НЕГОДЧЕНКО В. О.,
кандидат юридичних наук, доцент,
доцент кафедри
кримінально-правових дисциплін
*(ВНПЗ «Дніпропетровський
гуманітарний університет»)*

УДК 342.951

МІСЦЕ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ УКРАЇНИ

Наукову статтю присвячено характеристиці правових норм, що визначають порядок використання персональних даних як ідентифікуючого засобу та інформації з обмеженим доступом, у системі інформаційного забезпечення діяльності органів внутрішніх справ.

Ключові слова: *конфіденційна інформація, таємна інформація, бази даних, органи внутрішніх справ, персональні дані, ідентифікація.*

Научная статья посвящена характеристике правовых норм, определяющих порядок использования персональных данных как идентифицирующего средства и информации с ограниченным доступом, в системе информационного обеспечения деятельности органов внутренних дел.

Ключевые слова: *конфиденциальная информация, секретная информация, базы данных, органы внутренних дел, персональные данные, идентификация.*

Research paper is devoted to the characterization of legal rules governing the use of personal data as a means of identifying and classified information, the information system of internal affairs.

Key words: *confidential information, secret information, databases, police, personal data identification.*

Вступ. Правоохоронні відносини потребують ідентифікації їх учасників, персоналізації як юридичної відповідальності, так і захисного впливу уповноважених державних органів. Єдиним видом інформації, що здійснює ідентифікацію суб'єкта, є персональні дані, значні масиви яких накопичуються органами внутрішніх справ України (ОВС). 1 січня 2011 р. набув чинності Закон України «Про захист персональних даних» № 2297 від 01.06.2010 р., який регулює відносини, пов'язані із захистом персональних даних під час їх обробки. 1 січня 2014 р. набули чинності зміни до законодавства про захист персональних даних відповідно до Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [20], відповідно до якого основні повноваження Держслужби України із захисту персональних даних були передані, включаючи проведення перевірок, Уповноваженому Верховної Ради України із прав людини, а також змінено сам механізм реєстрації баз персональних даних на повідомлення Уповноваженого із прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних [18]. Зазначене свідчить про нагальну потребу дослідження змін у системі інформаційного забезпечення діяльності ОВС та правил використання персональних даних.

Постановка завдання. Метою статті є з'ясування значення персональних даних як ідентифікуючого засобу в системі інформаційного забезпечення діяльності органів внутрішніх справ. Відповідно до поставленої мети завданнями дослідження є такі: визначення поняття інформаційного забезпечення ОВС та його основних елементів; з'ясування місць основної концентрації персональних даних у системі інформаційного забезпечення ОВС, видів персональних даних, що використовуються у правоохоронній діяльності, та основних правових засад їх використання; вивчення проблем забезпечення правового захисту персональних даних та шляхи їх вирішення.

Стан розроблення проблеми. Проблематиці інформаційного забезпечення діяльності державних органів у науці адміністративного права приділялася значна увага такими вченими, як Є.Ю. Бараш, В.С. Бондар, Є.Д. Бондаренко, В.М. Брижко, Н.С. Калашник, Р.А. Коваль [10], С.Ф. Константінов, М.В. Корнієнко, А.О. Пугач, Д.Г. Терьохін, О.Г. Фролова та інші. Водночас окремі дослідження правового регулювання використання персональних даних у системі інформаційного забезпечення діяльності органів внутрішніх справ як окремого напрямку управлінської діяльності, враховуючи специфіку статусу цих органів, комплексно не проводились. У цьому контексті Н.С. Калашник вказує, що незважаючи на те, що процес тотальної інформатизації українського суспільства триває більше десяти років, науковцями недостатньо приділялося уваги питанням застосування інформаційних технологій у здійсненні правоохоронної діяльності [9].

