

Personnel reserve is one of the elements of human resources. Personnel reserve in the system of the Ministry of Internal Affairs is a socio-legal institution; its organizational mechanism promotes nominating candidates for filling a vacant post of heads (chiefs) depending on their professional and personal qualities, getting the required knowledge, skills, realization of the subjective right of an employee to promotion.

The analysis proves that the personnel reserve should be considered in three main aspects: as a leading body, the realization of the right of the employee (police officer, serviceman, public official) to promotion (official career) taking into account the results of the service activity, record of service (work), the level of proficiency and professional education; as HR technology that provides the formation of professional staff in government bodies; as a group of employees (officials, citizens) possessing the ability to management that meets the requirements of the personnel reserve.

Key words: *human resources, personnel reserve, system of the Ministry of Internal Affairs, official career.*

Стаття надійшла 22 лютого 2018 р.

УДК 342.681.3:519.872

С. С. Єсімов

ОСОБЛИВОСТІ ПРАВОВОГО РЕЖИМУ ІНФОРМАЦІЙНИХ СИСТЕМ З ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Досліджено особливості правового режиму інформаційних систем з обробки персональних даних. На підставі системного аналізу законодавства України, інших нормативно-правових актів розкрито сутність правового режиму інформаційних систем з обробки персональних даних, розглянуто класифікацію персональних даних.

Проаналізовано правові засоби захисту персональних даних, що обробляються в інформаційних системах у контексті відповідальності за порушення законодавства про персональні дані.

Ключові слова: *персональні дані, інформаційні системи, обробка персональних даних, захист персональних даних.*

Постановка проблеми. Інформаційно-комунікаційні технології дають змогу проводити збір, обробку, зберігання та розповсюдження значних обсягів інформації, що мають важливе соціальне значення, та інформації, що відноситься до категорії персональних даних, необхідних для більш ефективного функціонування різних державних

механізмів, розвитку суспільних процесів, реалізації прав і свобод людини та громадянина. Удосконалення інформаційних технологій та збільшення обсягу інформації забезпечує отримання доступу та використання різних банків і баз даних для будь-яких суб'єктів інформаційної сфери. Використовуючи інформаційні технології та маючи певний набір персональних даних, що використовується приватними особами для управління своїми матеріальними та фінансовими ресурсами, можна отримати неправомірний доступ та права на володіння цим ресурсом.

Розвиток різних інформаційних систем, зокрема і відкритих, має одну із своїх цілей захисту від витоків даних і запобігання несанкціонованому доступу до інформації персонального характеру. Це актуалізує та збільшує значущість різноманітних засобів захисту інформації технічними та законодавчими засобами.

Стан дослідження. Теоретичні аспекти правового режиму інформаційних систем з обробки персональних даних відображені у працях із загальної проблематики персональних даних таких відомих вчених, як: В. Авер'янов, Г. Атаманчук, О. Андрійко, О. Бандурка, Ю. Битяк, Л. Біла, Н. Бортник, В. Гаращук, Т. Коломоєць, М. Ковалів, В. Колпаков, А. Комзюк, О. Кузьменко, В. Ортинський, О. Остапенко, Д. Приймаченко, М. Тищенко, В. Шамрай та ін. Водночас адаптація національного законодавства до вимог ЄС викликають потребу комплексного аналізу проблем захисту персональних даних, які обробляються в інформаційних системах.

Метою статті є аналіз особливостей правового режиму інформаційних систем з обробки персональних даних.

Виклад основних положень. Угода про асоціацію України і ЄС зумовила низку нововведень у діяльність органів державної влади, серед яких чільне місце займають процеси інтеграції, що змінюють профіль системи суспільних відносин і впливають на розвиток національного права [1, с. 135]. У Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних, ратифікованій Законом України від 06.07.2010 № 2438-VI «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» під персональними даними розуміється інформація, що стосується конкретної особи чи особи, яка може бути ідентифікована («суб'єкт даних»).

Поняття «персональні дані» широко застосовується у багатьох нормативно-правових актах. Конституція України визначає як обо-

в'язкову умову згоду особи на збирання, зберігання, використання та розповсюдження інформації про приватне життя особи. Про це йдеться і у ст. 32 Конституції України, що збір, зберігання, використання та розповсюдження інформації про приватне життя особи без його погодження не допускаються. Згідно з основним джерелом регулювання відносин у сфері персональних даних Законом України від 01.06.2010 р. № 2297-VI «Про захист персональних даних» до них належить інформація про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Під інформаційними системами персональних даних розуміється сукупність персональних даних, які містяться в базах даних і інформаційних технологіях та технічних засобах, що забезпечують їх оброблення.

