УДК 342.1
DOI https://doi.org/10.24144/2307-3322.2024.84.3.9

СПОСОБИ І МЕТОДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ: ТЕОРЕТИЧНИЙ АНАЛІЗ ТА ПРАКТИЧНІ АСПЕКТИ

Головацький Н.Т.,
старший викладач кафедри
адміністративного, фінансового та інформаційного права
юридичного факультету
ДВНЗ «Ужгородський національний університет»

Головацький Н.Т. Способи і методи адміністративно-правового захисту персональних даних в мережі інтернет: теоретичний аналіз та практичні аспекти.

В даній науковій статті комплексно досліджуються різноманітні методи та підходи до адміністративно-правового захисту персональних даних в онлайн-середовищі. Акцентується увага на важливості комплексного застосування різних методів захисту, а також на необхідності постійного вдосконалення законодавства у цій сфері з урахуванням розвитку нових технологій та викликів.

У статті ґрунтовно вивчаються теоретичні засади адміністративно-правового захисту персональних даних. Досліджуються поняття «персональні дані» та «адміністративний захист» у контексті даної тематики. Аналізуються положення чинного законодавства України та Європейського Союзу, що регулюють питання захисту персональних даних.

Окрему увагу автори приділяють діяльності Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних. Розкриваються повноваження Уповноваженого, а також процедури проведення перевірок та застосування заходів адміністративного припинення порушення законодавства у сфері захисту персональних даних.

Важливим аспектом дослідження є аналіз адміністративної відповідальності за порушення законодавства про захист персональних даних. Описуються види порушень, за які передбачено адміністративну відповідальність.

У статті пропонуються низка рекомендацій щодо вдосконалення адміністративно-правового захисту персональних даних в Україні. До яких належать прийняття нових та внесення змін до чинних законодавчих актів, які б більш чітко регламентували питання захисту персональних даних в онлайн-середовищі; забезпечення належного фінансування діяльності Уповноваженого Верховної Ради України з прав людини; проведення регулярних тренінгів та семінарів для державних службовців та представників бізнесу з питань захисту персональних даних; посилення співпраці з міжнародними організаціями в сфері захисту персональних даних.

На основі проведеного дослідження автор робить висновок, що адміністративно-правові методи захисту персональних даних є важливою складовою комплексної системи захисту прав та свобод людини в цифровому середовищі. Ефективність захисту персональних даних може бути забезпечена лише за умови комплексного застосування різних методів, постійного вдосконалення законодавства та дієвого контролю за його дотриманням.

Ключові слова: персональні дані, адміністративний захист, Інтернет, законодавство, Уповноважений Верховної Ради України з прав людини, адміністративна відповідальність.

Holovatskiy N.T. Ways and methods of administrative and legal protection of personal data on the Internet: theoretical analysis and practical aspects.

This scientific article comprehensively examines various methods and approaches to the administrative and legal protection of personal data in the online environment. Emphasis is placed on the importance of comprehensive application of various methods of protection, as well as on the need for constant improvement of legislation in this area, taking into account the development of new technologies and challenges.

The article thoroughly studies the theoretical principles of administrative and legal protection of personal data. The concepts of «personal data» and «administrative protection» are studied in the context of this topic. The provisions of the current legislation of Ukraine and the European Union, which regulate the issue of personal data protection, are analyzed.

The authors pay special attention to the activities of the Commissioner of the Verkhovna Rada of Ukraine for human rights in the field of personal data protection. The powers of the Commissioner are disclosed, as well as the procedures for carrying out inspections and applying measures for administrative termination of violations of legislation in the field of personal data protection.

An important aspect of the research is the analysis of administrative liability for violation of the legislation on personal data protection. Describes the types of violations for which administrative responsibility is provided.

The article offers a number of recommendations for improving the administrative and legal protection of personal data in Ukraine. These include the adoption of new and amendments to current legislation that would more clearly regulate the issue of personal data protection in the online environment; ensuring adequate financing of the activities of the Commissioner of the Verkhovna Rada of Ukraine for human rights; conducting regular trainings and seminars for civil servants and business representatives on issues of personal data protection; strengthening cooperation with international organizations in the field of personal data protection.

Based on the conducted research, the author concludes that administrative and legal methods of personal data protection are an important component of a comprehensive system of protection of human rights and freedoms in the digital environment. The effectiveness of personal data protection can be ensured only under the condition of comprehensive application of various methods, constant improvement of legislation and effective control over its compliance.

