

Шинкар Тетяна Ігорівна,

доктор юридичних наук, доцент, доцент кафедри менеджменту та соціально-гуманітарних дисциплін Львівської філії Приватного вищого навчального закладу «Європейський університет», вул. Кушевича, 5, м. Львів, 79000; shtatyanai@gmail.com; <https://orcid.org/0000-0002-3252-2167>

ОБМЕЖЕННЯ ПРАВА НА ІНФОРМАЦІЮ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ОБОВ'ЯЗОК ДЕРЖАВИ ЩОДО «КОМПЕНСАЦІЇ» ВТРАЧЕНИХ ОСОБОЮ ІНФОРМАЦІЙНИХ МОЖЛИВОСТЕЙ

Анотація. У статті розглянуто проблемні питання застосування обмеження права на інформацію як інструменту стримування та протидії загрозам інформаційній безпеці України, нейтралізації інформаційної агресії, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвитку міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки; використання якого потребує «компенсації» втрачених особою інформаційних можливостей, який не став досі предметом наукової дискусії із фіксацією його результатів у документах стратегічного планування.

На підставі аналізу останніх досліджень і публікацій встановлено відсутність єдиного механізму компенсаційного обмеження права на інформацію, намагання судами України та державними органами, до компетенції яких належить регулювання інформаційної діяльності, напрацювати власні шляхи й механізми застосування обмеження права на інформацію із «найменшими втратами» суб'єктів інформаційної діяльності, які ґрунтуються насамперед на врахуванні власної практики надання правової оцінки кожному з таких випадків.

Виходячи з актуальності і значущості проблеми, метою статті визначено викладення результатів проведеного аналізу змісту обмеження права на інформацію як засобу забезпечення інформаційної безпеки та обов'язку держави та формулювання на цій основі науково обґрунтованих пропозицій щодо «компенсації» втрачених особою інформаційних можливостей.

Підкреслено необхідність подальшого аналізу та формування обґрунтованої позиції щодо кожного режиму забезпечення національної безпеки окремо можливості застосування механізмів обмеження права на інформацію у загальній практиці забезпечення інформаційної безпеки й спеціальних обмежувальних заходах до суб'єктів інформаційної діяльності.

Проаналізовано практику адміністративних судів із надання правової оцінки обґрунтованості визнання інформаційної та іншої діяльності суб'єкта інформаційних відносин протиправною, а також правової оцінки дій суб'єктів забезпечення національної безпеки у межах наданих їм повноважень і положень Конвенції про захист прав людини і основоположних свобод.

Подальші наукові розвідки у питанні обґрунтування окремих обмежень права на інформацію запропоновано акцентувати навколо розгляду суспільного інтересу як «компенсатора» певного обмеження права на інформацію й застосування «трискладового тесту» у практиці застосування обмежень.

Ключові слова: інформаційна безпека, право на інформацію, обмеження права на інформацію, компенсація, адміністративний суд.

RESTRICTION OF THE RIGHT TO INFORMATION AS A MEANS OF ENSURING INFORMATION SECURITY AND THE STATE'S OBLIGATION TO "COMPENSATE" FOR INFORMATION OPPORTUNITIES LOST BY A PERSON

Abstract. *The article deals with the problematic issues of applying restrictions on the right to information as a tool for deterring and counteracting threats to Ukraine's information security, neutralizing information aggression, creating an effective system of interaction between public authorities, local self-government bodies and society, and also developing international cooperation in the field of information security on the basis of partnership and mutual support; the use of which requires "compensation" for the information opportunities lost by a person, and which has not yet become the subject of*

Based on the analysis of recent studies and publications, the author has established the absence of a single mechanism for compensatory restriction of the right to information, and the attempts of Ukrainian courts and state bodies responsible for regulating information activities to develop their own ways and mechanisms for applying restrictions on the right to information with "the least losses" for information subjects, based primarily on their own practice of providing a legal assessment of each of such cases.

Given the relevance and significance of the issue, the purpose of the article is to present the results of the analysis of the content of restriction of the right to information as a means of ensuring information security and the State's obligation, and on this basis to formulate scientifically sound proposals for "compensation" for the information opportunities lost by an individual.

