УДК 004.056.523:004.6-027.552 DOI: 10.31673/2412-4338.2024.028190

Бакаєв Олег Олександрович
Інститут програмних систем, Київ
ORCID 0009-0004-5427-1196

Суський Георгій Валерійович
Інститут програмних систем, Київ
ORCID 0000-0001-8049-1687

МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Анотація. *У сучасному цифровому суспільстві захист персональної інформації стає надзвичайно важливим завданням. З розвитком інформаційних технологій та зростанням обсягів даних, що обробляються інформаційними системами, підвищується ризик несанкціонованого доступу, крадіжки та зловживання конфіденційними даними. Метою роботи є аналіз підприємств для виявлення фактори, що впливають на інформаційну безпеку .а також розробка та теоретичне обґрунтування методів знеособлення та де-знеособлення персональних даних, що дозволяють забезпечити їх конфіденційність, а також правила організації обробки знеособлених даних. Ця тема є актуальною для фахівців з інформаційної безпеки, розробників програмного забезпечення, а також для організацій, що оперують значними обсягами персональних даних, з метою забезпечення належного рівня захисту інформації та мінімізації ризиків кіберзагроз. Аналіз методів організації обробки та захисту персональних даних, показав, що запропоновані методи та створювані на їх основі системи захисту вимагають значних ресурсів для реалізації, мають сильну залежність від типу даних і високу надмірність при практичному застосуванні для роботи з масивами даних невеликої розмірності. Тому у ряді випадків доцільно застосовувати методи, що знімають вимоги до конфіденційності персональних даних, що значно скорочує витрати на захист. У роботі розглянуто один із ефективних та перспективних підходів до захисту персональних даних в інформаційних системах – знеособлення. Розроблено методику та правила обробки знеособлених персональних даних із залученням зовнішніх операторів, що дозволяє здійснювати захист персональних даних як на рівні оператора, так і на рівні користувача. Запропонована методика особливо ефективна при використанні дата-центрів та технології хмарних обчислень для обробки персональних даних різних малобюджетних організацій.*

Ключові слова: *персональні дані, інформаційні системи, захист даних, знеособлення, управління якістю, інформаційна безпека.*

Bakaiev Oleh
Institute of Software Systems, Kyiv
ORCID 0000-0003-2219-8196

Susskiy Georgiy
Institute of Software Systems, Kyiv
ORCID 0000-0001-8049-1687

METHODS OF PROTECTING PERSONAL INFORMATION IN INFORMATION SYSTEMS

Abstract. *In today's digital society, the protection of personal information becomes an extremely important task. With the development of information technologies and the growth of volumes of data processed by information systems, the risk of unauthorized access, theft and misuse of confidential data increases. The purpose of the work is the analysis of enterprises to identify factors affecting information security, as well as the development and theoretical substantiation of methods of depersonalization and de-personalization of*

personal data, which allow to ensure their confidentiality, as well as rules for organizing the processing of depersonalized data. This topic is relevant for information security specialists, software developers, as well as for organizations that operate large volumes of personal data, in order to ensure an adequate level of information protection and minimize the risks of cyber threats. The analysis of the methods of 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 implementation, have a strong dependence on the type of data and high redundancy in practical application for working with small data sets. Therefore, in a number of cases, it is advisable to apply methods that remove requirements for the confidentiality of personal data, which significantly reduces the costs of protection. The paper considers one of the effective and promising approaches to the protection of personal data in information systems - depersonalization. The methodology and rules for processing depersonalized personal data with the involvement of external operators have been developed, which allows protection of personal data both at the level of the operator and at the level of the user. The proposed method is particularly effective when using data centers and cloud computing technology to process personal data of various low-budget organizations.

Keywords: *personal data, information systems, data protection, depersonalization, quality management, information security.*

1. Вступ.