Зауважимо, що інформаційні системи персональних даних, у контексті Закону України від 05.07.1994 № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах» володіють такими ж компонентами та властивостями. Відмінність полягає у семантичному наповненні баз даних, тобто в утриманні в інформаційних системах персональних даних, до яких можна віднести: загальнодоступні персональні дані; персональні дані спеціальної категорії та біометричні дані. У перших двох випадках йдеться про семантичні властивості інформації, що стосується суб'єкта, а в разі біометричних даних – про специфічну технічну реалізацію ідентифікації, оскільки біометричні дані – це фізіологічні та біологічні особливості людини, тобто технічно реалізовані засоби ідентифікації суб'єкта з використанням ознак його фенотипу.

Наголосимо, що у роз'ясненні Міністерства юстиції України від 21.12.2011 р. «Деякі питання практичного застосування Закону України «Про захист персональних даних» вказано, що законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, в тому числі при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя [2].

Це підтверджує тезис про невизначеність терміна «персональні дані» та елементів правового режиму, що відносяться до персональних даних.

Ж. Удовенко виокремлює персональні дані в самостійну різновидність інформації з обмеженим доступом, основною особливістю якої є те, що більшість з них відкриті, але в певний момент можливо

обмеження доступу до них та їх використання з боку суб'єкта персональних даних [3].

Правовий режим конфіденційної інформації заснований на принципі збереження її в таємниці, а також заборону її збору та розголосу. Водночас можна говорити і про самостійний режим захисту персональних даних, так і про їх захист в режимі державної таємниці або іншого обмеженого доступу (службові таємниці, таємниці особистого та сімейного життя).

Персональні дані включаються в інформаційні системи різних організацій за ініціативою самої особи або на підставі закону для реалізації його прав, свобод і обов'язків за участі у найрізноманітніших соціальних відносинах. Будь-яка класифікація є умовною; в законі не можна враховувати безліч можливих ситуацій. На думку Р. Куценко, доцільно законодавчо закріпити поняття та зміст цієї категорії, а також регламентацію обсягу достатньої та обов'язкової інформації [4, с. 81]. Водночас до інформаційних систем, що містять персональні дані, висувають високі вимоги та доволі строгу відповідальність за порушення цих вимог.

За визначенням А. Новицького та А. Дяковського, які досліджували правове регулювання інформаційних баз даних, що містять персональні дані, база даних за своєю правовою природою є ширшим поняттям, ніж база персональних даних, включає сукупність взаємопов'язаних і систематизованих загальних елементів, що в сукупності утворюють базу даних. Своєю чергою, база персональних даних включає тільки окремі вужчий напрям – персональні дані. За таких обставин база даних як ширше поняття може включати персональні дані в сукупності з іншими елементами, а база персональних даних – лише сукупність даних у сфері оброблення даних фізичних осіб [5, с. 178].

У контексті формування інформаційних баз даних доцільно розділити персональні дані ідентифікації та персональні дані, які характеризують особу.

Персональні дані ідентифікації належать до даних, неправомірно володіння якими однозначно може завдати шкоди власнику цих ідентифікацій, використання яких потребує підвищеного захисту під час зберігання і обробки. Персональні дані, які характеризують особу, але не є даними ідентифікації, доцільно розділити на загальнодоступні, важливі та використання яких може завдати шкоди суб'єкту. Доцільно визначити режим персональних даних, використання яких може завдати шкоди суб'єкту, на самого суб'єкта при укладенні договорів про використання персональних даних між суб'єктом і оператором.

Суб'єктів правовідносин у сфері персональних даних можна розділити на категорії: суб'єкти, що надають персональні дані – фізичні особи; суб'єкти, які проводять обробку персональних даних (оператори); суб'єкти, що передають персональні дані; суб'єкти, що використовують оброблені персональні дані.