The author emphasizes the need for further analysis and formulation of a reasoned position with regard to each national security regime separately, and the possibility of applying mechanisms for restricting the right to information in the general practice of ensuring information security and special restrictive measures against information entities.

The author analyzes the practice of administrative courts in providing a legal assessment of the validity of recognizing information and other activities of a subject of information relations as unlawful, as well as a legal assessment of the actions of national security entities within the limits of their powers and the provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms.

The author suggests that further research on the issue of justification of certain restrictions on the right to information should be focused on the consideration of the public interest as a "compensator" for a certain restriction of the right to information and the application of the "three-part test" in the practice of applying restrictions.

Key words: *information security, right to information, restriction of the right to information, compensation, administrative court.*

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Здійснивши у 2010-2020 роках доктринальний перехід у тлумаченні «інформаційної безпеки» від «діяльності із запобігання нанесенню шкоди» [8] неповною невчасно отриманою та невірогідною інформацією (утвореного від цього негативного інформаційного впливу, застосування інформаційних технологій із негативними наслідками, несанкціонованого розповсюдження й використання інформації, порушення її цілісності, конфіденційності та доступності) до «посилення спроможностей держави, її інформаційного простору, підтримки інформаційними засобами та заходами

соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина» [10] сучасна правова наука утвердилася у необхідності окремого тлумачення її ролі у Стратегії національної безпеки та кожній з її сфер (інформаційна безпека сприймається як одна з них, що закріплено законодавчо у ст. 26, ч. 1, 3 ст. 27 Закону України «Про національну безпеку України» [7]), а також передбаченої ст. 31 Закону України «Про національну безпеку України» ролі для «...критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої вста-

новлена законом» [7]. При цьому інструментальна доцільність такого розподілу не стала досі предметом подальшої наукової дискусії із фіксацією лише у документах стратегічного планування організаційно-правових стримуючих заходів (кібероборони) та протидії інформаційній агресії, загрозам інформаційній безпеці України, нейтралізації, у тому числі спеціальних інформаційних операцій держави-агресора, інших дій, що спрямовані ним на підлив державного суверенітету й територіальної цілісності України (розвідувально-підливний діяльності у кіберпросторі та кібертероризму), забезпечення інформаційної стійкості суспільства та держави (окремих інформаційних систем та ресурсів), створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвитку міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки (зокрема у питаннях протидії кіберзлочинності, розвитку асиметричних інструментів стримування).

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття. У разі розгляду проблеми у більш вузькому, приватному її розумінні, науковий дискурс щодо «інформаційної безпеки» зміщує акценти з «безпеки інформації» на розширення її тлумачення до рівня, що вже «забезпечений» засобами кіберзахисту (сама інформація сприймається виключно «безпечною» – повною (достатньою), своєчасною (щодо її зібрання, отримання, зберігання), із високим ступенем вірогідності й достовірності, цілісності, конфіденційності та публічності (доступності щодо джерел)) тощо однак містить у собі реальні або потенційні загрози національній безпеці. За таких умов, вбачається, що право особи на інформацію в умовах мирного часу має буде реалізоване у повному обсязі, а будь-які спроби його обмеження не суб'єктами забезпечення національної безпеки зазнаватимуть відповідної «негативної» реакції держави, так як будуть протирічити державній інформаційній політиці.

При цьому врахуємо позицію В. Фурашева [14, с. 52], який ще на початку наведених розвідок (2012 рік) констатував переважаючий для подальшого формування її свідомості, підсвідомості та особистості вплив інформаційного масиву, в якому народилася особа. Окремо відзначимо його твердження, що «неповна,

невчасна, невірогідна або упереджена інформація, що використовується, у більшості випадків не завдає такої шкоди людині, що можна говорити про її небезпеку» [14, с. 52], а також твердження, щодо природнього стану сприйняття людиною інформації як «повної, своєчасної та вірогідної» [14, с. 52].

Розвиваючи ці, а також подібні твердження також припустимо, що, незалежно від стану розвитку суспільства, має місце створення, поширення, зберігання та використання інформації, яка, безумовно відповідаючи чинній суспільно-економічній формации, розвитку технологій комунікаційного обміну тощо, змістовно може бути спрямована на послаблення цього суспільства, держави (-в), певних територій, інститутів тощо. При цьому, як і у випадку із доктринальним плануванням майбутньої війни, що здійснюється на підставі досвіду попередніх воєн, нормативно-правове регулювання протидії шкідливій інформації, вже «відстає рівно на одну війну».