Надання інформації завжди було однією з ключових умов належного управління як державою, так і кожною організацією. У той час, коли основним джерелом інформації була піктограма, вона була загальнодоступною, пізніше інформація обмежувалася листом, надісланим посланцем. З часом були розроблені набагато швидші та безпечніші методи передачі даних, але цей фактор завжди залишався найслабшою ланкою в усій системі. Наразі розвиток телекомунікаційних систем дозволяє значною мірою усувати помилки. Однак слід підкреслити, що люди залишаються як споживачами, так і творцями інформації. На даний момент можна виділити дві основні області втрати даних. Перша — це навмисна атака на систему зберігання інформації через напад на центри обробки даних, друга — це цільова атака на робочу силу з використанням методу фішингу для цієї мети. Розвиток інформаційно-комунікаційних технологій надав людині багато можливостей для цілеспрямованих дій. Інформація, що зберігається в інформаційних системах, є однією з найбільш вразливих до різних видів атак. Саме тому так важливо захистити інформацію в кожній компанії. Найбільш поширеними методами, які наразі використовуються злочинцями, є: комп'ютерне шахрайство, знищення даних або комп'ютерних програм, комп'ютерний саботаж, злом комп'ютерної системи, підслуховування.

2. Аналіз останніх досліджень і публікацій.

Безпека у звичайному розумінні розуміється як стан відсутності загрози і була бажаною в багатьох сферах людської діяльності протягом століть [1]. У контексті інформаційної безпеки ми говоримо про ефективне функціонування процесів в організації. У літературі інформаційна безпека визначається як «якість організації, вільна від загроз, пов'язаних з інформаційною безпекою» [2]. Важливим елементом захисту інформації також є його призначення, тобто захист цінної інформації для організації – інформації, а також середовища, створеного апаратним і програмним забезпеченням [3]. Визначаючи інформаційну безпеку, було зазначено ряд аспектів, перш за все конфіденційність, автентичність, доступність, цілісність, відповідальність, надійність [4]. В роботі [2] також вказують на приватність як на один із аспектів, які потребують захисту через стосунки з людиною. Персональна інформація – це інформаційні ресурси, які мають власну конфіденційність, яка визначається як міра важливості, яку надає інформації її автор або довірена особа, щоб вказати на необхідність її захисту [5].

Складність створення систем захисту інформаційних систем полягає в постійній зміні загроз. Це стає ще складнішим, якщо сама інформаційна система продовжує розроблятися та вдосконалюватися. Тому розвиток системи захисту має бути спланований з урахуванням закономірностей еволюції інформаційних систем та рекомендацій чинних нормативних документів щодо функціональних профілів захищеності [6-7].

У роботі [8] проведено аналіз основних профілів захищеності для різних етапів розвитку на прикладі інформаційних систем медичного призначення, з урахуванням нормативних документів. Надано рекомендації щодо доцільних переходів між цими етапами. Також запропоновано логічну послідовність впровадження стандартних функціональних профілів захищеності, які відповідають відповідним етапам розвитку системи.

Незважаючи на значний прогрес у розробці методів захисту інформації, розробка нових та вдосконалення існуючих методів захисту персональних даних залишається актуальним та необхідним.

3. Мета і задачі дослідження.

Метою роботи є аналіз підприємств для виявлення фактори, що впливають на інформаційну безпеку .а також розробка та теоретичне обґрунтування методів знеособлення та де-знеособлення персональних даних (ПД), що дозволяють забезпечити їх конфіденційність, а також правила організації обробки знеособлених даних.

Для досягнення поставленої мети було проведено дослідження за такими напрямками:

- аналіз завдань та методів забезпечення безпеки ПД;
- дослідження властивостей ПД, як об'єктів обробки та захисту;
- розробка методів знеособлення та де-знеособлення ПД.

4. Основні результати

4.1. Захист персональних даних як частина інтегрованої системи управління якістю та інформаційною безпекою.

Моніторинг стану безпеки вимагає ідентифікації та ідентифікації елементів інформаційної безпеки. Важливими елементами процесу управління інформаційною безпекою є ресурси, загрози, вразливі місця, наслідки, ризики, запобіжні заходи та залишковий ризик. На рівень обізнаності співробітників у сфері безпеки впливає багато факторів. На основі спостережень, проведених на підприємствах, було розроблено діаграму взаємозв’язків, що включає фактори, що впливають на обізнаність працівників підприємств у сфері інформаційної безпеки (рис. 1).

Рис. 1. Діаграма взаємозв’язку інформаційної безпеки

На основі спостережень, проведених на підприємствах, визначено фактори, що впливають на інформаційну безпеку. Ці елементи були розділені на чотири групи: безпека, осередок безпеки, навчання та загрози. На їх основі визначено фактори, що впливають на

обізнаність працівників у сфері інформаційної безпеки (Jędrzyjczyk, Kucęba, 2016). З метою належного управління інформацією в компанії, яка є основою забезпечення інформаційної безпеки, представляється доцільним вивчити задоволеність управління інформацією серед співробітників. На це запитання респонденти дали наступні відповіді (рис. 2).