Оператори, незалежно від їх відомчої приналежності, повинні залучати до обслуговування інформаційних систем (зберігання, обробки та видачі персональних даних) спеціально навчених осіб і мати дозволи (ліцензії) на роботу з таким типом систем. Законодавчо встановлені заходи відповідальності за неправомірні дії з персональними даними, але немає диференціації залежно від того, які дані піддавали неправомірній обробці, розголошенню тощо. Необхідність зберігання та обробки персональних даних з урахуванням їх згаданої категоризації в автоматизованих інформаційних системах зумовлюють необхідність застосування спеціальних правових режимів у відношенні інформаційних систем, що забезпечують зберігання та обробку.

Згідно зі ст. 2 Закону України «Про захист персональних даних» обробка персональних даних здійснюється з використанням інформаційних (автоматизованих) систем. У нормативно-правових актах немає визначення поняття «інформаційна система для обробки персональних даних». Відповідно, інформаційна система для обробки персональних даних – це сукупність персональних даних, що містяться в базі даних, інформаційних технологій і технічних засобів, що дають змогу здійснювати обробку персональних даних з використанням засобів автоматизації. Обробка персональних даних в інформаційних системах представляє дію або сукупність дій, що здійснюються з використанням засобів автоматизації із персональними даними, включаючи збирання, записування, систематизацію, накопичення, зберігання, уточнення (оновлення, зміна), вилучення, використання, передачу (розповсюдження, надання, доступ), *знеособлення*, видалення, знищення персональних даних.

Обробка персональних даних в інформаційних системах повинна відповідати таким принципам обробки: законна та справедлива основа; обробка повинна обмежуватися досягненням конкретних, певних і законних цілей. Загальним правилом обробки персональних даних в Європейському Союзі є наявність угод суб'єкта даних на їх обробку. Будь-який виняток має бути передбачено законами. Наприклад, відповідно до законодавства обробка персональних даних може продовжуватися після відкликання згоди суб'єктом, навіть якщо йдеться про спеціальні категорії персональних даних, що стосуються расової,

національної приналежності, політичних поглядів, релігійних чи філософських переконань, стану здоров'я, інтимного життя у випадках, передбачених у п. 7 ч. 2 ст. 7 «Особливі вимоги до обробки персональних даних» Закону України «Про захист персональних даних».

Однією з основних причин актуальності внутрішніх загроз інформаційній безпеці є несанкціонований витік інформації за межі захищених інформаційних систем, обсяг якої має сталу тенденцію до зростання. Опинившись за межами захищеної інформаційної системи, персональні дані стають доступними практично необмеженому колу користувачів і можуть бути знищені чи спотворені, а також можуть бути використані з метою завдання шкоди особі, якої стосуються і моральної і матеріальної [6, с. 65]. Практично всі органи державної влади та місцевого самоврядування створюють і працюють з інформаційними системами персональних даних і зобов'язані забезпечити їх конфіденційність. У більшості цих органів діють внутрішні акти, що регулюють правила обробки персональних даних і встановлюють коло осіб, допущених до такої обробки, та відповідальність за порушення режиму захисту.

У всіх органах питання організаційно-технічних заходів захисту персональних даних пов'язані з проблемою інсайдерства, що з атаками хакерів є однією з головних загроз захисту персональних даних.

Загальні вимоги до обробки персональних даних в інформаційних системах містяться у Типовому порядку обробки персональних даних, затвердженому наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14.

Відповідно до Типового порядку обробки персональних даних головними критеріями у забезпеченні захисту є вміст і обсяг персональних даних; актуальність загрози; ознака того, чи є співробітник оператором чи ні. Шкода суб'єкта та види діяльності оператора і не розглядаються. Актуальним, але не зрозумілим з боку безпосереднього застосування, є введення низки дефініцій, зокрема автоматизованої системи.

Безпеку персональних даних під час їх обробки в інформаційній системі забезпечує оператор або особа, яка на підставі договору з оператором зобов'язується обробляти персональні дані. Як зазначає Б. Криклевенко, наказом Уповноваженого від 08.01.2014 № 1/02-14 затверджено Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує

роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації. Основним критерієм при визначенні того, чи становить певна обробка такий ризик, є те, які категорії персональних даних обробляються, що визначено у п. 1.2 Порядку повідомлення. Сьогодні можна виділити низку організаційно-технічних проблем, спрямованих на забезпечення безпеки персональних даних в інформаційних системах [7].