Результати дослідження. Інформаційне забезпечення кожної державної служби є важливим елементом її функціонування. Особливої важливості набуває інформаційне забезпечення державних служб, діяльність яких пов'язана із застосуванням державного примусу. Наявність примусового елементу під час виконання ОВС покладених на них обов'язків створює ускладнення у процесі отримання й використання персональних даних. Відповідно до ст. 11 Закону України «Про міліцію» міліція має право здійснювати обробку персональних даних в обсязі, структурі та порядку, що постають із завдань і функцій, покладених на міліцію цим та іншими законами, а також забезпечувати режим доступу до інформації [23]. Зазначене створює необхідність приділення окремої уваги правовому регулюванню використання персональних даних у процесі інформаційного забезпечення діяльності ОВС та конкретизації режиму персональних даних як виду інформації з обмеженим доступом.

Здійснення управління та управлінської діяльності в сучасних умовах, як зазначає Є.Ю. Бараш, можливе лише за умови належного інформаційного забезпечення, яке опосередковує й упорядковує відповідні управлінські зв'язки, що виникають між суб'єктом та об'єктом управління [1, с. 34]. Саме тому можна стверджувати, що від рівня якості розробки питання інформаційного забезпечення ОВС залежить і рівень захисту персональних даних, що нею використовуються, й ефективність захисту прав і свобод громадян України.

Як зауважує О.Г. Фролова, практика боротьби зі злочинністю переконливо свідчить не лише про суттєву, а в багатьох випадках – пріоритетну роль системи інформаційного забезпечення ОВС як ланки, що значною мірою зумовлює ефективність управління в ОВС та ефективність роботи вказаної системи в цілому. Пріоритетність системи інформаційного забезпечення управління в ОВС підкріплюють, підтверджують відповідні нормативно-правові акти, зокрема накази й розпорядження МВС України [29, с. 55]. М.В. Корнієнко вказує на необхідність надання особливої уваги під час проведення командно-штабних і тактико-спеціальних навчань питанням інформаційного забезпечення оперативного штабу в умовах постійної зміни оперативної обстановки [13, с. 13]. Він зазначає, що аналіз результатів практичної діяльності підрозділів органів внутрішніх справ щодо припинення групових порушень громадського порядку засвідчує, що на сьогодні досить проблемними залишаються питання обміну інформацією із взаємодіючими органами під час проведення зазначених дій [13, с. 16].

В.П. Пєтков вказує на пріоритетність надання уваги інформаційному забезпеченню правоохоронної діяльності в пенітенціарній системі [17, с. 4]. Аналогічної позиції дотримується й С.Ф. Константінов, проте вже у сфері запобігання і припинення правопорушень неповнолітніх [12, с. 254]. Поінформованість суб'єктів важлива також в адміністративному процесі [28].

Існують різні наукові підходи щодо визначення інформаційного забезпечення. Так, Є.Д. Бондаренко під інформаційним забезпеченням розуміє процес задоволення потреб в інформації, заснованої на застосуванні спеціальних засобів і методів її одержання, опрацювання, накопичення й видачі у зручному для використання вигляді, а структура цього забезпечення включає інформаційний фонд та спеціальні прийоми й методи інформаційного забезпечення, тобто це явище одночасно являє собою, по-перше, певну організаційну діяльність одержання, опрацювання, накопичення й видачі інформації, по-друге, прийоми та методи її здійснення, по-третє, певні матеріальні об'єкти – інформаційні фонди [3].

Досліджуючи інформаційне забезпечення ОВС, наведемо думку Є.Ю. Бараша, який визначає основні ознаки інформаційного забезпечення управління Державною кримінальною-виконавчою службою, а саме: за своєю сутністю воно виступає як процес обробки, одержання, опрацювання, накопичення й використання управлінської інформації про різні аспекти функціонування служби; за періодичністю воно являє собою неперервний процес обробки й використання інформації; за характером існування становить частину управлінської діяльності служби; за формою реалізації здійснюється за допомогою притаманних цьому виду засобів і методів; за наслідками здійснення інформаційного забезпечення пов'язане із формуванням певних інформаційних фондів, документів, нормативної бази; за метою функціонування спрямоване на забезпечення належного функціонування системи, наприклад, автоматизованої системи управління; за основним призначенням як інструмент ефективного управління знаходить свою реалізацію під час аналізу, планування й підготовки ефективних управлінських рішень [1, с. 35-36]. Безпосередньо приклад визначення інформаційного забезпечення такого правоохоронного органу як державна виконавча служба було надано П.В. Макушевим, який запропонував під інформаційним забезпеченням діяльності державної виконавчої служби розуміти частину управлінської діяльності з аналізу, планування й підготовки управлінських рішень, яка представляє собою неперервний процес обробки та використання інформації про стан функціонування системи державної виконавчої служби, яка здійснюється за допомогою інформаційних засобів і методів, призводить до формування інформаційних фондів та спрямована на забезпечення належного функціонування системи державної виконавчої служби України [14, с. 73]. На наш погляд, аналогічне визначення може бути застосоване й до поняття «інформаційне забезпечення діяльності ОВС».

