ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХОДІВ ПРИПИНЕННЯ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

ПЕТРИЦЬКИЙ Андрій Леонідович - Головний консультант Управління реформування правоохоронних органів та органів юстиції Адміністрації Президента України

УДК: 351.810:340

В статье рассмотрены актуальные проблемы пресечения правонарушений в сфере защиты персональных данных. Систематизированы меры судебного и внесудебного пресечения нарушений законодательства о защите персональных данных. Определены процессуальные недостатки их применения. Сформулированы предложения, направленные на повышение оперативности пресечения нарушений в сфере защиты персональных данных.

Ключові слова: інформація, персональні дані, захист персональних даних, правопорушення, примус, припинення.

Постановка проблеми

Невпинна інформатизація суспільства, стрімкий розвиток інформаційних технологій та їх проникнення у всі сфери суспільного життя зумовлюють актуалізацію проблематики захисту персональних даних. Як показує світова історія, інформація, що дозволяє ідентифікувати конкретну особу, може бути використана не лише на благо, а й на шкоду людині, її оточенню та суспільству загалом. При цьому застосування новітніх (більш швидкісних, більш високоємних) програмно-технічних засобів обробки персональних даних має не тільки позитивний ефект, а й відчутно збільшує ризики несанкціонованого доступу до конфіденційної інформації, її незаконного поширення, порушення права на конфіденційність приватного життя.

Стрімкий розвиток інформаційних технологій зумовлює появу нових видів делікності, диктуючи необхідність постійного вдосконалення примусових засобів боротьби з правопорушеннями в сфері захисту персональних даних. Важливе місце в системі цих засобів посідають заходи державного припинення. Насамперед, саме вони покликані забезпечують негайне припинення протиправних дій. Саме вони гарантують ефективність заходів юридичної відповідальності, і саме вони сприяють якнайшвидшому відновленню порушених прав громадян.

Аналіз наукових досліджень

По мірі зростання актуальності питань припинення в сфері захисту персональних даних, вони дедалі частіше виступають предметом ґрунтовного наукового аналізу. Посильний внесок у їх вирішення здійснили В.Ю.Баскаков, Г.М.Линник та О.М.Шевчук(1, 2, 3). Водночас, ціла низка ключових аспектів припинення порушень законодавства про захист персональних даних лишаються без належної уваги. Переважна більшість вчених-правників у своїх доробках або висвітлюють їх фрагментарно, або не торкаються зовсім. Викладене зумовлює необхідність докладного висвітлення проблем припинення в сфері захисту персональних даних, а також пошуку оптимальних шляхів їх розв'язання.

Виклад основного матеріалу

Термін "припиняти" є багатозначним. В академічному словнику української мови він наділяється такими сенсами: "зупиняти

рух або розвиток чого-небудь"; "змушувати кого-небудь перестати робити щось"; "відміняти що-небудь, переривати яку-небудь дію або діяльність" [, с. 704]. Як неважко помітити, попри деякі змістовні відмінності, у всіх випадках припинення розглядається як акт, спрямований на зупинення певного процесу (руху, діяльності, розвитку), що триває в об'єктивній дійсності.

Власне кажучи, саме такий характер мають і заходи державного припинення. Як наголошує Т.О.Гуржій, головне їх призначення полягає в тому, щоб вчасно відреагувати на суспільно-небезпечні діяння, зупинити "розгортання" протиправної поведінки в часі, запобігти настанню її шкідливих наслідків або, принаймні, мінімізувати їх негативний вплив на суспільні відносини [5, с. 98].

Таким чином, головна функція державного припинення в сфері захисту персональних даних полягає в якнайшвидшому (оперативному) зупиненні правопорушень, які посягають на конфіденційність приватного життя та інформаційну безпеку людини. Реалізація цієї функції покладена на систему контролю за додержанням законодавства про захист персональних даних, до якої належать суди та Уповноважений Верховної Ради України з прав людини.

