

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

ADMINISTRATIVE REMEDIES FOR PERSONAL DATA PROTECTION

Самойленко Ю.С., аспірант кафедри адміністративного права,
процесу та адміністративної діяльності

Дніпропетровський державний університет внутрішніх справ

У статті визначено систему адміністративно-правових засобів забезпечення захисту персональних даних, здійснено аналіз нормативно-правових актів, наукової думки щодо поняття та видів адміністративно-правових засобів забезпечення захисту персональних даних, їх систематизації та визначено ефективні шляхи їх реалізації.

З'ясовано, що під адміністративно-правовими засобами забезпечення захисту персональних даних слід розуміти систему заходів попередження (превентивних заходів), припинення порушень, що посягають на право володіння та розпорядження персональними даними, та застосування заходів адміністративної відповідальності органами публічної влади, які відповідно до законодавства мають забезпечувати їх захист.

Визначено процесуальні особливості порядку застосування заходів адміністративної відповідальності за правопорушення щодо захисту персональних даних. Так, відповідно до ст. 255 правом складення протоколу про адміністративні правопорушення за ст. 188-39 КУпАП, а також оформлення матеріалів справи мають уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини або представники Уповноваженого Верховної Ради України з прав людини. Відповідно до ст. 221 КУпАП таку категорію справ розглядає суд. Відповідно до ст. 276 КУпАП ці злочини розглядаються за місцем їх вчинення, а згідно зі ст. 277 КУпАП вони розглядаються у п'ятнадцятиденний строк з дня одержання органом (посадовою особою), правомочним розглядати справу, протоколу про адміністративне правопорушення та інших матеріалів справи. Запропоновано удосконалити окремі положення законодавства стосовно притягнення особи до адміністративної відповідальності за порушення законодавства щодо захисту персональних даних. Зокрема, пропонується конкретизувати, що місцем розгляду справи є юридична адреса володільця персональних даних, а також продовжити строки притягнення до відповідальності та накладення стягнення за порушення законодавства про захист персональних даних до одного року.

Ключові слова: персональні дані, захист персональних даних, об'єкт, суб'єкт захисту, адміністративно-правові засоби забезпечення захисту персональних даних.

The article defines the system of administrative and legal means of ensuring the protection of personal data, analyzes the normative legal acts, scientific opinion on the concept and types of administrative and legal means of ensuring the protection of personal data, their systematization and defines an effective way of their implementation.

It has been found out that administrative and legal means of ensuring the protection of personal data should be understood as a system of preventive measures (preventive measures), termination of violations affecting the right to possess and dispose of personal data, and the application of measures of administrative responsibility by public authorities, which according to the legislation have to protect them.

The procedural peculiarities of the procedure for the application of measures of administrative liability for offenses concerning the protection of personal data are determined. Thus, according to Art. 255 the right to draw up a protocol on these administrative offenses, namely under Art. 188-39 of the Code of Administrative Offenses and registration of case files are authorized by the persons of the Secretariat of the Ombudsman of Ukraine or by representatives of the Ombudsman of Ukraine; in accordance with Art. 221 of the Administrative Code, such a category of cases is considered by the court, and in accordance with Art. 276 of the Code of Administrative Offenses – are considered at the place of their commission and according to Art. 277 of the Code of Administrative Offenses within fifteen days from the date of receipt by the body (official) competent to consider the case, the protocol on administrative offense and other case files. It is proposed to improve certain provisions of the law regarding the holding of a person to administrative responsibility for violation of the legislation on protection of personal data, namely: to specify that the place of consideration of the case is the legal address of the holder of the personal data; to extend the term of prosecution and imposition of penalties for violation of the legislation on protection of personal data up to one year; etc.

Key words: personal data, protection of personal data, object, subject of protection, administrative and legal means for ensuring protection of personal data.

Актуальність статті. Вільний широкий доступ до інформації та можливість продукувати нову інформацію сприяють створенню можливостей та розвитку особистості, але стрімкий розвиток інформаційно-комунікаційних технологій потребує розроблення та впровадження адекватних захисних механізмів, спроможних реально захистити персональні права та свободи власників особистих даних. Попри значну увагу з боку суспільства та держави до питання захищеності персональних даних від втручання та потенційного оприлюднення сторонніми особами, в сучасних умовах воно й досі залишається відкритим. Виникає необхідність вироблення відповідної державної політики у сфері обігу та обробки персональних даних, щоб контролювати та раціонально використовувати потужності інформаційно-телекомунікаційних технологій збору, обігу та обробки будь-якої інформації, зокрема й персонального характеру. Зазначена політика має базуватись на глибокому і всебічному теоретичному осмисленні правового, зокрема й адміністративно-правового забезпечення відносин обігу та обробки персональних даних, сутності та механізму публічного управління у зазначеній сфері. Система права запропонувала та продовжує продукувати різноманітні правові механізми

захисту персональних даних, серед яких вагоме місце відведене адміністративно-правовим засобам захисту персональних даних, започаткування дослідження яких пропонується здійснити в межах даної наукової статті.