Елементами інформаційно-аналітичної системи органів державної влади, як зазначає А.О. Пугач, повинні бути бази даних необхідної інформації, системи зв'язку та передачі даних, системи обробки даних, автоматизовані робочі місця державних службовців. Первинними елементами інформаційно-аналітичної системи є периферійні об'єктно-спеціалізовані автоматизовані інформаційні підсистеми, елементами кожної з яких є комплекси технічних засобів, до яких входить обчислювальна техніка, системне і спеціальне програмне забезпечення, колективи відповідних спеціалістів [25]. Таким чином, важливим елементом системи інформаційного забезпечення ОВС є бази даних (БД).

Відповідно до Інструкції з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України [7] до системи інформаційного забезпечення ОВС входять такі бази даних, що містять у тому числі персоналізовану інформацію, тобто персональні дані: БД «Факт», в якій містяться відомості щодо злочинів (правопорушень), подій, які загрожують особистій чи громадській безпеці, надзвичайних подій, викладених у заявах (повідомленнях, рапортах) та зареєстрованих у черговій

частині ОВС; БД «Злочин» – відомості щодо зареєстрованих злочинів (особливо тяжкі, тяжкі, середньої тяжкості), вчинених на території обслуговування ОВС, у тому числі за матеріалами яких заведено ОРС категорії «Злочин»; БД «Доставлені» – доставлені до ОВС особи; БД «Контур» – електронні фотографії, опис зовнішності та особливих прикмет; БД «Особа» – відомості щодо осіб, які вчинили правопорушення та щодо яких здійснюється профілактична робота працівниками ОВС; БД «Розшук» – відомості щодо оголошених у державний, міждержавний, міжнародний розшук; БД «Адміністративне правопорушення» – відомості щодо зареєстрованих в ОВС адміністративних правопорушень; БД «Корупційне правопорушення» – відомості щодо зареєстрованих корупційних правопорушень; БД «Мігрант» – відомості щодо осіб, які порушили законодавство України про правовий статус іноземців та осіб без громадянства, виявлених працівниками ОВС; БД «Угон» – відомості щодо транспортних засобів (автомобілів, мотоциклів та мопедів), які розшукуються, а також виявлених безгосподарних, у тому числі викрадених і втрачених державних номерних знаків ТЗ; БД «Річ» – відомості щодо речей, викрадених, вилучених з ознаками підробки, заборонених або обмежених в обороті у громадян і службових осіб, безгосподарних, що знайдені або вилучені із камер схову вокзалів, портів, аеропортів, та зданих до ОВС; АРМ «Антикваріат» – культурні цінності – об'єкти матеріальної і духовної культури, що мають художнє, історичне, етнографічне та наукове значення, в тому числі їх електронні аналоги; БД «Втрачені документи» – відомості щодо документів (бланків документів), викрадених, утрачених, вилучених (з ознаками підробки) у громадян і службових осіб, паспортів померлих громадян України, не зданих до ОВС, паспортів осіб, які знаходяться в розшуку, та які мають індивідуальні заводські (фабричні) номери і знаходяться в державному обігу; БД «Кримінальна зброя» – відомості щодо зброї викраденої, утраченої, знайденої, зданої до ОВС, вилученої працівниками ОВС із числа тієї, що незаконно зберігалася, незалежно від її технічного стану, що має індивідуальні заводські (фабричні) номери або номери деталей; БД «Зареєстрована зброя» – відомості щодо зброї, що має індивідуальні заводські (фабричні) номери, перебуває в користуванні громадян, підприємств, установ, організацій, господарських об'єднань, яким надано відповідно до законодавства дозвіл на її придбання, зберігання, носіння, перевезення, та яка обліковується підрозділами дозвільної системи ОВС; БД «Електронний рапорт» – відомості, які було отримано/виявлено працівниками ОВС у процесі виконання ними своїх службових обов'язків або під час проведення гласних оперативно-розшукових заходів від громадян і посадових осіб (без розкриття джерела інформації) і лише відкритого характеру. Це лише невелика частина баз даних, що містять персональні дані та використовуються правоохоронними органами.