Аналіз процесуальних повноважень судів загальної юрисдикції свідчить про те, що, залежно від спеціалізації, у сфері захисту персональних даних ними можуть застосовуватись такі заходи припинення:

у порядку адміністративного судочинства – заборона вчиняти певні дії або вжиття інших припиняючих заходів, якщо існує очевидна небезпека заподіяння шкоди правам, свободам та інтересам позивача до ухвалення рішення в адміністративній справі, або захист цих прав, свобод та інтересів стане неможливим без вжиття таких заходів, або для їх відновлення необхідно буде докласти значних зусиль та витрат, а також якщо очевидними є ознаки протиправності рішення, дії чи бездіяльності суб'єкта владних повноважень (ст. 117 КАС України) [6];

у рамках адміністративно-деліктного провадження – вилучення речей і документів (ст. 265 КУпАП України) [7];

у рамках цивільного провадження – накладення арешту на майно, що належить відповідачеві і знаходиться у нього або в інших осіб; заборона вчиняти певні дії; встановлення обов'язку вчинити певні дії; інші заходи забезпечення (ст. 152 ЦПК України) [8];

у рамках кримінального провадження – тимчасове вилучення майна (зокрема, пристроїв, які використовуються для обробки та зберігання електронних баз даних. – А.П.) (див.: ст. 167 КК України) [9].

Попри очевидні змістовні відмінності, перераховані заходи володіють цілою низкою спільних ознак. По-перше, вони реалізуються в ході деліктних проваджень та підпорядковані їх загальній меті. По-друге, вони переслідують подвійну ціль – недопущення продовження протиправної поведінки та забезпечення об'єктивного розгляду справи про відповідальність за правопорушення в сфері захисту персональних даних. По-третє, вони виступають заходами процесуального забезпечення, тобто не мають самостійного характеру. По-четверте, на відміну від багатьох інших припиняючих заходів, вони не спрямовані на виявлення правопорушень (практично у всіх випадках їх застосування відбувається за фактом виявлених протиправних діянь). По-п'яте, вони можуть застосовуватись за ініціативою не лише суду, а й інших суб'єктів юридичного процесу (потерпілого, позивача тощо).

Заходи судового припинення в сфері захисту персональних даних є вельми різноманітними. При цьому основну частку в їхньому масиві становлять організаційні заходи, пов'язані з забороною вчинення певних дій або ж із зобов'язанням вчинити певні дії. Саме вони найчастіше застосовуються судами на практиці, і саме вони слугують головним інструментом припинення правопорушень у сфері прайвесі.

На відміну від судів, уповноважених застосовувати широкий спектр заходів припинення, Уповноважений Верховної Ради України з прав людини має в своєму розпорядженні тільки один подібний захід: видання припису про усунення порушень законодавства про захист персональних даних (див.: ст. 23 Закону України "Про захист

персональних даних") [10]. Такий припис видається Уповноваженим на підставі Акту перевірки додержання вимог законодавства про захист персональних даних у разі, якщо під час перевірки було виявлено порушення вимог щодо обробки персональних даних в автоматизованих системах або картотеках.

Відповідно до наказу Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 "Про затвердження документів у сфері захисту персональних даних", у приписі зазначаються: номер, дата та місце складання припису; для суб'єкта перевірки - органу державної влади та місцевого самоврядування: найменування, місцезнаходження; для суб'єкта перевірки - юридичної особи: найменування, місцезнаходження, прізвище, ім'я та по батькові керівника юридичної особи; для суб'єкта перевірки - фізичної особи та/або фізичної особи - підприємця: прізвище, ім'я та по батькові, місце її проживання; підстава для видачі припису; заходи, необхідні для усунення порушень, виявлених під час перевірки; строк виконання припису; строк інформування суб'єктом перевірки Уповноваженого про усунення виявленого порушення; підпис уповноваженої посадової особи (осіб), яка проводила перевірку [10].

Що ж стосується безпосередньо самих заходів по усуненню порушень законодавства про захист персональних даних, то їх орієнтовний перелік наведений у п. 5 ч. 1 ст. 23 Закону України "Про захист персональних даних". Наразі до цього переліку входять такі заходи, як: зміна персональних даних, видалення персональних даних, знищення персональних даних, забезпечення доступу до персональних даних, надання чи заборона надання персональних даних третій особі, зупинення обробки персональних даних та припинення обробки персональних даних.

Вказаний перелік не є вичерпним. Зміст п. 5 ч. 1 ст. 23 Закону України "Про захист персональних даних" сформульовано в спосіб, який допускає можливість застосування й інших, крім вказаних у Законі, заходів щодо усунення порушень законодавства про захист персональних даних. У якості таких заходів можуть застосовуватись знеособлення персональних даних, реєстрація персональних даних, перегляд персональних даних, отримання згоди суб'єкта персональних даних на їх обробку при зміні мети обробки, вимога привести внутрішньо-організаційні процедури або акти до вимог законодавства про захист персональних даних та інші.