Key words: personal data, administrative protection, Internet, legislation, Commissioner of the Verkhovna Rada of Ukraine for human rights, administrative responsibility.

Постановка проблеми. У зв'язку з стрімким розвитком цифрових технологій та збільшенням обсягів обробки персональних даних в мережі Інтернет, виникає актуальна проблема ефективного захисту конфіденційності та безпеки цих даних. З моменту збору до зберігання та передачі, персональні дані стають уразливими перед різноманітними кіберзагрозами та порушеннями приватності. Подолання цієї проблеми вимагає ретельного теоретичного аналізу та визначення оптимальних способів та методів адміністративно-правового захисту персональних даних в мережі Інтернет.

На сьогоднішній день існують невирішені питання та невідомі аспекти, пов'язані з оптимальним використанням адміністративно-правових інструментів для забезпечення цілісності, доступу та конфіденційності персональних даних в онлайн-середовищі. Крім того, зростання технологічних викликів, які включають розвиток штучного інтелекту та аналізу даних, підкреслює необхідність актуалізації підходів до захисту персональних даних.

Отже, постановка проблеми в цій науковій роботі полягає в необхідності вивчення та аналізі різних способів та методів адміністративно-правового захисту персональних даних в мережі Інтернет, а також визначенні їхньої ефективності в контексті вирішення складних викликів цифрового середовища.

Аналіз останніх досліджень і публікацій. Дослідженням проблематики захисту персональних даних в Україні приділяється надзвичайно багато уваги, оскільки відносяться до основоположних прав людини.

Значний вклад до вирішення окресленої проблеми проявляли М.В. Бем, І.М. Городинський, М.В. Різак, О.М. Родіоненко, О.Г. Рогова, Т.П. Попович, С.Й. Литвин, В.М. Брижко, К.С. Мельник, Т. Обуховська, В.В. Оніщенко та інші вчені.

Проте стан вирішення окресленої проблематики потребує подальшого дослідження та кінцевого вирішення, оскільки станом на сьогоднішній день існують ймовірності розкриття персональних даних та незаконної передачі їх третім особам, що є грубиш порушенням прав особи.

Мета статті полягає в дослідженні різноманітних методів та підходів до адміністративно-правового захисту персональних даних в онлайн-середовищі. Головною метою статті є розкриття теоретичних засад та практичних аспектів застосування адміністративно-правових інструментів для ефективного контролю та забезпечення конфіденційності та безпеки персональних даних ко-

ристувачів в Інтернеті. Також буде спроба в аналізі теоретичних засад та практичних аспектів адміністративно-правового захисту персональних даних в мережі Інтернет з метою визначення ефективних методів та підходів для забезпечення конфіденційності та безпеки цих даних.

Виклад основного матеріалу. Поняття «персональні дані» та «адміністративний захист» є ключовими у контексті дослідження адміністративно-правового захисту персональних даних в Інтернеті. Персональні дані визначаються як будь-яка інформація, що стосується ідентифікованої фізичної особи або такої, яка може бути ідентифікована [1].

Відповідно до Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», ідентифікація особи - встановлення особи шляхом порівняння наданих даних (параметрів), у тому числі біометричних, з наявною інформацією про особу в реєстрах, картотеках, базах даних тощо [2].

Згідно з Угодою між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво ратифікованої Законом України від 12.07.2017 року № 2129-VIII, термін «Персональні дані» означає будь-які дані, що стосуються ідентифікованої або такої, яка може бути ідентифікована, фізичної особи: фізична особа, яка може буде ідентифікована, – це особа, яка може бути прямо або опосередковано ідентифікована, зокрема за допомогою її ідентифікаційного номеру або одного чи декількох факторів щодо її фізичної, фізіологічної, психологічної, економічної, культурної або соціальної ідентичності [3].

Можна припустити, що така інформація може включати ім’я, адресу, номери телефонів, електронні адреси, а також більш складні дані, такі як генетичні, біометричні, фізичні, фізіологічні, психологічні, економічні, культурні або соціальні, які в своїй природі дадуть змогу встановити особу. Тобто такі дані відносяться до інформації приватного характеру та можуть бути використаними чи зібраними виключно на підставі добровільної згоди суб’єкта-носія таких даних.