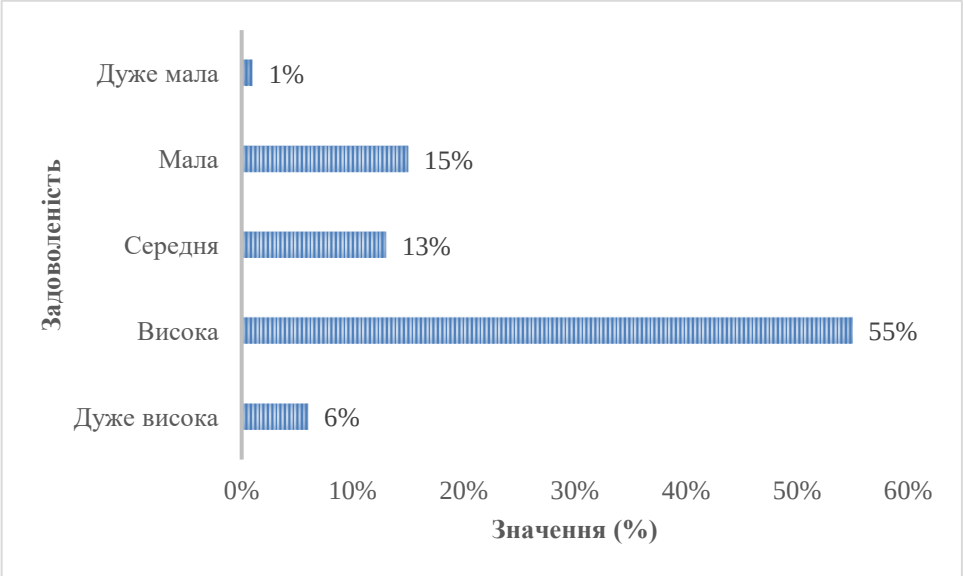

Рис. 2. Задоволеність працівників заходами інформаційної безпеки на досліджуваних підприємствах

Опитування показало, що працівники розуміють важливість управління інформацією для належного функціонування підприємства. Лише 16% працівників опитаних підприємств не бачать важливості інформаційної безпеки для підприємств. Двадцять чотири респонденти вказують на призначення інспектора із захисту персональних даних, і в цих випадках обов’язки та повноваження, які містять вимоги законодавства, були чітко визначені. Тому необхідно надати інспектору відповідні дозволи. Сорок два респонденти підтвердили, що вони чітко визначили ролі, обов'язки та повноваження щодо забезпечення інформаційної безпеки. Однак у 64 випадках респонденти вказали, що ключову роль відіграє менеджмент. Понад 25% респондентів не вказали відповідальність з цього приводу. Результати не є однозначними, і певним натяком в інтерпретації результатів є вкрай низький рівень поінформованості щодо вимог до безпеки персональних даних. Цитуючи результати дослідження, слід зазначити, що згідно з декларацією майже половина респондентів подає дані за межі України, з них 37% до країн ЄС. При такій низькій обізнаності респондентів щодо вимог можна зробити висновок про дуже ймовірні розбіжності в цьому відношенні. Відповіді на питання про наявність необхідної документації можна чітко оцінити. Лише 8 респондентів заявили про наявність необхідної політики безпеки персональних даних, але не всі з них вже мають інструкції з управління інформаційною системою. 21 респондент зазначив, що ці вимоги їх не стосується, а 15 – що не встановлювали зазначені документи. Аналіз такого типу документів ще більш вражаючий. Найчастіше це лише формальне виконання вимог, яке готується за формулою, яка навіть найменшою мірою не адаптована до реалій організації. Найчастіше це прояв повної необізнаності. В окремих випадках цей факт випливає з регламентації принципів нагляду за персональними даними в документації системи управління інформаційною безпекою.

4.2. Захист персональних даних як інтегрований елемент системи управління якістю та інформаційної безпеки

Зазвичай, компанія – це визнаний і великий постачальник багатьох продукції. Одна з ключових функцій компанії це продаж продукції чи послуг та обслуговування клієнтів. Специфіку організації найкраще відображає її карта процесу (рис. 3), розроблена як частина системи управління якістю та управління інформаційною безпекою, а також цілі, пов’язані зі стандартизацією та вимірюванням продуктивності.