У сучасній науковій інформаційно-правовій літературі, присвяченій проблемі захисту прав людини, сформульовано чимало ідей, які стосуються проблематики інформаційної безпеки, а також обґрунтованих положень щодо засобів її забезпечення. Проте, вітчизняна й зарубіжна інформаційно-правові наукові школи не приділяли достатньої уваги розробці подібних за глибиною «обґрунтувань» для кожного з окремих випадків обмеження права на інформацію, рівно як й встановленню обов'язку держави «компенсувати» особі втрачені при забезпеченні інформаційної безпеки правові можливості. Це вказує на наявні та потенційні істотні прогалини у законодавстві України. Водночас, у 2019–2022 роках судова гілка влади, в особі адміністративних судів, неодноразово здійснювала спроби їх заповнення власними рішеннями.

З іншого боку, у суспільствознавчих та загально-наукових дослідженнях (Андрієнко О., Павленко К., Попович О. та інші), а також приватно-правових дослідженнях (Гаєвий В., Єфімов О., Краснова М., Куліцька С., Майстер І., Островерх А., Парінов А., Протченко С., Сонін О., Цимбалюк С. та інші) в якості предмету дослідження використовується формулювання «компенсації втрат». При цьому у працях з питань публічно-правового регулювання (Грищук О., Крикунов О., Нескороджена Л., Сіроткін М., Стебелев А., Бассуні Ш. та інші) вказане формулювання стає частиною формулювання предмета дослідження механізмів від-

шкодування (компенсації) шкоди від заборони чи навіть загального обмеження певного права.

Отже, як нами неодноразово наголошувалося, відсутні наукові розробки (окрім дослідження у 1998 році Л. Корчевною проблеми компенсації моральної шкоди, завданої порушенням особистих немайнових прав [1]) обґрунтування способів здійснення компенсування обмеження права на інформацію, яке виникло внаслідок здійснення заходів забезпечення національної (інформаційної) безпеки, захисту окремих інформаційних джерел тощо.

Формулювання мети статті (постановка завдання). Метою статті є викладення результатів проведеного аналізу змісту обмеження права на інформацію як засобу забезпечення інформаційної безпеки та обов'язку держави, формулювання пропозицій щодо «компенсації» втрачених особою інформаційних можливостей як науково обґрунтованих на цій основі.

Виклад основного матеріалу дослідження. В сучасній історії України є багато прикладів широкого тлумачення категорії «інформаційна безпека» та розширення за її допомогою обсягів заходів забезпечення національної безпеки, які ставилися, на доктринально-інструментальному рівні, «у залежність» від неї. Прикладом цього є віднесення окремих суб'єктів інформаційної діяльності та інших громадян, яким гарантовано право на інформацію до осіб, які перебувають під контролем іноземної юридичної особи чи фізичної особи-нерезидента, іноземців, осіб без громадянства, а також суб'єктів, які здійснюють терористичну діяльність (застосування санкцій – спеціальних економічних та інших обмежувальних заходів).

Відповідно, у змісті позовних вимог до держави та її органів, з якими, зокрема, звертаються такі особи до національних судів та ЄСПЛ, поставало питання як обґрунтованості таких рішень, так і «компенсації» обмеженого права. Прикладом останнього є рішення у справі, де позивач обґрунтовує свої вимоги порушенням його права як споживача аудіовізуальної інформації, а відповідач – наполягає на застосуванні «презумпції правомірності»: «... без необхідності здійснення обґрунтування своїх дій» [11], отже, не вбачає необхідності компенсування втрат. При цьому Велика Палата Верховного Суду підтверджуючи право позивача на «компенсацію» [4] не визнає, що його право на інформацію було порушено в оскаржуваному випадку через індивідуальний характер дії Указу Президента України.