В.С. Бондар, Д.Г. Терьохін зазначають, що сучасний потенціал високих технологій містить потужні можливості проведення моніторингу нерозкритих злочинів шляхом утворення єдиних інтегрованих інформаційних систем. Функціональна класифікація, що найбільш точно відображає існуючу структуру інформаційних підсистем ГУ МВС в областях, на їх думку, складається з наступного: а) автоматизованої інформаційно-пошукової системи «Армор», яка виконує пошукові, облікові, довідкові, прогнозуючі функції; б) інформаційно-аналітичної системи «Сова», яка виконує аналітичні, плануючі, діагностичні функції; в) інтегрованої біометричної системи «Аргус», окрім функцій цих систем, тут реалізовано можливості біометричної ідентифікації людини за обличчям. АІПС «Армор», зокрема, об'єднує 19 комп'ютерних інформаційних підсистем: АІС «Особа», АІС «Дактилоскопічні обліки», АІС «Оріон», АІС «Нерозкриті злочини» з відомостями про нерозкриті злочини, вчинені на території області (розбої, скоєні із застосуванням вогнепальної зброї, викрадення цінностей із металевих сховищ, викрадення антикваріату, культурних та історичних цінностей тощо) [2].

Науковці виділяють різні аспекти функціонування інформаційної системи державних органів, у тому числі правоохоронної діяльності працівників ОВС: 1) доступ-

ність (можливість за обмежений час отримати інформацію); 2) цілісність (актуальність і несуперечливість інформації, її захищеність від знищення та несанкціонованої зміни); 3) конфіденційність (захист від несанкціонованого ознайомлення) [4, с. 68]. Водночас система інформаційного забезпечення ОВС України розроблена ще не повністю, особливо великі прогалини існують у сфері організаційно-правового забезпечення безпеки використання конфіденційних відомостей, отриманих у процесі службової діяльності працівників міліції, особливо персональних даних.

Особливості використання персональних даних визначені Законом України «Про захист персональних даних» [21]. Аналізуючи перелік відомостей, що складають персональні дані, нами з'ясовано, що в Законі України «Про захист персональних даних» чітко не вказано зміст відомостей, що складають персональні дані, проте Законом України «Про інформацію» до конфіденційної інформації про фізичну особу віднесено дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата й місце народження [22]. Конституційний Суд України Рішенням від 30 жовтня 1997 р. № 5-зп відніс до конфіденційної інформації про фізичну особу, ще й відомості про її майновий стан та інші персональні дані [27], а рішенням від 20 січня 2012 р. № 2-рп/2012, даючи офіційне тлумачення ч. 1, 2 ст. 32 Конституції України, пояснив, що до інформації про особисте та сімейне життя особи (персональні дані про неї) входять відомості про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я тощо [26]. Проте законодавством України не встановлено й не може бути встановлено, як роз'яснює Міністерство юстиції України, чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону «Про захист персональних даних» до різноманітних ситуацій, у тому числі під час обробки персональних даних в інформаційних (автоматизованих) базах і картотеках персональних даних, що можуть виникнути в майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя [5].

Конституційний Суд України також вважає, що перелік даних про особу не є вичерпним, більша їх частина визнається конфіденційною інформацією. Основними правилами використання такої інформації є недопущення збирання, зберігання, використання й поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата й місце народження [22]. В абз. 2 ст. 11 Закону України «Про інформацію» зазначено: «Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди». Це означає, що є частина персональних даних, які носять відкритий характер, тобто не є інформацією з обмеженим доступом. Це питання вирішує ст. 5 Закону України «Про захист персональних даних», у ч. 2 якої зазначено, що персональні дані, крім знеособлених персональних даних, за режимом доступу є інформацією з обмеженим доступом. Наведене свідчить про сприйняття законодавцем конфіденційного характеру персональних даних. Віднесення персональних даних до відкритої інформації або до інформації з обмеженим доступом здійснюється за ключовою ознакою – можливістю ідентифікувати особу – суб'єкта персональних даних. Як правило, в системі інформаційного забезпечення ОВС використовуються конфіденційні персональні дані, хоча під час віднесення їх до державної таємниці їх режим використання може бути, як у таємної інформації.