По-перше, оскільки не є загальнодоступними персональні дані, які належать до категорії конфіденційної інформації, для здійснення заходів захисту необхідно отримати ліцензію Державної служби спеціального зв'язку та захисту інформації України на діяльність у галузі технічного захисту конфіденційної інформації. Під час використання засобів криптографічного захисту інформації також необхідна наявність ліцензій. Водночас отримання зазначених ліцензій вимагає від організації наявності висококваліфікованого персоналу, спеціального обладнання та приміщень, що часто є нелегким завданням для працівників багатьох організацій.

Іншою проблемою є безпрецедентно високі вимоги, що висуваються до системи захисту. Наприклад, рівень захисту для деяких інформаційних систем персональних даних відповідає рівню захисту державної таємниці. Зокрема обов'язковим є забезпечення захисту інформації від витоків за рахунок електромагнітних випромінювань і наведень від засобів обчислювальної техніки та ліній зв'язку. Також слід враховувати, що до такого класу належать системи, в яких обробляється велика кількість інформації та системи, в яких обробляються спеціальні категорії персональних даних.

Існує низка підходів, що дають змогу забезпечити захист персональних даних відповідно до вимог ціною розумних витрат. Насамперед знизити витрати на побудову системи захисту можна шляхом вибору архітектури самої інформаційної системи на етапі її проектування. Наприклад, поділ великої інформаційної системи персональних даних на кілька територіальних дозволяє скоротити кількість персональних даних, оброблюваних у кожній системі, а використання умовних ідентифікаторів дає можливість обмежити доступ до даних.

Особливу зацікавленість з погляду «архітектури» побудови систем набуває технологія термінального доступу, при якій вся обробка даних здійснюється на сервері, а робочі станції використовуються тільки для відображення інформації і отримання даних від користувача. За правильного використання подібний підхід дозволяє

заощадити на засобах захисту і атестації за вимогами безпеки. Водночас зменшуються витрати на управління інформаційною інфраструктурою та закупівлю засобів обчислювальної техніки за рахунок централізації системи і зниження вимог до апаратних характеристик комп'ютерів користувачів.

Однією з проблем, зумовлених використання мережі Інтернет під час обробки персональних даних з використанням інформаційних систем, є відсутність нормативної основи, що б дала змогу реалізувати зазначені дії з забезпеченням їх безпеки. Подібна ситуація пов'язана з двома факторами: у законодавстві недостатньо гарантій забезпечення прав суб'єктів персональних даних в процесі їх транскордонної обробки. Також необхідно враховувати, що конфіденційна інформація і персональні дані по-різному визначаються в різних державах. Ще однією особливістю персональних даних є те, що в процесі ідентифікації найчастіше зацікавлений саме суб'єкт персональних даних, який визначає характер впливу на його приватне життя діями третіх осіб.

На законодавчому рівні визначено лише один вид суб'єктів відносин, пов'язаних з процесом обробки персональних даних – оператор. Під ним розуміється державний орган, орган місцевого самоврядування, юридична чи фізична особа, яка самостійно або спільно з іншими особами організують і (або) здійснюють обробку персональних даних, визначають цілі обробки та склад персональних даних, що підлягають обробці, дії (операції), що здійснюються з персональними даними.

З погляду на дослідження М. Різака, операторів обробки персональних даних доцільно розділити на дві групи: перша – органи державної влади та місцевого самоврядування, організації та підприємства, які визначають мету збору та напрями роботи з інформацією про суб'єктів персональних даних і створюють автоматизовані інформаційні системи персональних даних; друга – спеціалізовані організації (приватні організації та державні унітарні підприємства), яким в порядку аутсорсингу передаються функції з обробки персональних даних [8, с. 70].

Органи державної влади та місцевого самоврядування, юридичні особи, будучи організаторами обробки персональних даних, одночасно є користувачами одержуваного продукту в результаті обробки. Користувачами можуть бути і інші суб'єкти, правовий статус яких має значення.

Документи, що встановлюють застосування заходів відповідальності при зберіганні, обробці та наданні персональних даних, також слід готувати з урахуванням запропонованої категоризації.

Основною причиною правопорушень у цій сфері є неспроможне поширення персональних даних. У більшості випадків порушником є оператор персональних даних – державний орган, орган місцевого самоврядування, юридична або фізична особа, що організують і здійснюють обробку персональних даних, визначають цілі та зміст обробки персональних даних [9].