Слід зазначити, що припис стосовно усунення порушень законодавства про захист персональних даних, хоч і має обов'язковий характер, але не обмежує адресата у виборі форм його реалізації.

Наочним прикладом може слугувати Припис від 13.09.2013 № 125 Про усунення порушень вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки Державної адміністрації залізничного транспорту України («Укрзалізниця»).

Зокрема, п. 1 Припису містить вимогу: "забезпечити внесення до проїзних документів прізвища та імені пасажира зі слів особи, яка здійснює оплату проїзного документа, при оформленні у квитковій касі повних та дитячих проїзних документів, без зберігання персональних даних таких пасажирів у базах даних Єдиної автоматизованої системи керування пасажирськими перевезеннями, яка експлуатується ДП "ГІОЦ Укрзалізниці", та в будь-яких інших базах даних (підкреслено мною. – А.П.)".

Зі свого боку, Укрзалізниця рамках поставленої вимоги здійснила оновлення програмного забезпечення Єдиної автоматизованої системи керування пасажирськими перевезеннями (АСК ПП УЗ), внаслідок чого при друкуванні прізвища та ім'я пасажира в бланку проїзних документів відповідні дані перестали заноситись та зберігатись у базі даних АСК ПП УЗ. Програмне забезпечення з внесеними змінами було введено в експлуатацію з 28 листопада 2013 року [10].

Подібно багатьом іншим заходам державного примусу, припинення порушень законодавства про захист персональних даних реалізується за чітко визначеною процедурою, покликаною забезпечити послідовність і впорядкованість юрисдикційної діяльності, об'єктивність і своєчасність роз-

гляду справи, одноманітність правозастосування, всебічне забезпечення прав учасників правовідносин.

Деталі цієї процедури, а також юридичні наслідки її порушення конкретизовані в наказі Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 "Про затвердження документів у сфері захисту персональних даних". Згідно з п.п. 5.12-5.17 цього наказу, у разі виявлення порушень інформаційного законодавства під час перевірки суб'єкта обробки персональних даних, уповноважена посадова особа складає припис про їх усунення в двох примірниках. Перший примірник не пізніше 5 робочих днів з дня складання Акта перевірки надсилається суб'єкту перевірки чи уповноваженій ним особі рекомендованим листом з повідомленням про вручення. Другий – зберігається в Секретаріаті Уповноваженого.

У свою чергу, адресат припису (читай – суб'єкт перевірки) повинен протягом зазначеного в приписі строку (не менше ніж 30 календарних днів) вжити заходи щодо усунення порушень, зазначених у приписі, та письмово поінформувати про них Уповноваженого разом із наданням копій документів, що це підтверджують.

У разі невиконання припису адресатом щодо нього складається протокол про адміністративне правопорушення, передбачене ст. 188-40 КУпАП "Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини" [6].

Аналіз наведених положень змушує констатувати надмірну і, на наш погляд, невиправдану "розтягнутість" процедури реалізації заходів, спрямованих на припинення порушень законодавства про захист персональних даних.

Як відомо, необхідною умовою ефективності припиняючих заходів є невідкладність їх здійснення. Чим швидше припиняється порушення, тим більше шансів на цілковите відновлення дестабілізованих ним правовідносин, тим вища ймовірність відвернення (мінімізації) його шкідливих наслідків, тим дієвіша система захисту прав та інтересів людини. Саме тому заходи припинення передбачають спрощений (порівняно з заходами юридичної відповідальності) порядок реалізації. І саме тому в основу їх застосування покладено принцип оперативності.

Наразі цього не можна сказати про державне припинення в сфері захисту персональних даних. Згідно з існуючою процедурою, мінімальний строк реалізації відповідних заходів становить 30 (!) календарних днів, та й то – за умови невідкладного винесення припису про усунення виявлених порушень. На практиці ж цей строк практично завжди є більшим.