Обов'язки осіб, уповноважених на виконання функцій держави не розголошувати й не використовувати в інший спосіб конфіденційну інформацію, що стала їм відома у зв'язку з виконанням своїх службових повноважень, крім випадків, встановлених законом, визначаються також Законом України «Про правила етичної поведінки» [24], загальними правилами поведінки державного службовця [6] та етичними кодексами

окремих відомств. Проте у Правилах поведінки та професійної етики осіб рядового та начальницького складу органів внутрішніх справ України [19] відсутні положення, що зобов'язують зберігати конфіденційність інформації, у тому числі персональних даних саме працівників органів внутрішніх справ. Позитивним прикладом врегулювання такого питання у правоохоронних органах є Кодекс професійної етики та поведінки працівників прокуратури, ст. 11 якого зобов'язує працівників прокуратури забезпечувати конфіденційність інформації, яка стала їм відома у зв'язку з виконанням своїх службових повноважень, та особливу увагу приділяти питанням обмеження доступу до персональних даних громадян [11]. На наш погляд, необхідно аналогічні положення закріпити й у Правилах поведінки та професійної етики осіб рядового та начальницького складу ОВС України. Ці положення набувають особливої актуальності з огляду на те, що законодавством передбачено проведення службового розслідування уповноваженим на те начальником ОВС щодо працівника ОВС у разі розголошення ним конфіденційної, таємної, службової або іншої інформації, яка містить таємницю, що охороняється законом [8]. Пам'ятаючи про режим персональних даних як конфіденційної інформації, вважаємо, що норми Інструкції про порядок проведення службових розслідувань в органах внутрішніх справ України можуть бути застосовані й під час порушення норм законодавства про захист персональних даних.

З'ясовуючи види персональних даних, що використовують ОВС у своїй діяльності, зазначимо, що законодавством передбачено персональні дані загального характеру, формування баз даних яких не потребує державного контролю, та персональні дані вразливого характеру. Забезпеченню конфіденційності останніх присвячений Порядок повідомлення Уповноваженого Верховної Ради України із 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[18], прийнятий 08.01.2014 р. на виконання Закону України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [20].

Цей закон набув чинності 1 січня 2014 р. Відповідно до нього основні повноваження Держслужби України із захисту персональних даних були передані, включаючи проведення перевірок, Уповноваженому Верховної Ради України із прав людини, а також змінено сам механізм реєстрації баз персональних даних на повідомлення Уповноваженого із прав людини щодо обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних [18]. Цей закон призвів до змін у правовому режимі персональних даних, виокремивши групу персональних даних, обробка яких становить особливий ризик для прав і свобод суб'єктів, а саме: 1) расове, етнічне та національне походження; 2) політичні, релігійні або світоглядні переконання; 3) членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи у громадських організаціях світоглядної спрямованості; 4) стан здоров'я; 5) статеве життя; 6) біометричні дані; 7) генетичні дані; 8) притягнення до адміністративної чи кримінальної відповідальності; 9) застосування щодо особи заходів у межах досудового розслідування; 10) вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»; 11) вчинення щодо особи тих чи інших видів насильства; 12) місцеперебування та/або шляхи пересування особи [18]. Таким чином, у системі інформаційного забезпечення ОВС використовуються як звичайні персональні дані, так і персональні дані, обробка яких становить особливий ризик для прав і свобод суб'єктів.

