суб'єктам, пов'язаних з доступом до їх персональних даних, практично неможлива; запропоновані рішення для створення систем захисту персональних даних можуть привести до необґрунтованих витрат, «універсальність» пропонованих засобів і методів захисту багато в чому обумовлена їх надмірністю; пропоновані підходи до захисту занадто «чутливі», так як навіть незначні (за складом і обсягом) зміни в складі персональних даних можуть привести до необхідності істотних змін в системі захисту; контроль операторів персональних даних на основі звернень суб'єктів і планових перевірок є необхідним для підвищення відповідальності операторів.

Аналіз методів організації обробки і захисту ПД, показав, що пропоновані методи і створювані на їх основі системи захисту вимагають значних ресурсів для реалізації, мають сильну залежність від типу даних і високою надмірністю при практичному застосуванні для роботи з масивами даних невеликої розмірності. Тому в ряді випадків доцільно застосовувати методи, що знімають вимоги до конфіденційності ПД, що значно скорочує витрати на захист. Одним з ефективних і перспективних підходів до захисту ПД в інформаційних системах є знеособлення.

У зв'язку з цим доцільно провести дослідження в наступних напрямках: аналіз основних визначень і підходів до організації обробки персональних даних, створення математичної моделі персональних даних; розробка досить універсальних і мало витратних методів і засобів перетворення персональних даних, що забезпечують зниження вимог до захисту; серед таких методів можна виділити знеособлення персональних даних; розробка методики застосування знеособлення при організації захисту персональних даних; розробка методів оцінки якості захисту персональних даних при знеособлення; розробка інформаційної системи для реєстрації операторів персональних даних та контролю за їх діяльністю.

Зв'язки між елементами персональних даних  $ПД_i$  зручно представити у вигляді неорієнтованого графа, де вершинами є елементи підмножин  $ПД_{i1}$  і  $ПД_{i2}$ , а ребра показують зв'язки між вершинами (елементами множини персональних даних). Використання графової моделі дозволяє застосовувати методи оптимізації на графах для отримання оптимальних параметрів моделі.

Для зберігання знеособлених даних можна використовувати бази даних, файлові системи, інформаційні системи, які не мають спеціальних засобів захисту, які відповідають вимогам, визначеним у відповідних документах. У зв'язку з цим, процедури знеособлення можна розглядати як перспективні методи захисту і обробки персональних даних, мають досить широкі можливості для застосування на практиці.

#### ЛІТЕРАТУРА:

1. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия-Телеком, 2006. – 544 с.
2. Шаньгин В.Ф. Комплексная защита информации в корпоративных компьютерных системах: Учебн. пособие / В.Ф. Шаньгин - М.: ИД «ФОРУМ»: ИНФРА-М, 2010. – 592 с.
3. Щербаков А.Ю. Современная компьютерная безопасность. Практические аспекты. /А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.
4. Сабанов А.Г. Защита персональных данных в организациях здравоохранения // А.Г. Сабанов, В.Д. Зыков. - Москва, Горячая линия Телеком, 2012. – 206 с.
5. Грибунин В.Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
6. Васильков А.В. Безопасность и управление доступом в информационных системах: Учебное пособие// А.В. Васильков, И.А. Васильков - М.:ФОРУМ, 2010. – 368 с.
7. Разработка и эксплуатация автоматизированных информационных систем / Л.Г. Гагарина, Д.В., Киселев Е.Л. Федотова - М.: ИНФРА-М, ФОРУМ 2011 г. – 384 с.
8. Петрыкина Н.И. Правовое регулирование оборота персональных данных / Н.И. Петрыкина - М.: Статут, 2011. –134 с.
9. Кормен Т. Х. Часть VI. Алгоритмы для работы с графами // Т. Х. Кормен - Алгоритмы: построение и анализ = Introduction to Algorithms. – 2-е изд. – М.: Вильямс, 2006. – С. 1296.
10. Вифлеемский А.Б. Обработка персональных данных в образовательном учреждении: как выполнить требования законодательства / А.Б. Вифлеемский, И.Г. Лозинский - М.: «Сервис-Пресс», 2011. – 189 с.
11. Закон України Про захист персональних даних. [Electronic resource]. - Mode of access: <http://zakon1.rada.gov.ua/laws/show/2297-17>.
12. Порядок обробки персональних даних у базах персональних даних. [Electronic resource]. - Mode of access: [http://unba.org.ua/assets/uploads/legislation/poryadki/2017-11-16-poryadki-250\\_5a449b1c28668.pdf](http://unba.org.ua/assets/uploads/legislation/poryadki/2017-11-16-poryadki-250_5a449b1c28668.pdf).

#### REFERENCES:

1. Belov, E.B., Los, V.P., Mescheryakov, R.V. and Shelupanov A.A. (2006),” Osnovyi informatsionnoy bezopasnosti. Uchebnoe posobie dlya vuzov” [Fundamentals of Information Security. Textbook for high schools], М.: Goryachaya liniya-Telekom, 544p.
2. Shangin, V.F. (2010),” Kompleksnaya zaschita informatsii v korporativnyih kompyuternyih sistemah: Uchebn. posobie.” [Comprehensive information protection in corporate computer systems: Textbook], М.: ID «FORUM»: INFRA-M, 592p.
3. Scherbakov, A.Y. (2009),” Sovremennaya kompyuternaya bezopasnost. Prakticheskie aspektyi.” [Modern computer security. Practical aspects.],М.: Knizhnyiy mir, 2009. 352p.
4. Sabanov, A.G. and Zyikov, V.D. (2012),” Zashchita personalnyih danyih v organizatsiyah zdavoohraneniya” [Protection of personal data in health care organizations.], Moskva, Goryachaya liniya Telekom, 206 p.
5. Gribunin, V.G. and Chudovskiy, V.V. (2009),”Kompleksnaya sistema zaschityi informatsii na predpriyatii: ucheb. posobie dlya stud. vyissh. ucheb. zavedeniy” [Integrated information security system at

the enterprise: a textbook for students of higher educational institutions], M.: Izdatelskiy tsentr «Akademiya», 416 p.