У світлі викладеного існуючі строки винесення та виконання припису Уповноваженого про усунення порушень інформаційного законодавства виглядають необґрунтованими. Насамперед, це стосується строку, відведеного на реалізацію припису адресатом. Парадоксально, але факт: на відміну від більшості правозастосовних процедур, процедура реалізації припиняючих заходів у сфері захисту персональних даних не тільки не спонукає до якнайшвидшого припинення порушень, а навпаки – всіляко його відтерміновує. Саме такий висновок випливає зі змісту п. 5.13 наказу Уповноваженого від 8 січня 2014 року № 1/02-14, яким передбачено, що зазначений в приписі строк усунення порушень повинен бути меншим, ніж 30 календарних днів [6].

У результаті маємо ситуацію, коли виявлене порушення правил обробки та захисту персональних даних, замість негайного припинення, триває й далі, продовжуючи чинити деструктивний вплив на суспільні відносини та створюючи загрозу інформаційним правам людини.

Про причини існування настільки значної прогалини між часом складання припису та часом реалізації передбачених ним заходів сьогодні можна тільки здогадуватись. Як засвідчили результати опитування посадових осіб секретаріату Уповноваженого та Державної служби України з питань захисту персональних даних (до 2014 року ця служба здійснювала контроль у сфері захисту персональних даних за аналогічною процедурою), 20% респондентів пояснюють наявність такої прогалини тим, що усунення виявлених порушень може вимагати великих часових затрат, пов'язаних із змінами

програмного забезпечення, вдосконаленням технічних систем захисту інформації, розробкою регламентних документів тощо.

На думку 40% опитаних, 30-денний строк виконання припису Уповноваженого зумовлений аналогічною тривалістю строків, відведених на здійснення оператором персональних даних обов'язкових організаційних дій, зокрема: повідомлення Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод їх суб'єктів; повідомлення суб'єкта про збирання та обробку пов'язаних з ним персональних даних; задоволення запиту на доступ до персональних даних і т.п. На підставі цього робиться припущення, що, оскільки впродовж 30 днів необхідну дію може бути виконано в цілком законному порядку, констатувати порушення раніше – означає порушувати права володільця/розпорядника персональних даних.

Варто додати, що більша третина (40%) учасників опитування взагалі не спромоглась дати логічне пояснення 30-денної тривалості припису про усунення порушень у сфері персональних даних.

Власне, це і не дивно, адже при детальному розгляді вищенаведені пояснення виглядають недостатньо переконливими. По-перше, далеко не завжди усунення інформаційних порушень пов'язане з удосконаленням (модернізацією) програмно-технічного забезпечення обробки персональних даних. Зазвичай, такі порушення мають суто організаційний характер і полягають у недотриманні вимог щодо способів збору й накопичення персональних даних, строків та умов зберігання персональних даних, зміни, видалення або знищення персональних даних, порядку доступу до персональних даних, отримання згоди на обробку персональних даних, задоволення законних вимог суб'єкта персональних даних, своєчасного повідомлення про обробку персональних даних etc. Відповідно, припинення цих порушень може і повинно здійснюватись у якнайшвидший строк.

По-друге, теза про доцільність 30-денного строку для усунення виявлених порушень, на тій підставі, що аналогічний строк відводиться на вчинення обов'язкових дій по організації обробки персональних даних, не витримує перевірки практикою. На практиці припис про усунення порушень правил обробки персональних даних видається Уповноваженим в ході планових або позапланових перевірок стану дотримання інформаційного законодавства. Планові перевірки проходять не частіше одного разу на рік, а плани їх проведення заздалегідь оприлюднюються на сайті Уповноваженого. Це дозволяє презюмувати обізнаність суб'єкта обробки персональних даних із часом проведення перевірки. Останній завжди має змогу прискорити здійснення необхідних організаційних операцій і вчинити їх до початку перевірки, або ж, якщо це об'єктивно неможливо, зазначити точний час їх здійснення безпосередньо в акті перевірки. У будь-якому разі організаційні заходи, не здійснені на момент перевірки, однак заплановані у визначений законом строк, не вважаються порушенням, а отже, не можуть слугувати підставою для вжиття припиняючих заходів.

Що ж до позапланових перевірок, то, як правило, вони проводяться вже за фактом виявлених порушень (при безпосередньому виявленні порушень вимог законодавства про захист персональних даних Уповноваженим, при наявності інформації про порушення вимог інформаційного законодавства в ЗМІ, при наявності звернення фізичних та юридичних осіб з повідомленням про порушення), тобто тоді, коли строки вчинення необхідних організаційних дій, пов'язаних з обробкою персональних даних, вже сплили. За таких умов жодної потреби в 30-денному "очікуванні" немає. Навпаки, потрібне негайне припинення наявних порушень та якнайшвидше усунення їхніх наслідків.