Наступною за поширеністю причиною є впровадження шкідливого програмного забезпечення. У цьому разі основним порушником є фізична особа. У частині справ про неспроможне використання персональних даних порушується ст. 188-39 «Порушення законодавства у сфері захисту персональних даних» КУпАП. Шкоду, заподіяну позивачам внаслідок дій правопорушників, можна оцінювати у різних масштабах: від порушення працездатності персонального комп'ютера до заподіяння шкоди безпеці життя. Взагалі, завдані збитки неможливо точно і повністю оцінити, оскільки одне лише правопорушення в сфері інформаційного права може тягти за собою незворотні наслідки. Залежно від сфери, в якій відбулося правопорушення, порушник несе адміністративну або кримінальну відповідальність.

Відшкодування шкоди обмежується лише відшкодуванням моральної шкоди за порушення законодавства про персональні дані або ж відшкодуванням працездатності персональних комп'ютерів або програмного забезпечення, які були навмисно пошкоджені. Актуальними залишаються питання, пов'язані з надмірністю оброблюваних персональних даних суб'єкта персональних даних відповідно до цілей обробки.

Проблема надмірності оброблюваних персональних даних стосовно мети обробки багатоаспектна, виражена у формі надання суб'єктом персональних даних на вимогу оператора додаткової інформації, зокрема спеціальних категорій персональних даних (інформація про судимість, національну приналежність), відомостей про близьких родичів при наданні певного виду послуг або під час прийняття на роботу. У процесі розгляду та вивчення інформаційних систем персональних даних необхідно акцентувати на захисті персональних даних в цих системах, оскільки в системах деяких організацій персональні дані досягають значних обсягів, що зумовлено особливістю побудови та функціонування органів виконавчої влади щодо організаційних зв'язків структурних одиниць системи [10, с. 26].

Вирішення проблеми захисту персональних даних криється у взаємодії операторів персональних даних, виробників програмного забезпечення і засобів захисту інформації, організацій, що спеціалізуються на захисті інформації, державних органів на всіх етапах життєвого циклу інформаційних систем. Особливістю правового режиму інформаційних систем персональних даних є характер, правова природа персональних даних, які можуть бути інформацією обмеженого доступу та загальнодоступною інформацією. Крім того, спеціальний набір організаційно-технічних засобів захисту є частиною правового режиму згаданих інформаційних систем.

На підставі аналізу діяльності головного регулятора в сфері захисту персональних даних можна стверджувати, що рівень грамотності населення у цій галузі зростає. Збільшення планових і позапланових перевірок Уповноваженого Верховної Ради України з прав людини, звернень громадян і юридичних осіб змушує операторів дотримуватися законодавства.

На основі підсумків діяльності Уповноваженого Верховної Ради України з прав людини можна зробити висновок, що основними порушеннями є: порушення вимог конфіденційності під час обробки персональних даних; неповідомлення громадянина про початок обробки його персональних даних [11, с. 68–71]. Ці порушення мають організаційний характер і можуть бути усунені силами оператора персональних даних. Організація захисту інформаційних систем персональних даних вимагає постійного аналізу для забезпечення виконання нових різноманітних вимог, що постійно виникають, до заходів, сервісів і засобів захисту інформації.

Особи, винні у порушенні вимог захисту персональних даних, несуть передбачену законодавством відповідальність.

Суб'єкти персональних даних мають право на відшкодування моральних збитків, завданих внаслідок порушення прав, правил обробки персональних даних, вимог до захисту, встановлених Законом України «Про захист персональних даних».

Відшкодування моральної шкоди здійснюється незалежно від відшкодування майнової шкоди та понесених суб'єктом персональних даних збитків. Ст. 188-39 КУпАП регламентує відповідальність спеціальних суб'єктів. Згідно з цією статтею порушення встановленого законом порядку збору, зберігання, використання або поширення інформації про персональні дані тягне за собою накладення адміністративного штрафу.

Висновки. Проведений аналіз свідчить, що відповідно до наведеної класифікації персональних даних необхідно диференціювати

заходи відповідальності залежно від ступеня завдання шкоди. Перспективи України у сфері створення правового захисту інформаційних систем персональних даних і, природно, самих персональних даних мають вагоме обґрунтування. Про це свідчать прийняті нормативні акти і, найважливіше, впровадження постанов і вказівок – ведення роботи та захисту персональних даних відповідно до законодавства в кожній організації оператора персональних даних. Специфіка правового режиму інформаційних систем персональних даних полягає в правовій природі персональних даних, які можуть бути інформацією обмеженого доступу та загальнодоступною інформацією.