Рис. 3 Карта процесів досліджуваного підприємства

Ключовими процесами є технологічні рішення, які по суті пов'язані з виробництвом. Це група процесів: виробництво, обробка, що забезпечує її якість, збут. Основні процеси побудовані процесами: якісне дослідження, технічна підтримка та обслуговування клієнтів. Крім того, було визначено процес вищого характеру - управління змінами, який поєднує в собі необхідність дотримання керівних принципів, застосовних у всій корпорації, та управління всередині організації.

4.3. Управління якістю, інформаційна безпека та захист персональних даних

Компанія чітко розподілила ролі у сфері управління якістю, безпеки та законодавчої відповідальності щодо захисту персональних даних. Ключову роль у цьому відіграє менеджер з якості та інформаційної безпеки, який також є інспектором із захисту персональних даних. Таким чином, на практиці ця особа несе повну відповідальність перед керівництвом за впровадження, підтримку та розвиток системи управління та взяла на себе переважну більшість обов’язків організації (оператора персональних даних). У рамках системи управління також є:

- власники процесу – відповідальні за управління даним процесом, починаючи від документації і закінчуючи вимірюваннями;
- власники баз персональних даних – призначені працівники, відповідальні за бази персональних даних. Вони також відповідають за звітність про осіб, які мають бути уповноважені обробляти дані;
- члени форуму безпеки – відповідають за оцінку загроз інформаційній безпеці, узгодження та прийняття планів управління ризиками. Форум безпеки також готує огляд керівництва, який відбувається покроково під час щотижневих засідань правління.

На практиці менеджер з якості та інформаційної безпеки є координатором дуже розпорошених дій, розташованих в окремих процесах. Відповідно до прийнятих припущень, реалізовані ним завдання були включені до групи десяти пріоритетних завдань для розвитку організації:

- процесний підхід та документація – передбачає перевірку карти процесів та підпорядкування її припущення щодо оптимізації та вимірювання ефективності через

те, що перше було підпорядковане лише вимогам стандартів, які становлять основу системи;

- управління ризиками – плани управління ризиками за результатами оцінки ризиків не є реальним, зрозумілим елементом вдосконалення системи;
- управління персональними даними – завдяки усвідомленню обсягу даних, які обробляються як оператор персональних даних і довірені головним офісом організації, а також завдяки універсальній передачі даних за межі зони ЄС.

Вимоги щодо захисту персональних даних повністю інтегровані з системою управління якістю та інформаційною безпекою, що гарантує відповідальність однієї особи безпосередньо перед керівництвом. Ключовими документами, пов'язаними з наглядом за персональними даними, є політика захисту персональних даних та інструкції з нагляду за IT-мережею, розроблені як частина процесу управління якістю та інформаційної безпеки.

У розглянутій компанії модель документації описана на двох рівнях. Перший рівень — це особливості процесів у формі так званих посібників з процесу, які посилаються на політики та інструкції. Перш за все згадуються ключові документи щодо захисту персональних даних :

- декларація про застосування, яка визначає всі гарантії, що застосовуються в організації, включаючи безпеку щодо IT-мереж та, ширше, інформаційно-комунікаційних технологій;
- плани забезпечення безперервності бізнесу та план відновлення після аварії;
- інструкції щодо роботи з інцидентами інформаційної безпеки;
- каталог послуг із зазначенням мінімальних параметрів надання послуг, у тому числі включаючи угоду стандартного рівня;
- інструкції з моніторингу та оцінки ефективності інформаційної безпеки.

Відповідно до вимог, системний адміністратор відповідає за ведення баз даних, у тому числі персональних даних. Вони вказані в контрольованому файлі як так званий відкритий реєстр. Кожна база даних характеризується назвою, основним користувачем, списком осіб, уповноважених обробляти персональні дані, зазначенням адміністратора бази даних, ідентифікацією мети обробки даних, характеристиками персоналу, наявною базою даних, типом даних, зібраних у база даних і структура даних. Крім того, реєстр доповнюється низкою інших більш детальних функцій. Забезпечити ефективний нагляд за цим надзвичайно важко, це серйозна проблема, оскільки йдеться про майже 50 баз даних і майже 250 працівників, колег, часто за межами компанії чи зони ЄС.