З урахуванням викладеного, встановлення для реалізації заходів щодо усунення порушень у сфері захисту персональних даних мінімального строку в 30 календарних днів видається необґрунтованим. На наш погляд, у наказі Уповноваженого від 8 січня 2014 року № 1/02-14 має йтися не про встановлення відповідного часового зазору, а про обов'язок суб'єкта обробки персональних даних усунути допущені порушення

в розумний строк – тобто в найкоротший строк, достатній для своєчасного (без невиправданих зволікань) припинення порушення та відновлення порушених прав, свобод та інтересів.

Ще одним чинником, який гальмує припинення порушень законодавства про захист персональних даних, є надмірна тривалість процедури складання та надіслання відповідного припису. Діючий порядок контролю за додержанням законодавства про захист персональних даних (п. 5.12 наказу Уповноваженого від 8 січня 2014 року № 1/02-14) відводить на цю процедуру 5 робочих днів. В умовах, коли порушені права людини потребують невідкладного захисту та відновлення, такий строк навряд чи можна визнати оптимальним. Більше того, є всі підстави для висновку про доцільність його скорочення.

Як уже зазначалося, припис щодо порушень законодавства у сфері захисту персональних даних складається на підставі раніше складеного Акта перевірки. При цьому останній обов'язково містить інформацію: "… про виявлені в діяльності суб'єкта перевірки порушення вимог законодавства про захист персональних даних, їх детальний опис із посиланням на норми чинного законодавства, які порушено" (див.: п. 5.3. наказу Уповноваженого від 8 січня 2014 року - № 1/02-14) [6].

Фактично, це означає, що виявлення, кваліфікація та аналіз всіх юридично-значущих обставин порушення відбуваються на етапі складання Акта перевірки. Натомість, процес складання припису щодо усунення виявлених порушень не вимагає проведення складних логіко-юридичних і технічних операцій – дані про вчинене правопорушення "механічно" переносяться до нього з Акту перевірки.

Не вимагає особливих часових затрат і розробка заходів припинення. Зазвичай, суб'єкт перевірки (Уповноважений) такі заходи в приписі не конкретизує, обмежуючись вимогою усунення порушень законодавства та покладаючи вибір необхідних для цього засобів на розсуд самого порушника.

Таким чином, складання та надислання припису про усунення порушень у сфері захисту персональних даних – це відносно "негроміздка", в бюрократичному і технічному відношеннях, процесуальна дія. Вона може і повинна здійснюватись у максимально стислий строк, що дозволить якнайшвидше припинити наявне порушення, усунути пов'язані з ним ризики, відновити порушені ним права, нейтралізувати його шкідливі наслідки.

Що ж стосується тривалості цього строку, то, вочевидь, він не повинен перевищувати 3-х робочих днів з дня складання Акту перевірки Уповноваженого. Саме такий висновок випливає з результатів опитування працівників секретаріату Уповноваженого та Державної служби України з питань захисту персональних даних. Майже дві третини респондентів (60%) вважають 3-денний строк цілком достатнім для якісного складання та оперативного надислання припису щодо усунення порушень у сфері захисту персональних даних.

Висновок

Отже, з урахуванням викладеного, можемо констатувати, що на сьогодні в сфері захисту персональних даних застосовується розмаїта система заходів припинення. Вона охоплює широкий комплекс майнових та організаційних заходів, котрі реалізуються як в судовому, так і в позасудовому порядку. Аналіз практики застосування цих заходів свідчить про достатньо високий рівень їх ефективності. У більшості випадків вони характеризуються своєчасністю, обґрунтованістю, доцільністю й результативністю, що забезпечує чітке припинення правопорушень та мінімізацію їх шкідливих наслідків.