Конституційний Суд України дійшов висновку, що збирання, зберігання, використання й поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках

і лише в інтересах національної безпеки, економічного добробуту та прав людини. Ч. 2 ст. 14 Закону України «Про захист персональних даних» вносить уточнення щодо поширення персональних даних без згоди суб'єкта персональних даних: поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини. Відповідно до ст. 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією й законами України [15]. Чинного нормативно-правового відомчого акта, який визначав би порядок використання персональних даних у системі інформаційного забезпечення діяльності ОВС, не прийнято, що, на наш погляд, є недоліком, оскільки ОВС під час використання персональних даних є їх держателями або володільцями.

У вітчизняному законі «Про захист персональних даних» окремо не об'єднані в одну норму права й обов'язки володільця (держателя персональних даних). Проте вони є подібними до тих, що визначає ст. 13 «Права та обов'язки держателя персональних даних» Модельного кодексу «Про персональні дані». Юридичні та фізичні особи отримують право на дії з персональними даними на підставі дозволу суб'єкта персональних даних, передбаченого національним законодавством. Держатель персональних даних зобов'язаний здійснювати наступне: 1) отримувати персональні дані безпосередньо від суб'єкта або з інших джерел за його згодою, за винятком випадків, передбачених чинним законодавством; 2) забезпечувати режим конфіденційності під час використання персональних даних у передбачених законодавством випадках; 3) документально визначати порядок роботи з персональними даними службовців, а також осіб, які несуть юридичну відповідальність за дотримання режиму конфіденційності і збереження персональних даних; 4) забезпечувати збереження персональних даних, їх уточнення, а також встановлений у нормативному порядку режим доступу до них; 5) повідомляти суб'єкту на його вимогу інформацію про наявність персональних даних про нього, а також самі персональні дані, за винятком випадків, передбачених законом. Також відповідно до міжнародного й вітчизняного законодавства працівники ОВС, яким персональні дані стають відомими завдяки їх посадовим обов'язкам, беруть на себе зобов'язання й несуть відповідальність за забезпечення конфіденційності дій із цими персональними даними. Зобов'язання залишаються чинними й після закінчення роботи з персональними даними протягом терміну збереження режиму конфіденційності. Передача персональних даних ОВС іншому правоохоронному органу можлива лише в тому випадку, якщо цілі використання персональних даних новим власником відповідають цілям їх отримання. Передача персональних даних у цілях, не відповідних до цілей їх отримання, здійснюється або за згодою суб'єкта, або на підставі закону. Під час передачі персональних даних іншому держателю на нього покладається обов'язок дотримуватися режиму конфіденційності [16]. Усі зазначені положення повинні бути акумульовані в єдиному підзаконному нормативно-правовому акті, який визначав би порядок використання й захисту персональних даних ОВС.

Висновки. Інформаційне забезпечення діяльності ОВС можна визначити як частину управлінської діяльності з аналізу, планування й підготовки управлінських рішень, яка представляє собою неперервний процес обробки й використання інформації про стан функціонування системи ОВС, яка здійснюється за допомогою інформаційних засобів і методів, призводить до формування інформаційних фондів та спрямована на забезпечення належного функціонування системи державної виконавчої служби України. Забезпечення інформаційних потреб ОВС вимагає збору, накопичення, обробки, систематизації, зберігання, використання й обміну значними обсягами персональних даних, що локалізуються та концентруються в інформаційних базах ОВС. Переважна біль-

шість персональних даних, що використовуються ОВС, є конфіденційною інформацією, оскільки слугує ідентифікуючим засобом учасників правоохоронних і правозахисних відносин. Водночас чинне законодавство не містить єдиного відомчого нормативно-правового акта, який деталізував би положення Закону України «Про захист персональних даних» з урахуванням особливостей діяльності ОВС. Вважаємо за потрібне розробити внутрішньовідомчий документ, що визначив би відділи й посади працівників, відповідальних за забезпечення захисту персональних даних, комплекс організаційних і технічних заходів, права й обов'язки всіх працівників ОВС щодо захисту персональних даних у процесі реалізації покладених на них правоохоронних і правозахисних функцій. Предметом подальших наукових пошуків у цій сфері стане визначення особливостей використання та забезпечення захисту персональних даних окремими підрозділами ОВС.

Список використаних джерел:

1. Бараш Є.Ю. Інформаційне забезпечення управління Державною кримінальною-виконавчою службою / Є.Ю. Бараш // Форум Права. – 2011. – № 3. – С. 34–40. – [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/e-journals/FP/2011-3/11beikvc.pdf.