4.4. Захист персональних даних в інформаційних системах методом знеособлення

Важливе значення забезпеченню безпеки персональних даних (ПД) надається під час їх обробки в автоматизованих інформаційних системах ПД (ІСПД), які містять бази ПД, використовують відповідні інформаційні технології та технічні засоби. Це пов'язано з появою в таких системах нових можливостей несанкціонованого доступу до інформації щодо каналів зв'язку та із застосуванням шкідливого програмного забезпечення, наявністю ринку послуг із забезпечення протиправного доступу до інформації, що міститься в базах даних.

Для вибору необхідних методів та способів захисту ПД. Необхідно провести класифікацію ІСПД. У ході класифікації визначаються:

- категорія та обсяг оброблюваних ПД,
- тип та структура інформаційної системи,
- режими обробки ПД
- розмежування прав доступу користувачів,
- наявність підключень до мереж.

Аналіз документів показав, що ІСПД всіх класів мають забезпечувати конфіденційність ПД.

Заходи щодо захисту ІСПД трудомісткі та можуть призвести до значних фінансових та тимчасових витрат, пов'язаних з одержанням необхідних ліцензій, підготовкою персоналу,

встановленням сертифікованих засобів захисту. Крім того, вимоги до створення систем захисту роблять її надто чутливою до змін специфіки оброблюваних ПД.

Для усунення зроблених зауважень доцільно проводити обробку знеособлених ПД, що знімає вимоги до забезпечення їх конфіденційності.

Для аналізу властивостей ПД та визначення вимог до процедури знеособлення розроблено модель ПД, що дозволяє визначити процедури знеособлення, отримати умови, при виконанні яких ПД стають знеособленими.

При побудові моделі кожному суб'єкту i відповідала своя множина елементів ПД - Ω_i $(i = 1, 2, \dots, D)$. Множина Ω_i складається з підмножин, що не перетинаються – $\Omega_i = \Omega_{i1} \cup \Omega_{i2}$.

$\Omega_{i1} = (\omega_{i11}, \omega_{i12}, \dots, \omega_{i1Mi}) = \bigcup_{j=1}^{Mi} \omega_{i1j}$ - підмножина первинних даних, однозначно визначаючих (ідентифікуючих) суб'єкт i. Тут $\omega_{i1j} = (\omega_{i1j1}, \omega_{i1j2}, \dots, \omega_{i1\,jR_{i1j}})$ – підмножина даних типу j (j=1, 2, … , M_i), де R_{i1j} – розмірність цієї підмножини $(\infty > R_{i1j} \geq 1)$; M_i – число типів.

$\Omega_{i2} = (\omega_{i21}, \omega_{i22}, \dots, \omega_{i2Ni}) = \bigcup_{j=1}^{Ni} \omega_{i2j}$ - підмножина вторинних даних про суб'єкт i, які не дозволяють ідентифікувати суб'єкт Тут $\omega_{i2j} = (\omega_{i2j1}, \omega_{i2j2}, \dots, \omega_{i2\,jR_{i2j}})$ – підмножина даних типу j (j=1, 2, … , N_i), де R_{i2j} – розмірність підмножини $(\infty \geq R_{i2j} \geq 1)$; N_i – число типів.

Між елементами підмножин Ω_{i1} та Ω_{i1} встановлені зв'язки, які дозволяють формуати персональні дані суб'єкта *i.*

Множина Ω_i всіх персональних даних, що відносяться до суб'єкту *i*, є повною множиною персональних даних суб'єкта. Зв'язки між елементами множини Ω_i зручно представляти у вигляді неорієнтованого графу $\boldsymbol{\Gamma(\Omega_i, X_i)}$, де $\boldsymbol{\Omega_i}$ - множина вершин графа, що відповідає елементам множини $\boldsymbol{\Omega_i}$, X_i - множина ребер. Було досліджено властивості графа $\boldsymbol{\Gamma(\Omega_i, X_i)}$, обумовлені особливостями зв'язків між ПД суб'єкта. Показано, що для будь-якої пари вершин існує хоча б один шлях, який пов'язує ці дві вершини. Визначено властивості даних, які використовуються при знеособленні.

Розглянемо підхід до організації системи обробки ПД, коли в оператора зберігаються та обробляються знеособлені дані. Ідентифікація результатів обробки (ПД, отриманих внаслідок обробки) проводитися засобами користувача чи суб'єкта.