Крім того, спеціальний набір правових і організаційно-технічних засобів захисту є невід'ємною частиною правового режиму інформаційних систем персональних даних. Правова природа персональних даних ускладнює можливість формування єдиної політики щодо правового регулювання інформаційних систем. Оскільки персональні дані є і інформацією обмеженого доступу, захист інформаційних систем персональних даних технічними засобами повинен відповідати вимогам центрального органу виконавчої влади у сфері спеціального зв'язку та захисту інформації України.

1. Бондаренко В. А. Окремі аспекти підвищення ефективності норм адміністративного права у період адаптації законодавства до вимог Європейського Союзу. *Науковий вісник Львівського державного ун-ту внутрішніх справ*. 2016. Вип. 3. С. 134–142.

2. Деякі питання практичного застосування Закону України «Про захист персональних даних»: Роз'яснення Міністерства юстиції України від 21.12.2011. URL: <http://zakon3.rada.gov.ua/laws/show/n0076323-11>

3. Удовенко Ж. В. Сутність інформації про особисте життя та її види кандидат. 2015. URL: <http://oaji.net/articles/2015/1739-1431336462.pdf>

4. Куценко Р. В. Поняття та склад персональних даних за трудовим законодавством України. *Наук. вісник публічного та приватного права*. 2017. Вип. 2. С. 78–82.

5. Новицький А., Дяковський О. Правове регулювання інформаційних баз даних, що містять персональні дані. *Підприємництво, господарство і право*. 2017. № 10. С. 177–181.

6. Гулак Г. М., Козачок В. А., Складанний П. М., Бондаренко М. О., Вовкотруб Б. В. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. *Сучасний захист інформації*. 2017. № 2 (30). С. 65–71.

7. Крикливенко Б. Лист Уповноваженого Верховної Ради України з прав людини від 03.03.2014 № 2/9-227067.14-1/НД-129 «Щодо захисту персональних даних». URL: <http://zakon5.rada.gov.ua/laws/show/v7067715-14>

8. Різак М. Практика країн Європейського Союзу та України у сфері судочинства щодо гарантування безпеки обігу та обробки персональних даних. *Підприємництво, господарство і право*. 2017. № 7. С. 68–72.

9. Мельник К. С. Обробка та захист персональних даних в процесі верифікації соціальних виплат громадян. *Інформація і право*. 2017. № 1 (20). С. 39–44.

10. Ковалів М. В., Стахура І. Б. Особливості адміністративно-правового статусу органів виконавчої влади. *Вісник Національного ун-ту «Львівська політехніка»*. Юридичні науки. 2014. № 807. С. 22–26.

11. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні / Секретаріат Уповноваженого Верховної Ради України з прав людини. К., 2017. 627 с. URL: file:///C:/Users/User/Downloads/Dopovid_2017.pdf

Yesimov S. S. Peculiarities of the legal regime of information systems for processing personal data

Information and communication technologies allow for the collection, processing, storage and distribution of large information content that has an important social value, and information relating to the category of personal data required for more effective functioning of various state institutions, development of social processes, implementation of the rights and freedoms of man and citizen. Applying information technology and having a specific set of personal data that is used by individuals to control their material and financial resources, you can get unlawful access and rights to possession of this resource. The development of information systems is aimed at protection of data leakage and prevention unauthorized access to information of a personal nature.

This increases the significance of various means of information protection by technical and legislative means. Prospects of Ukraine in the field of legal protection of information systems of personal data and the personal data have the relevant feasibility study. It is proved by adopted normative acts and implementation of the resolutions and instructions in real life – carrying out work and personal data protection according to the legislation in each organization.

The peculiarity of the legal regime of information systems of personal data consists in the legal nature of personal data, which may be information of limited access and public information. A special set of legal, organizational and technical means of protection is an integral part of the legal regime of personal data information systems. The legal nature of personal data complicates the possibility of forming a unified policy of the legal regulation of information systems. Since personal information is the information of restricted access, protection of information systems of personal data by technical means must meet the requirements of the central body of the Executive power in the field of special communication and information protection of Ukraine.

Key words: *personal data, information systems, processing of personal data, protection of personal data.*

Стаття надійшла 22 лютого 2018 р.