Проблема дослідження правових засобів захисту персональних даних не є новою для правової науки. Так, останнім часом особливий інтерес до висвітлення даної проблеми проявляли М.В. Бем, І.М. Городинський, Г. Саттон, О.М. Родіоненко, О.Г. Рогова, С.С. Єсімов, В.О. Волосецький, В.М. Брижко, К.С. Мельник, Т. Обуховська, О. Мервінський, М. Кравчук, Ж.В. Удовенко, В.В. Оніщенко та інші вчені. Сутність персональних даних і окремі аспекти їх адміністративно-правового захисту досліджували такі вчені: Р.В. Ігонін, Р.А. Калюжний, А.В. Кучеренко, С.Й. Литвин, А.В. Пазюк, В.П. Радкевич, К.М. Рудой, В.О. Серьогін, І.М. Солілко, В.І. Теремецький, А.М. Чвалюк, О.О. Шарібурина, М.Я. Швець та інші вітчизняні й зарубіжні науковці. Серед сучасних наукових праць, присвячених проблемам адміністративно-правового регулювання обігу, обробки та захисту персональних даних, слід виділити роботи В.М. Брижко «Організаційно-правові питання захисту персональних даних» (2004 р.) [1], А.М. Чернобай «Правові засоби захисту

персональних даних працівника» (2006 р.) [2], М.В. Різак «Правове регулювання відносин обігу персональних даних» (2012 р.) [3], А.В. Тунік «Правові основи захисту персональних даних» (2012 р.) [4], Д.В. Цвірюк «Адміністративно-правовий захист персональних даних в Україні» (2014 р.) [5]. Однак, попри значну увагу науковців, системне дослідження адміністративно-правових засобів захисту персональних даних на монографічному рівні або в межах наукової статті не здійснювалось, що зумовлює доцільність проведення такого дослідження. Актуальність даного дослідження викликана необхідністю вироблення раціональної та ефективної системи адміністративно-правових заходів захисту персональних даних.

Отже, *метою* дослідження в межах наукової статті є визначення системи адміністративно-правових засобів забезпечення захисту персональних даних, *завданням* дослідження на виконання його мети є аналіз нормативно-правових актів, наукової думки щодо поняття та видів адміністративно-правових засобів забезпечення захисту персональних даних, їх систематизації та визначення ефективних шляхів їх реалізації.

Виклад основного змісту. Слід спочатку зауважити, що законодавче визначення адміністративно-правових, як і інших правових засобів захисту персональних даних, відсутнє. Так, Закон України «Про захист персональних даних» [6] визначає тільки у ст. 5 об'єкти такого захисту як персональні дані, обходячи стороною суб'єктів їх захисту, а також частково у ст. 24 визначає структурно-організаційну форму забезпечення захисту персональних даних, вказуючи, що «в органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці» [6], не вказуючи при цьому засоби та способи захисту персональних даних та не зазначаючи конкретні процедурні форми такого захисту. Отже, ми не будемо першими авторами, які вказують на недосконалість цього закону, а в результаті дослідження запропонуємо власні науково обгрунтовані пропозиції щодо насичення його нормами, які визначають конкретні форми захисту персональних даних.

Однак перед визначенням системи адміністративно-правових засобів забезпечення захисту персональних даних необхідно з'ясувати теоретичну сутність адміністративно-правових засобів захисту прав громадян в тій чи іншій сфері та форми її практичної реалізації. Не вдаючись в детальний теоретико-правовий аналіз сутності адміністративно-правових засобів захисту прав громадян, які давно вже вироблені загальною теорією права та теорією адміністративного права, слід лише констатувати, що адміністративно-правовими засобами захисту права громадян на свободу слова є сукупність різних за своєю сутністю та призначенням правових явищ, інструментів, заходів, які спільно вирішують завдання запобігання та припинення порушень вказаного права, а також його відновлення у разі порушення. Під адміністративно-правовими способами захисту права громадян на свободу слова слід розуміти врегульовану адміністративно-правовими нормами діяльність уповноважених органів та їх посадових осіб, спрямовану на правильне розуміння та застосування чинного законодавства, що визначає право громадян на свободу слова, на вільне вираження своїх поглядів та переконань [7, с. 34; 8, с. 240].