Суть полягає в поділі вихідної множини ПД суб'єкта – $\boldsymbol{\Omega}$ на первинні (ідентифікаційні) - Ω_1, і вторинні - Ω_2 та присвоєнні первинним і вторинним даними єдиного ідентифікатора. Ці дії проводяться засобами (програмними) користувача чи суб'єкта під час реєстрації даних. Ідентифікаційні дані разом з ідентифікатором зберігаються в ідентифікаційних базах даних користувача та кожного пов'язаного з ним суб'єкта. Вторинні дані, разом з ідентифікаторами, знеособлюються та надходять для обробки в ІСПД оператора, який, не маючи бази ідентифікаційних даних, не в змозі провести де-знеособлення та ідентифікацію ПД.

Знеособлені ПД після обробки де-знеособлюються та ідентифікуються з використанням ідентифікаційної бази даних.

Розроблено структуру даних, що обробляються в системі (рис. 4).

Схема організації обробки ПД не вимагає забезпечення їхньої конфіденційності в оператора та забезпечує захист від несанкціонованого доступу суб'єктів та користувачів, оскільки ідентифікаційні бази даних створюються для кожної групи користувачів та суб'єктів, об'єднаних рішенням загальних завдань. Проблема захисту персональних даних виникла для малобюджетних організацій (вузи, лікарні, школи, туристичні фірми тощо). Такі організації не мають апаратних та програмних ресурсів, підготовленого персоналу, досвіду та фінансових можливостей для забезпечення обробки ПД.

Для вирішення проблеми доцільно забезпечити цим організаціям набір послуг для роботи з ПД шляхом залучення зовнішніх операторів у вигляді спеціалізованих центрів

обробки ПД (далі - центри). Кожен такий центр може обслуговувати групу організацій, що входять до зони його обслуговування, забезпечуючи захист та надання ПД користувачам.