6. Vasilkov, A.B and Vasilkov, I.A. (2010), "Bezopasnost i upravlenie dostupom v informatsionnyih sistemah: Uchebnoe posobie" [Security and Access Control in Information Systems: Textbook], M.: FORUM, 368p.

7. Gagarina, L.G., Kiselev, D.V. and Fedotova, E.L. (2011), "Razrabotka i ekspluatatsiya avtomatizirovannyih informatsionnyih sistem" [Development and operation of automated information systems], M.: INFRA-M, FORUM, 384p.

8. Petryikina, N.I. (2011), "Pravovoe regulirovanie oborota personalnyih dannyih." [Legal regulation of the turnover of personal data], M.: Statut, 134p.

9. Kormen, T. X. (2006), "Chast VI. Algoritmy dlya raboty s grafami" [Part VI. Algorithms for working with graphs], Algoritmy: postroyeniye i analiz = Introduction to Algorithms. - 2-e izd. M.: Vilyame, 1296p.

10. Vifleemskiy, A.B. and Lozinskiy, I.G. (2011), "Obrabotka personalnyih dannyih v obrazovatel'nom uchrezhdenii: kak vyipolnit trebovaniya zakonodatel'stva" [Processing of personal data in an educational institution: how to fulfill the requirements of legislation], M.: «Servis-Press», 189p.

11. Zakon UkraYini Pro zahist personalnih danih. [Electronic resource]. - Mode of access: <http://zakon1.rada.gov.ua/laws/show/2297-17>

12. Poryadok obrobki personalnih danih u bazah personalnih danih. [Electronic resource]. - Mode of access: [http://unba.org.ua/assets/uploads/legislation/poryadki/2017--11-16-poryadki-250\\_5a449b1c28668.pdf](http://unba.org.ua/assets/uploads/legislation/poryadki/2017--11-16-poryadki-250_5a449b1c28668.pdf)

**к.т.н., с.н.с. Мирошниченко О.В., к.т.н. Красильников С.Р., Ковальчук Я.В., Купратий В.О.  
ИССЛЕДОВАНИЯ И АНАЛИЗ МЕТОДОВ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

*В статье предложен подход к представлению персональных данных в виде неориентированного графа, использование графовой модели позволит применять методы оптимизации на графах для получения оптимальных параметров модели.*

*Исследования и анализ методов организации обработки и защиты персональных данных, показал, что предлагаемые методы и создаваемые на их основе системы защиты требуют значительных ресурсов для их реализации, имеют сильную зависимость от типа данных и высокую избыточность при практическом применении для работы с массивами данных небольшой размерности. Поэтому в ряде случаев целесообразно применять методы, которые снимают требования к конфиденциальности персональных данных, что значительно сокращает расходы на защиту. Одним из эффективных и перспективных подходов к защите персональных данных в информационных системах является обезличивание персональных данных. В связи с этим целесообразно провести исследования в следующих направлениях: анализ основных определений и подходов к организации обработки персональных данных, создание математической модели персональных данных; разработка достаточно универсальных и мало затратных методов и средств преобразования персональных данных, обеспечивающих снижение требований к защите. Среди таких методов можно выделить обезличивания персональных данных; разработка методики применения обезличивания при организации защиты персональных данных; разработка методов оценки качества защиты персональных данных при обезличивании; разработка информационной системы для регистрации операторов персональных данных и контроля за их деятельностью. Для хранения обезличенных данных можно использовать базы данных, файловые и информационные системы, которые не имеют специальных средств защиты, которые соответствуют требованиям, определенным в соответствующих документах. В связи с этим, процедуры обезличивания можно рассматривать как перспективные методы защиты и обработки персональных данных, имеют достаточно широкие возможности для применения на практике.*

*Ключевые слова: обезличивание данных, персональные данные, базы данных, средства защиты, информационные системы, конфиденциальность.*



*The article suggests an approach to the representation of personal data in the form of an undirected graph, the use of a graph model will make it possible to apply optimization methods on graphs to obtain optimal model parameters. Research and analysis of methods for organizing the processing and protection of personal data showed that the proposed methods and the protection systems created on their basis require significant resources for their implementation, have a strong dependence on the type of data and high redundancy in practical use when working with small data sets. Therefore, in a number of cases it is advisable to apply methods that remove the requirements for the confidentiality of personal data, which significantly reduces the cost of protection. One of the most effective and promising approaches to the protection of personal data in information systems is the depersonalization of personal data. In this regard, it is expedient to carry out researches in the following areas: analysis of the main definitions and approaches to the organization of personal data processing, the creation of a mathematical model of personal data; the development of sufficiently universal and low-cost methods and means of converting personal data that reduce the requirements for protection. Among such methods, one can distinguish the depersonalization of personal data; the development of methods for the use of depersonalization in the organization of protection of personal data; the development of methods for assessing the quality of personal data protection in the case of depersonalization; Development of an information system for the registration of personal data operators and control over their activities. To store depersonalized data, you can use databases, file and information systems that do not have special security features that meet the requirements specified in the relevant documents. In this regard, the procedures of depersonalization can be considered as promising methods of protecting and processing personal data, and have ample opportunities for practical application.*

*Keywords: depersonalization of data, personal data, databases, means of protection, information systems, confidentiality.*