Якщо ж вести мову про адміністративно-правові засоби забезпечення захисту персональних даних, то під ними, на нашу думку, слід розуміти систему заходів з попередження (превентивних заходів), припинення порушень, що посягають на право володіння та розпорядження персональними даними, та застосування заходів адміністра-

тивної відповідальності органами публічної влади, які відповідно до законодавства мають забезпечувати їх захист.

Одним із дієвих засобів адміністративно-правового захисту персональних даних є застосування заходів попередження порушень законодавства у сфері захисту персональних даних, які відповідно до закону, зокрема ст. 4, мають вживати такі особи: володільць персональних даних, розпорядник персональних даних та Уповноважений Верховної Ради України з прав людини. При цьому володільцями чи розпорядниками персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи-підприємці, які обробляють персональні дані відповідно до закону. Розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу. Володільць персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного письмово. Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, які визначені у договорі [6]. Та все ж основним суб'єктом, який уповноважений застосовувати заходи попередження порушень законодавства у сфері захисту персональних даних, є Уповноважений Верховної Ради України з прав людини (далі – Уповноважений). Такі повноваження щодо контролю за дотриманням законодавства про захист персональних даних були надані цьому інституту державної служби Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», який набув чинності 1 січня 2014 року. Він був прийнятий з метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [9]. Слід зауважити, що Законом не визначена система заходів попередження порушень законодавства у сфері захисту персональних даних, однак його аналіз дає можливість виділити дві групи попереджувальних (превентивних) заходів, зокрема ті, які застосовуються володільцями, розпорядниками персональних даних, та ті, які застосовуються посадовими особами Уповноваженого. Так, володільці та розпорядники персональних даних створюють (визначають) структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці. Цей підрозділ (особа) вживає такі заходи попередження порушень законодавства у сфері захисту персональних даних: забезпечує захист цих даних від випадкової втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних; інформує та консулює володільця або розпорядника персональних даних з питань дотримання законодавства про захист персональних даних; взаємодіє з Уповноваженим та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних. Зі свого боку Уповноважений вживає такі заходи попередження порушень законодавства у сфері захисту персональних даних: отримує пропозиції та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймає рішення за результатами їх розгляду; проводить на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; отримує на свою вимогу та має доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі

доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом; затверджує нормативно-правові акти у сфері захисту персональних даних; за підсумками перевірки, розгляду звернення видає обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних; надає рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснює права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб; взаємодіє із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організують роботу, пов'язану із захистом персональних даних при їх обробці, оприлюднює інформацію про такі структурні підрозділи та відповідальних осіб; звертається з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних; надає за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проєктів кодексів поведінки у сфері захисту персональних даних та змін до них; інформує громадськість шляхом виступу з трибуни Верховної Ради України про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними (Уповноважений включає до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан дотримання законодавства у сфері захисту персональних даних); здійснює моніторинг нових практик, тенденцій та технологій захисту персональних даних; організовує та забезпечує взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних; бере участь у роботі міжнародних організацій з питань захисту персональних даних тощо.

Наступними за логікою та доцільністю застосування є заходи адміністративно-правового припинення порушення законодавства щодо захисту персональних даних, до яких слід віднести такі: безпосереднє усунення володільцем або розпорядником персональних даних порушень законодавства про захист персональних даних; отримання Уповноваженим скарг фізичних і юридичних осіб з питань захисту персональних даних та прийняття рішень за результатами їх розгляду; здійснення Уповноваженим позапланових перевірок володільців або розпорядників персональних даних із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; видання Уповноваженим вимоги (припису) про усунення порушень законодавства про захист персональних даних та підстав, які зумовлювали таке порушення. Метою внесення припису є припинення порушення законодавства про захист персональних даних та у міру можливості його виправлення, а також усунення обставин, що сприяли його виникненню, чи інших, що можуть призвести до його виникнення в майбутньому. З цією метою припис може містити, крім іншого, вказівки щодо: 1) зміни, 2) видалення або 3) знищення персональних даних, 4) забезпечення доступу до них, 5) надання чи 6) заборони їх надання третій особі, 7) зупинення або припинення обробки персональних даних. Вказані вимоги

є зрозумілими і окремого роз'яснення не потребують. Їх мета – припинити порушення Закону (наприклад, видалити дані, що обробляються незаконно), відновити порушені права (наприклад, надати суб'єкту доступ до його персональних даних чи змінити його персональні дані, що не відповідають дійсності) або запобігти потенційним порушенням в майбутньому (наприклад, припинити обробку (зокрема, збір, зберігання та використання) персональних даних, що не є необхідними для досягнення задекларованої легітимної мети їх обробки), запровадити додаткові заходи захисту персональних даних.