Стаття 32 Конституції України закріплю положення про недоторканість особистого та сімейного життя, а саме:

– Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

– Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

– Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

– Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім’ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Відтак, Рішенням Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від 20.01.2012 р., встановив, що інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов’язані з особою та членами її сім’ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною [5].

Тобто будь яка інформація про особу, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень відноситься виключно до конфіденційної інформації та носить приватний характер.

Адміністративний захист відіграє важливу роль у забезпеченні конфіденційності, цілісності персональних даних та доступності до них. Це сукупність заходів, політик, процедур та технічних засобів, спрямованих на захист даних від несанкціонованого доступу, втручання та зміни.

Постановою Кабінету Міністрів України № 518 від 19 червня 2019 р. «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» визначено, що політика ін-

формаційної безпеки – політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки [6].

В свою чергу інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [7].

Проте при користуванні мережею Інтернет існує загроза порушення інформаційної безпеки в електронних комунікаціях, які використовуються суб'єктами владних повноважень для здійснення своїх безпосередніх функцій.

Закон України «Про електронні комунікації» закріплює, що електронна комунікаційна мережа – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг [8].

Також цим Законом визначено поняття «безпека мереж і послуг», що є здатністю електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги.

Не менш важливою участю в адміністративному забезпеченні захисту персональних даних є діяльність Уповноваженого Верховної Ради з прав людини, оскільки здійснюється безпосереднє усунення порушень вимог Закону про захист персональних даних. Уповноважений ВРУ з прав людини здійснює контроль за додержанням законодавства про захист персональних даних шляхом проведення перевірок, на підставі Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних [9].

Цим Порядком встановлюється процедура здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням вимог законодавства про захист персональних даних шляхом проведення перевірок фізичних осіб, фізичних осіб - підприємців, підприємств, установ і організацій усіх форм власності, органів державної влади та місцевого самоврядування, що є володільцями та/або розпорядниками персональних, а також оформлення і розгляд результатів перевірок. Варто зауважити, що цей Порядок передбачає як попередження порушень у сфері захисту персональних даних, так і реагування Уповноваженим на вже вчинені правопорушення. У Порядку визначено, що є виїзні та безвиїзні, планові та позапланові перевірки суб'єктів, які є володільцями та/або розпорядниками персональних даних.

Для розгляду нашого питання, цікавість викликають саме позапланові перевірки, оскільки через призму таких перевірок можна зрозуміти оперативне реагування на порушення норм законодавства у сфері захисту персональних даних.

Виходячи з положень вищезгаданого порядку, позапланові перевірки суб'єктів перевірки можуть проводитись за наявності наступних підстав:

– за власною ініціативою Уповноваженого;

– при безпосередньому виявленні порушень вимог законодавства про захист персональних даних Уповноваженим, в тому числі і в результаті здійснення дослідження системних проблем щодо забезпечення права на приватність, повагу до приватного та сімейного життя;

– при наявності інформації про порушення вимог законодавства про захист персональних даних в повідомленнях, опублікованих в засобах масової інформації, оприлюднених в мережі Інтернет;

– обґрунтовані звернення фізичних та юридичних осіб з повідомленням про порушення фізичною особою, фізичною особою-підприємцем, підприємством, установою і організацією усіх форм власності, органом державної влади чи місцевого самоврядування, що є володільцями та/або розпорядниками персональних даних вимог законодавства про захист персональних даних;

– виявлення недостовірності у відомостях (даних), наданих суб'єктом перевірки на письмовий запит Уповноваженого щодо здійснення безвиїзної перевірки, та/або якщо такі відомості (дані) не дають змоги оцінити виконання суб'єктом перевірки вимог законодавства про захист персональних даних;

– контроль за виконанням суб'єктом перевірки приписів щодо усунення порушень вимог законодавства про захист персональних даних, виданих за результатами проведення перевірок [9].

З огляду на вказані підстави для перевірки, можна відзначити те, що для реагування Уповноваженого на порушення законодавства про захист персональних даних, може бути і фактичне повідомлення про правопорушення, а також можуть бути обставини, які дають підстави вважати, що таке правопорушення вже вчинене або може бути вчинене при відсутності активних дій в попередженні таких порушень.

За результатами виїзної, безвиїзної, планової чи позапланової перевірки складається Акт перевірки додержання вимог законодавства про захист персональних даних, який встановлює наявність або відсутність порушень законодавства у сфері захисту персональних даних. На підставі Акту перевірки, при виявленні порушень законодавства у сфері захисту персональних даних складається припис про усунення порушень вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки, який повинен бути виконаний у встановлені строки.