2. Бондар В.С., Терьохін Д.Г. Шляхи оптимізації облікової діяльності при розслідуванні злочинів (за матеріалами кримінальних справ про шахрайство, вчинені шляхом незаконного отримання споживчого кредиту) // Український юридичний портал «Радник». – [Електронний ресурс]. – Режим доступу : http://radnuk.info/statti/556-protses/15076-2011-01-21-05-35-38.html.

3. Бондаренко Є.Д. Особливості інформаційного забезпечення торгівельного підприємства / Є.Д. Бондаренко // Актуальні проблеми сучасної науки : п'ята всеукр. наук.-практ. інтеренет-конференція // [Електронний ресурс]. – Режим доступу : http://intkonf.org/bondarenko-ed-osoblivosti-informatsionogo-zabezpechennya-torgovelnogo-pidpriemstva.

4. Брыжко В.М., Цимбалюк В.С., Орехов А.А. Е-будущее и информационное право / под ред. докт. юрид. наук, проф. Р.А. Калюжного, докт. экон. наук, проф. М.Я. Швеца. – К. : Интеграл, 2002. – 264 с.

5. Деякі питання практичного застосування Закону України «Про захист персональних даних» : Роз'яснення Міністерства юстиції України від 21.12.2011 р. // [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/n0076323-11/print1329875570254855.

6. Загальні правила поведінки державного службовця : Наказ Головного управління державної служби України від 04.08.2010 р. № 214 // Офіційний вісник України. – 2010. – № 90. – С. 211. – Ст. 3208. – Код акта 53581/2010.

7. Інструкція з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : Наказ Міністерства внутрішніх справ України від 10.03.2010 р. № 75.

8. Інструкція про порядок проведення службових розслідувань в органах внутрішніх справ України : Наказ МВС України від 12.03.2013 р. № 230.

9. Калашник Н.С. Проблеми впровадження та використання інформаційно-комунікаційних технологій в управлінні діяльністю органу виконавчої влади / Н.С. Калашник // [Електронний ресурс]. – Режим доступу : http://www.kvs.zp.ua/index.php&option=com_content&task=view&id=177&itemid=192.

10. Коваль Р.А. Інформаційно-аналітичне забезпечення діяльності органів державної влади / Р.А. Коваль // Теорія та практика державного управління : зб. наук. праць. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2006. – № 1 (113).

11. Кодекс професійної етики та поведінки працівників прокуратури : схвалено Всеукраїнською конференцією працівників прокуратури 28 листопада 2012 року ; затверджено Наказом Генерального прокурора України від 28 листопада 2012 року № 123 //

[Електронний ресурс]. – Режим доступу : http://gp.gov.ua.ua/file_downloader.html.

12. Константінов С.Ф. Інформаційне забезпечення ОВС – один з пріоритетних напрямів роботи міліції щодо запобігання та припинення правопорушень неповнолітніх // Науковий вісник Київського національного університету внутрішніх справ. – 2006. – № 1. – С. 254–257.

13. Корнієнко М.В. Управління силами і засобами органів внутрішніх справ при ускладненні оперативної обстановки в сфері охорони громадського порядку : автореф. дис. ... канд. юрид. наук : 12.00.07 / М.В. Корнієнко ; Нац. юрид. акад. України ім. Ярослава Мудрого. – Х., 2000. – 22 с.

14. Макушев П.В. Персональні дані як елемент системи інформаційного забезпечення державної виконавчої служби України // Право і суспільство. – 2013. – № 4. – С. 70–76.

15. Методичні рекомендації щодо надання персональних даних на запити правоохоронних органів // Одеська обласна державна адміністрація Управління взаємодії з правоохоронними органами, оборонної роботи, запобігання та виявлення корупції обласної державної адміністрації (відділ з питань запобігання та виявлення корупції) : веб-сайт. – Одеса, 2013. – [Електронний ресурс]. – Режим доступу : http://uvpo.odessa.gov.ua/files/uvpo_portal/metodichn_rekomendac_wodo_nadannya_personal_nih_danih_na_zapiti_pravoohoronnih_organ_v.pdf.