Невід'ємним складником дієвих засобів адміністративно-правового захисту персональних даних є застосування заходів адміністративної відповідальності за такі правопорушення: неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей; невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних; повторне протягом року вчинення порушення з числа передбачених частинами першою або другою цієї статті, за яке особу вже було піддано адміністративному стягненню; недотримання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних; повторне протягом року вчинення порушення, передбаченого частиною четвертою цієї статті, за яке особу вже було піддано адміністративному стягненню (ст. 188-39 КУпАП) [10]. Такі зміни до КУпАП були внесені Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» від 3 липня 2013 року № 383-VII [9], яким було виключено норму, яка встановлювала адміністративну відповідальність за неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних, мету збору цих даних і про осіб, яким ці дані передаються. Самі права суб'єкта персональних даних визначені в ст. 8 Закону. Цей перелік складається із 12 пунктів. Отже, відповідальність за неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних застосовується лише у разі, коли це призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, хоча неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права вже є порушенням прав суб'єкта персональних даних [11, с. 195].

Слід відзначити окремі процесуальні особливості порядку застосування заходів адміністративної відповідальності за правопорушення щодо захисту персональних даних. Відповідно до ст. 255 правом складання протоколу про адміністративне правопорушення за ст. 188-39 КУпАП, а також оформлення матеріалів справи мають уповноважені особи секретаріату Уповноваженого Верховної Ради України з прав людини або представники Уповноваженого. Відповідно до ст. 221 КУпАП таку категорію справ розглядає суд. Відповідності до ст. 276 КУпАП такі злочини розглядаються за місцем їх вчинення. Згідно зі ст. 277 КУпАП вони розглядаються у п'ятнадцятиденний строк з дня одержання органом (посадовою особою), правомочним розглядати справу, протоколу про адміністративне правопорушення та інших матеріалів справи. Водночас окремі положення законодавства унеможливають в окремих випадках притягнення особи до адміністративної відповідальності за порушення законодавства

щодо захисту персональних даних. Зокрема, як було зазначено вище, статтею 276 КУпАП встановлено, що дана категорія справ розглядається за місцем вчинення злочинів, яке іноді важко встановити, адже внесення, обробка і поширення персональних даних з порушенням законодавства може здійснюватись володільцем дистанційно (через використання ЕОМ та інтернету), тому потрібно конкретизувати, що місцем розгляду справи є юридична адреса володільця персональних даних, хоча постраждала особа шляхом звернення до суду може клопотати про розгляд справи за місцем її проживання. У такому разі суд або задовольняє клопотання, або мотивовано відмовляє в його задоволенні. Окремо слід звернути увагу на загальні строки розгляду таких справ. Так, відповідно до ст. 38 КУпАП, якщо справи про адміністративні правопорушення підвідомчі суду (судді), стягнення може бути накладене не пізніше як через три місяці з дня вчинення правопорушення. На нашу думку, слід продовжити строк притягнення до адміністративної відповідальності та накладення стягнення, адже за цей час особа повинна встигнути направити скаргу, Уповноважений має розглянути її, зібрати матеріали, оформити правопорушення (зокрема, скласти протокол), ознайомити з матеріалами правопорушника, направити матеріали до суду, а суд має розглянути справу. Переважно суб'єкт направляє скаргу із запізненням (часто навіть після закінчення трьохмісячного строку). Саме тому доцільно продовжити строки притягнення до відповідальності та накладення стягнення за порушення законодавства про захист персональних даних до одного року. Зазначене є актуальним, навіть якщо право вносити постанови у справах про порушення законодавства про захист персональних даних буде передане Уповноваженому.

Окрім цього, одним із дієвих засобів адміністративно-правового захисту персональних даних є позасудове та судове оскарження рішення про відстрочення або відмову в доступі до персональних даних. Так, статтею 18 Закону визначена можливість оскарження рішення про відстрочення або відмову у доступі до персональних даних: позасудового – до Уповноваженого Верховної Ради України з прав людини, підстави якого визначені у ст. 23 Закону; судового – до адміністративного суду у порядку, визначеному КАСУ [12]. Слід врахувати те, що якщо запит зроблено суб'єктом персональних даних щодо даних про себе, то обов'язок доведення в суді законності відмови у доступі покладається на володільця персональних даних, до якого подано запит.