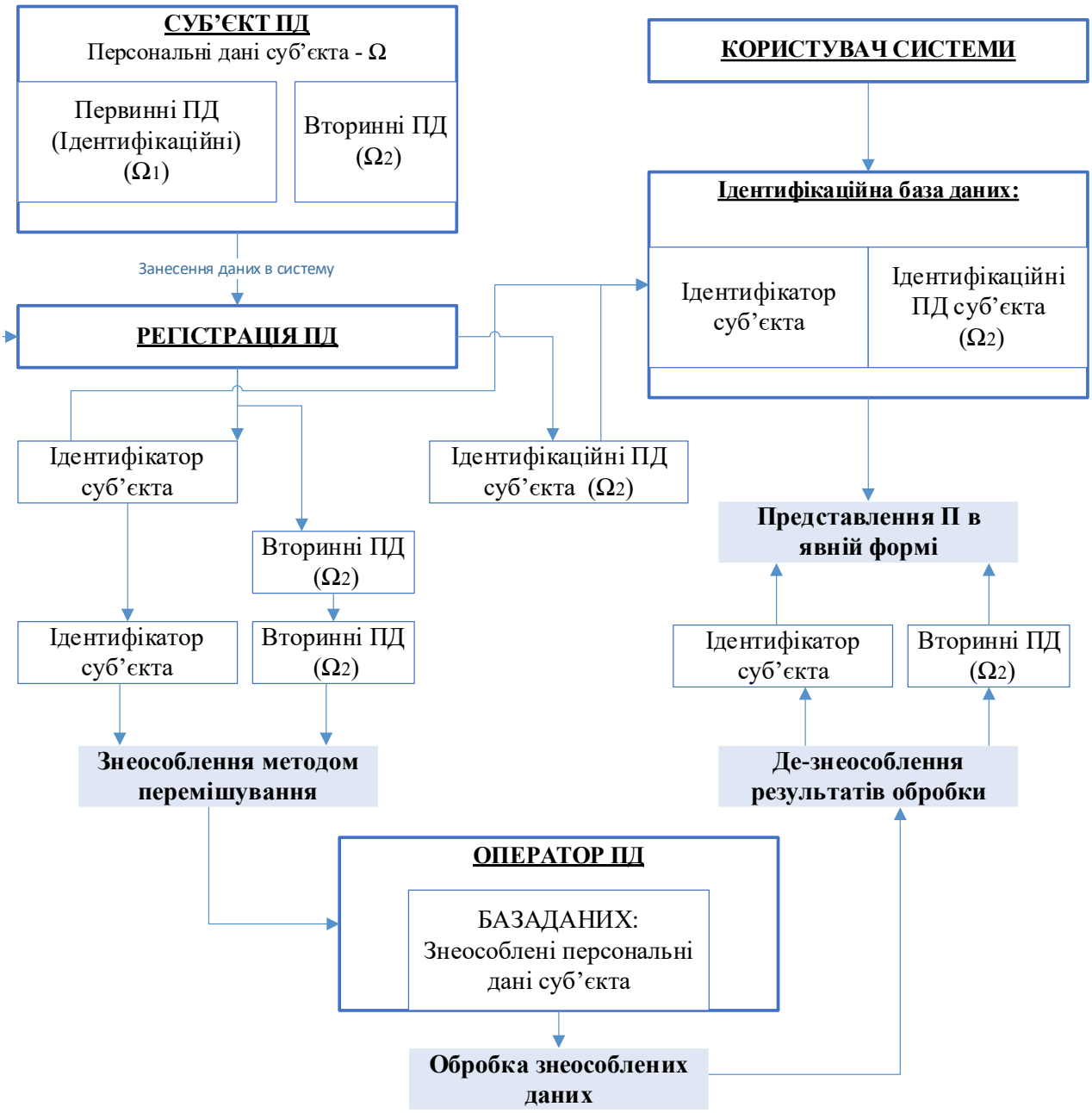

Рис 4. Узагальнена схема захищеної обробки ПД

У свою чергу, центри можуть бути пов'язані в мережу, утворюючи єдиний інформаційний простір ПД.

Послуги центру, що надаються користувачам, включають:

- збирання та зберігання ПД (у знеособленій формі);
- забезпечення санкціонованого доступу користувачів до ПД;
- захист збережених ПД засобами центру;
- захист ПД при взаємодії з користувачами каналами зв'язку;
- обробку ПД за погодженими з користувачами алгоритмами;
- зв'язок та інформаційна взаємодія з іншими подібними центрами.

Користувачі центру створюють робочі станції (клієнти). Центр через захищене середовище передачі даних побудовану на базі територіальної (регіональної, муніципальної, корпоративної) телекомунікаційної системи, зв'язується з клієнтськими місцями користувачів, що входять до його зони обслуговування, утворюючи локальну інформаційну систему обробки ПД.

При такій організації також вирішується проблема персистентних (довготривалих) даних, які можуть залишатися в центрі після завершення обробки, оскільки в центрі є лише знеособлені дані, а де-знеособлення засобами центру неможливе. Показано можливості об'єднання центрів у систему, що дозволяє створювати інформаційні простори ПД на вирішення різних завдань, тобто. створювати спеціалізовані хмари з обробки ПД.

5. Висновки.

Інформаційна безпека є важливим аспектом управління бізнесом. Враховуючи його специфіку, він може бути критичним через ринкову вартість, яка може вплинути на конкурентну перевагу. Персональні дані повинні бути захищені в будь-якому випадку, наприклад, через вимоги, викладені в правових аспектах. Відповіддю на потреби і навіть вимоги ринку є системні рішення в області управління безпекою даних. Вони можуть базуватися на міжнародно визнаному стандарті ISO/IEC 27001. При впровадженні, підтримці та розвитку системи управління інформаційною безпекою необхідно виконувати декілька груп вимог. Необхідною умовою для створення та впровадження ефективної системи управління інформаційною безпекою є виконання вимог законодавства, в тому числі щодо захисту персональних даних. Результати дослідження проведені31’у на вибірці відібраних підприємств із додатковим аналізом одного з них, свідчать про дуже низьку обізнаність працівників щодо необхідності захисту персональних даних, що може спричинити недостатню турботу про права їх власників. Нерозсудливість у цій сфері проявляється навіть у незнанні законодавчої бази, встановлення та документування необхідної політики та інструкцій, а також у збереженні записів бази даних. На обстежених підприємствах виникають критичні несумісності; в цьому випадку представники оператора персональних даних можуть бути притягнуті до кримінальної відповідальності та втратять довіру на ринку.