У випадку невиконання припису протягом вказаного у ньому строку Уповноважений або уповноважена посадова особа складає протокол про адміністративне правопорушення, передбачене статтею 188-40 Кодексу України про адміністративні правопорушення. Норма статті 188-40 передбачає відповідальність за невиконання законних вимог Уповноваженого Верховної Ради України з прав людини, яке тягне за собою накладення штрафу на посадових осіб, громадян - суб'єктів підприємницької діяльності від ста до двохсот неоподатковуваних мінімумів доходів громадян [10].

Проте нормою статті 188-39 КУпАП закріплено відповідальність за порушення законодавства у сфері захисту персональних даних, а саме:

– 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

– недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних.

З огляду на це, можна стверджувати, що невиконання конкретно приписів, на підставі результатів проведених перевірок, передбачена відповідальність за статтею 188-40 КУпАП, оскільки за статтею 188-40 КУпАП, законною вимогою Уповноваженого може бути не лише припис, а й звернення Уповноваженого до того чи іншого суб'єкта володільця та/або розпорядника персональних даних.

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; 3) знищення персональних даних; 4) забезпечення доступу до них; 5) надання; 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 [11], 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 України «Про захист персональних даних» [1].

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.

Висновки. Отже, в результаті проведеного дослідження можна дійти до висновків, що існують різноманітні методи та підходи до адміністративно-правового захисту персональних даних в онлайн-середовищі, кожен з яких має свої переваги та недоліки. Важливо комплексно використовувати різні методи та підходи для забезпечення ефективного захисту персональних даних.

Постійне вдосконалення законодавства про захист персональних даних є важливим з урахуванням розвитку нових технологій та викликів. Важливу роль у захисті персональних даних відіграє діяльність Уповноваженого Верховної Ради України з прав людини. Застосування заходів адміністративно-правового припинення порушення законодавства щодо захисту персональних даних та адміністративної відповідальності за такі правопорушення є важливим інструментом забезпечення дотримання законодавства.

В цілому, адміністративно-правові методи захисту персональних даних є важливою складовою комплексної системи захисту прав та свобод людини в цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист персональних даних. Закон України від 01.06.2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
2. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус. Закон України від 20.11.2012 № 5492-VI. *Відомості Верховної Ради України* від 20.12.2013. № 51, стор. 2733, стаття 716.
3. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво. Україна, Європейський Союз; Угода, Міжнародний документ від

14.12.2016. *Офіційний вісник України* від 08.08.2017. № 62 / № 71, 2017, ст. 2192, код 87142/2017 / стор. 5, стаття 1901, код акта 86777/2017.
4. Конституція України. Закон від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради*. 1996. № 30. 141 с.
5. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України № 2-рп/2012 від 20.01.2012 р. *Вісник Конституційного Суду України* від 2012 р., № 2, стор. 14
6. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Постанова. Кабінет Міністрів України від 19.06.2019 № 518. *Урядовий кур'єр* від 26.06.2019, № 118.
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Указ Президента України від 28.12.2021 № 685/2021 *Офіційний вісник Президента України* від 05.01.2022. № 1, стор. 52, стаття 31
8. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. *Офіційний вісник України* від 26.01.2021 р., № 6, стор. 10, стаття 306, код акта 102665/2021.
9. Про затвердження документів у сфері захисту персональних даних. Наказ Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14. *Бізнес-Бухгалтерія-Право. Податки. Консультації* від 03.03.2014 р., № 9, стор. 14.
10. Кодекс України про адміністративні правопорушення від 7 груд. 1984 р. № 8073-X. *Відомості Верховної Ради УРСР*. 1984 р., № 51, стаття 1122.
11. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних. Закон України від 03.07.2013 № 383-VII. *Відомості Верховної Ради*, 2014, № 14, ст. 252.
12. Бєлова М.В., Бєлов Д.М., Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник УжНУ. Серія «Право».* Випуск 79(5). 2023. С. 289–294.
13. Бєлов Д.М., Бєлова М.В., Штучний інтелект в судочинстві та судових рішеннях, потенціал та ризики. *Науковий вісник УжНУ. Серія «Право».* Випуск 78(4). Ч. 3. 2023. С. 122–129.