Висновки. Аналітичні матеріали застосування адміністративно-правових заходів захисту персональних

даних показують, що на сьогодні вказані (хоч і не такі значні, як наприклад, незаконне поширення) правопорушення в їх сукупності чи окремо призводять до недоліків функціонування системи захисту персональних даних [13, с. 146]. Наприклад, навіть якщо очевидно, що персональні дані особи були поширені, відсутність обліку операцій, пов'язаних з обробкою персональних даних, часто унеможливує встановлення особи, причетної до такого поширення. Особу рідко повідомляють про збір її персональних даних, унаслідок чого вона і не знає про те, що її персональні дані обробляються новим володільцем, і не направляє скаргу з цього приводу. Також слід зазначити, що інколи в ході перевірки неможливо встановити конкретну особу, яка причетна до вчинення правопорушення, хоча очевидно, що воно було вчинене конкретним володільцем. Наприклад, медична інформація про особу потрапила у відкритий доступ. До цього така інформація була лише в медичному закладі, де особа проходила лікування. Очевидно, що витік інформації/персональних даних трапився у вказаній лікарні, однак встановити конкретну особу, відповідальну за незаконне поширення персональних даних, неможливо. КУПАП передбачає відповідальність лише фізичних осіб, хоча у цій ситуації стягнення слід накладати саме на юридичну особу. Найчастіше такі питання виникають, коли ідеться про недоліки процесу організації обробки персональних даних володільцем, які базуються на внутрішніх правилах володільця, які інколи є недостатньо чіткими та формальними. Отже, вкрай необхідно змінити КУПАП в частині можливості накладення стягнення на юридичних осіб. Така практика вже давно присутня в державах Європейського Союзу. Зокрема, в проєкті Регламенту викладено чіткий перелік порушень, які тягнуть за собою відповідальність як фізичних, так і юридичних осіб (стаття 79). Окремо слід наголосити, що передбачені Законом заходи реагування спрямовані на припинення/виправлення порушення законодавства про захист персональних даних та накладення стягнення на особу, відповідальну за його вчинення. Однак вони не передбачають будь-якого виду компенсації особі, чії права могли бути порушені вчиненим правопорушенням. При цьому за особою залишається право на звернення до суду з позовом про відшкодування шкоди, завданого порушенням її права на захист персональних даних. У такому разі основним доказом порушення прав особи буде відповідний припис Уповноваженого або рішення суду за результатами розгляду протоколу про притягнення до адміністративної відповідальності.

ЛІТЕРАТУРА

1. Брижко В.М. Організаційно-правові питання захисту персональних даних : дис... канд. юрид. наук : 12.00.07. Київ, 2004. 251 с.
2. Чернобай А.М. Правові засоби захисту персональних даних працівника : дис. ... канд. юрид. наук : 12.00.05 ; Одеська національна юридична академія. Одеса, 2006. 216 с.
3. Різак М.В. Правове регулювання відносин обігу персональних даних : дис. ... канд. юрид. наук : 12.00.07 ; Держ. НДІ МВС України. Київ, 2012. 214 с.
4. Тунік А.В. Правові основи захисту персональних даних : дис. ... канд. юрид. наук : 12.00.07 ; Національний авіаційний університет. Київ, 2012. 213 с.
5. Цвірюк Д.В. Адміністративно-правовий захист персональних даних в Україні : дис. ... канд. юрид. наук : 12.00.07 ; Національний авіаційний університет. Київ, 2014. 220 с.
6. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
7. Бородин І.Л. Адміністративно-правові способи захисту прав та свобод людини і громадянина : монографія. Херсон : Вид-во «Олді-плюс», 2003. 218 с.
8. Збирак Т.В. Сутність і значення адміністративно-правових засобів та способів захисту права громадян на свободу слова. *Форум права*. 2013. № 3. С. 239–244. URL: http://nbuv.gov.ua/jpdf/FP_index.htm_2013_3_41.pdf.
9. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних : Закон України від 3 липня 2013 року № 383-VII. *Відомості Верховної Ради України*. 2014. № 14. Ст. 252.
10. Кодекс України про адміністративні правопорушення від 7 груд. 1984 р. № 8073-X. *Відомості Верховної Ради УРСР*. 1984. Додаток до № 51. Ст. 1122.
11. Різак М.В. Адміністративна відповідальність за порушення законодавства у сфері обігу персональних даних: сучасний стан та перспективи подальшого розвитку. *Вісник Харківського національного університету внутрішніх справ*. 2013. № 1 (60). С. 190–197.
12. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 року. *Відом. Верхов. Ради України*. 2005. № 35–36, № 37. Ст. 446.
13. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: правове регулювання та практичні аспекти : науково-практичний посібник. Київ : К.І.С., 2015. 220 с.