Разом з тим, варто звернути увагу на надмірну тривалість процедури застосування припиняючих заходів у позасудовому порядку. Існуючі нормативні обмеження фактично унеможливлюють миттєве реагування на делікт. Наразі мінімальна тривалість процедури усунення порушень, які виявляються в ході перевірок суб'єктів обробки персональних даних, становить 30 календарних днів з дня винесення припису про усунення таких порушень. Враховуючи, що це лише мінімальний строк, а також те, що на складання й надіслання відповідного

АНОТАЦІЯ

У статті розглянуті актуальні проблеми припинення правопорушень у сфері захисту персональних даних. Систематизовано заходи судового та позасудового припинення порушень законодавства про захист персональних даних. Визначені процесуальні недоліки їх застосування. Сформульовані пропозиції, спрямовані на підвищення оперативності припинення порушень у сфері захисту персональних даних.

припису відводиться 5 робочих днів, процес застосування припиняючих заходів, як правило, триває значно довше. В умовах необхідності якнайшвидшого припинення інформаційних правопорушень подібний стан справ неможливо визнати прийнятним.

Оптимальним способом розв'язання цієї проблеми є оптимізація строків складання, надислання та виконання припису Уповноваженого щодо усунення порушень у сфері захисту персональних даних. З цією метою пропонуємо внести до наказу Уповноваженого від 8 січня 2014 року № 1/02-14 наступні зміни:

абз. 8 п. 5.11. наказу викласти в такій редакції: "строк виконання припису (найкоротший строк, достатній для своєчасного (без невиправданих зволікань) припинення порушення та відновлення порушених прав, свобод та інтересів)";

п. 5.12. наказу викласти в такій редакції: "Припис складається у двох примірниках: перший примірник не пізніше 3 робочих днів з дня складання Акта перевірки надсилається суб'єкту перевірки чи уповноваженій ним особі рекомендованим листом з повідомленням про вручення, а другий примірник залишається в Секретаріаті Уповноваженого";

у п. 5.13 слова "(не менше ніж 30 календарних днів)" вилучити.

Як уявляється, пропоновані зміни забезпечать істотне прискорення процесу припинення порушень у сфері захисту персональних даних, гарантуючи якнайшвидше відновлення порушених прав, стабілізацію інформаційних правовідносин, усунення причин і умов, що сприяють деліктності.

SUMMARY

The article discusses topical issues stopping offenses in the sphere of personal data protection. Judicial and non-judicial measures of stopping violations the rules of personal data protection are systematized. Procedural shortcomings of their application are defined. Proposals aimed at improving efficiency of stopping measures in the sphere of personal data protection are formulated.

Література

1. Баскаков В. Ю. Адміністративно-правовий режим інформації з обмеженим доступом : дис. ... канд. юрид. наук : 12.00.07 / Баскаков Володимир Юрійович. – К., 2012. – 194 с.

2. Линник Г. М. Особливості адміністративних правопорушень інформаційного характеру /- Г. М. Линник // Підприємництво, господарство і право. – 2010. – № 7. – С. 69-72.

3. Шевчук Ю. М. Адміністративно-правове регулювання у сфері забезпечення інформаційної безпеки : дис. ... канд. юрид. наук : 12.00.07 / Шевчук Юрій Миколайович. – Запоріжжя, 2011. – 210 с.

4. Словник української мови. – в 11 томах . [О. Є. Марцинківська, Л. О. Родніна, В. М. Русанівський та ін.] ; за ред. І. К. Білодіда, К. : Наукова думка, 1976. – Т. 7. – 458 с.

5. Гуржій Т. О. Адміністративне право України : [навчальний посібник] / Т. О. Гуржій. – К. : КНТ, 2011. – 680 с.

6. Кодекс адміністративного судочинства України // Офіційний вісник України. – 2005. –- № 32. – Ст. 1918.

7. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР. – 1984. – додаток до № 51. – Ст. 1122.

8. Цивільний процесуальний кодекс України // Офіційний вісник України. – 2004. – № 16. – Ст. 1087.

9. Кримінальний процесуальний кодекс України // Відомості Верховної Ради України. – 2013. – № 9-10, № 11-12, № 13. – Ст.88.

10. Закон України "Про захист персональних даних" // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

11. Наказ Уповноваженого Верховної Ради України з прав людини від 8 січня 2014 року № 1/02-14 "Про затвердження документів у сфері захисту персональних даних" // Бізнес-Бухгалтерія-Право. Податки. Консультації. – 2014. – № 9. – С. 14.

12. Укрзалізницею виконано вимоги припису ДСЗПД України // Офіційний сайт Державної служби України з питань захисту персональних даних [Електронний ресурс]. – Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/64463;jsessionid=42C6519EBAD7A8F3117218BB82786E50