Аналіз методів організації обробки та захисту персональних даних, показав, що запропоновані методи та створювані на їх основі системи захисту вимагають значних ресурсів для реалізації, мають сильну залежність від типу даних і високу надмірність при практичному застосуванні для роботи з масивами даних невеликої розмірності. Тому у ряді випадків доцільно застосовувати методи, що знімають вимоги до конфіденційності ПД, що значно скорочує витрати на захист. У роботі розглянуто один із ефективних та перспективних підходів до захисту ПД в інформаційних системах – знеособлення.

Список використаної літератури

1. Żywiołek, J. Zarządzanie wiedzą o systemie bezpieczeństwa i higieny pracy w przedsiębiorstwie. In: *Światowy Dzień Bezpieczeństwa i Ochrony Zdrowia w Pracy*, 2017. pp. 114.

2. Mottord, H.J. and Whitman, M.E. Management of Information Security, 2nd ed., Boston: Thomson. 2008.

3. Humphreys, E., Implementing the ISO/IEC 27001. *Information Security Management System Standard*, Artech House, Norwood.

4. Żywiołek, J. Monitoring of Information Security System Elements in the Metallurgical Enterprises, *MATEC Web of Conferences*. 2019. Available at: https://www.matec-conferences.org/articles/matecconf/pdf/2018/42/matecconf_qpi2018_01007.pdf.

5. Białas, A. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. 2017. P. 550

6. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено нак. Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 р. №22. зі Зміною №1, затвердженою наказом Адміністрації Держспецзв’язку від 15.10.2008 № 172.: НД ТЗІ 2.5-005-99. – 2008. – 20 с.

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

7. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затв.нак. Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.1999 р. №22 із змінами згідно нак. Адміністрації Держспецзв'язку від 28.12.2012 № 806: НД ТЗІ 2.5-004-99. [електронний ресурс] – 2012. – Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342

8. Шевченко А.В. Стабілізація функціональної стійкості інформаційної системи шляхом управління динамікою розвитку профілів захищеності / Толубко В.Б., Курченко О.А., Шевченко А.В. // *Сучасний захист інформації.* – 2018. – №3. – С.51-57.

References

1. Żywiołek, J. Knowledge management about the occupational health and safety system in the enterprise. In: World Day for Safety and Health at Work, 2017. pp. 114.

2. Mottord, H.J. and Whitman, M.E. Management of Information Security, 2nd ed., Boston: Thomson. 2008.

3. Humphreys, E., Implementing the ISO/IEC 27001. Information Security Management System Standard, Artech House, Norwood.

4. Żywiołek, J. Monitoring of Information Security System Elements in the Metallurgical Enterprises, MATEC Web of Conferences. 2019. Available at: https://www.matec-conferences.org/articles/matecconf/pdf/2018/42/matecconf_qpi2018_01007.pdf.

5. Białas, A. Security of information and services in a modern institution and company. 2017. R. 550

6. Klasyfikatsiya avtomatyzovanykh system i standartni funktsional′ni profili zakhyshchenosti obroblyuvanoyi informatsiyi vid nesanktsionovanoho dostupu. Zatverdzheno nak. Departamentu spetsial′nykh telekomunikatsiynykh system ta zakhystu informatsiyi SB Ukrayiny vid 28 kvitnya 1999 r. №22. zi Zminoyu №1, zatverdzhenoyu nakazom Administratsiyi Derzhspetszv″yazku vid 15.10.2008 № 172.: ND TZI 2.5-005-99. – 2008. – 20 s. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

7. Kryteriyi otsinky zakhyshchenosti informatsiyi v komp″yuternykh systemakh vid nesanktsionovanoho dostupu. Zatv.nak. Departamentu spetsial′nykh telekomunikatsiynykh system ta zakhystu informatsiyi SB Ukrayiny vid 28.04.1999 r. №22 iz zminamy z·hidno nak. Administratsiyi Derzhspetszv'yazku vid 28.12.2012 № 806: ND TZI 2.5-004-99. [elektronnyy resurs] – 2012. – Rezhym dostupu: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342

8. Shevchenko A.V. Stabilizatsiya funktsional′noyi stiykosti informatsiynoyi systemy shlyakhom upravlinnya dynamikoyu rozvytku profiliv zakhyshchenosti / Tolubko V.B., Kurchenko O.A., Shevchenko A.V. // Suchasnyy zakhyst informatsiyi. – 2018. – №3. – S.51-57.