16. Модельный закон «О персональных данных» : опубликован 16 октября 1999 года ; принят на 14 пленарном заседании Межпарламентской ассамблеи государств-участников СНГ (постановление № 14-19 от 16 октября 1999 года).

17. Пєтков В.П. Управління виховно-виправним процесом : автореф. дис. ... докт. юрид. наук : 12.00.07 / В.П. Пєтков ; Ун-т внутр. справ. – Х., 1998. – 40 с.

18. 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 // [Електронний ресурс]. – Режим доступу : http://www.ombudsman.gov.ua/index.php?option=com_content&view=article&id=3413:2014-01-10-09-58-05&catid=202:2011-11-25-14-59-08&Itemid=202. – Дата звернення: 10 січня 2014 р.

19. Правила поведінки та професійної етики осіб рядового та начальницького складу органів внутрішніх справ України : Наказ МВС України від 22.02.2012 р. № 155 // Офіційний вісник України. – 2012. – № 36. – С. 342. – Ст. 1357. – Код акта 61517/2012.

20. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України від 3 липня 2013 року № 383-VII // Урядовий кур'єр. – 2013. – 31 липня. – № 136.

21. Про захист персональних даних : Закон України від 13 січня 2011 року № 2939-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

22. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

23. Про міліцію : Закон України від 20 грудня 1990 року № 565-XII // Голос України. – 1991. – 4 січня.

24. Про правила етичної поведінки : Закон України від 17 травня 2012 року № 4722-VI // Голос України. – 2012. – 12 червня. – № 106.

25. Пугач А.О. Сутність процесу інформаційно-аналітичного забезпечення органів державної виконавчої влади в Україні // Електронне наукове фахове видання «Державне управління: удосконалення та розвиток». – [Електронний ресурс]. – Режим доступу : http://www.dy.nayka.com.ua/?op=1&z=165.

26. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) від 30 жовтня 1997 року № 5-зп : справа

№ 18/203-97 // [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/v005p710-97.

27. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин 1, 2 статті 32, частин 2, 3 статті 34 Конституції України № 1-9/2012 від 20 січня 2012 року № 2-рп/2012 // [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/go/v002p710-12.

28. Тищенко М.М. Адміністративно-процесуальний статус громадянина України: проблеми теорії та шляхи вдосконалення законодавчого регулювання : автореф. дис. ... докт. юрид. наук : 12.00.07 / М.М. Тищенко ; Нац. юрид. акад. України ім. Ярослава Мудрого. – Х., 1999. – 32 с.

29. Фролова О.Г. Проблеми правового регулювання інформаційно-методичного управління в ОВС // Проблеми правознавства та правоохоронної діяльності. – 2002. – № 1. – С. 53−62.

ПОТІП М. М.,
кандидат юридичних наук,
викладач кафедри
цивільно-правових дисциплін
(Дніпропетровський гуманітарний університет)

КОРНІЄНКО М. В.,
доктор юридичних наук, професор,
професор кафедри
загально-правових дисциплін
(Дніпропетровський гуманітарний університет)

УДК 34.07

АДМІНІСТРАТИВНО-ПРАВОВИЙ РЕЖИМ РОЗМЕЖУВАННЯ КОМПЕТЕНЦІЇ ОРГАНІВ ДЕРЖАВНОЇ ВИКОНАВЧОЇ ВЛАДИ ТА МІСЦЕВОГО САМОВРЯДУВАННЯ

Розглянуто поняття адміністративно-правового режиму розмежування компетенції органів державної виконавчої влади та місцевого самоврядування, його предмет, засоби й методи.

Ключові слова: *правовий режим, компетенція, виконавча влада, місцеве самоврядування.*

Рассмотрено понятие административно-правового режима разграничения компетенции органов государственной исполнительной власти и местного самоуправления, его предмет, средства и методы.

Ключевые слова: *правовой режим, компетенция, исполнительная власть, местное самоуправление.*

The concept of administrative and legal regime of distribution of powers of state executive bodies and local authorities, of his subject, means and methods.

Key words: *legal mode, competence, executive power, local government.*