На цьому прикладі можемо констатувати відсутність повноважень вчиняти дії, які спрямовані на обмеження права, у т.ч. керуючись завданнями забезпечення інформаційної безпеки, у жодної посадової особи незалежно від здійснення нею тлумачення важливості та суспільної користі від таких заходів. З іншого боку, Суд вимагає наводити обґрунтування такого обмеження відповідно до конструкції «обмеження не завдають більше шкоди особі ніж приносять користі безпеці». При цьому вбачається, що отримавши «обґрунтування» така особа й набуватиме компенсації її втрат від застосування такого обмеження.

Іншим прикладом є рішення у справі, де суд, посилаючись на недотримання самої процедури, як в частині рівня обґрунтованості встановлюваних обмежувальних заходів, так і в частині «компенсації» (проведення правової експертизи та складання відповідного рішення Комісією), урахував наявність окремих, обов'язкових як для суб'єктів забезпечення національної безпеки, обмежувально-компенсаційних процедур щодо суб'єктів інформаційної діяльності (засновників друкованих засобів масової інформації), які, у судовому порядку, зобов'язують суб'єкта інформаційної діяльності здійснювати певні дії [13], однак відмовив позивачеві у задоволенні його позову, залишивши таке рішення без зміни в апеляційній [5] та касаційній [3] інстанціях.

Відповідні механізми обґрунтування доступу широкого кола осіб до певної категорії інформації, рівно як і його обмеження, закріплено у Законі України «Про доступ до публічної інформації» (ч. 2 ст. 6). При цьому основною причиною такого виступив факт віднесення заходу до забезпечення національної (інформаційної) безпеки [6], а не вимога за якою завдані обмеженням втрати будуть компенсовані. На нашу думку, існує як можливість застосування таких механізмів щодо кожного режиму забезпечення національної безпеки окремо, так і широка практика такого обмеження права на інформацію в інтересах інформаційної безпеки. Зокрема, до неї слід віднести застосування спеціальних економічних та інших обмежувальних заходів до суб'єктів інформаційної діяльності.

При цьому вбачається, що в умовах новітніх режимів забезпечення національної безпеки, таких як воєнний стан, який діє сьогодні, а також під час відбудовного періоду після закінчення воєнних дій необхідно «розробити» окремі обґрунтування застосування кожного з них для подальшого їх застосування судами. Так, сучасна

практика адміністративних судів вже демонструє наявність такої необхідності коли Суд, надаючи правову оцінку дій Служби безпеки України чи інших суб'єктів забезпечення національної безпеки у межах наданих їм повноважень і положень ст. 10 Конвенції про захист прав людини і основоположних свобод, фактично з'ясовує наявність обґрунтування визнання інформаційної та іншої діяльності суб'єкта інформаційних відносин протиправною. Зауважимо, що він вимушений або керуватися «сталою» практикою мирного часу (звідси виникає проблематика некомпенсаційного обмеження права на інформацію в інтересах національної (інформаційної) безпеки, що пов'язана з відсутністю у Конвенції вимог, які, зокрема, перешкоджають державам здійснювати ліцензування (позбавлення ліцензії) та посилювати ліцензійні вимоги до такої діяльності), або формувати новітні рішення.

З іншого боку, Закон України «Про доступ до публічної інформації» [6], «компенсує» будь-які обмеження задоволенням суспільного інтересу до такої інформації. Так, Суд у рішенні у справі щодо «суспільного інтересу» [12], фактично встановив коло осіб – отримувачів такої «компенсації» (запитувачі, розпорядники інформації, структурний підрозділ або відповідальна особа з питань запитів на інформацію). Погодимося, що змістовно компенсація відображається у доступі до даних, які або свідчать про загрозу державному суверенітету, територіальній цілісності України, або забезпечують реалізацію конституційних прав особи, або вказують на «можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо» [2, с. 178].

«Компенсатор незабезпеченого суспільного інтересу», як необхідність, виділяється також Уповноваженою Верховної Ради України з прав людини, яка вказує, що 11% від усіх скарг, що надійшли до неї стосуються додержання права на доступ до публічної та суспільно важливої інформації [2, с. 4]. При цьому відмічається необхідність розпочати відповідний нормотворчий процес та вказується на необхідність дискусії навколо тлумачення «схиляння до надання інформації» саме як «компенсатора» ймовірного обмеження права на інформацію, про методику якого вказано, зокрема, у Рекомендаціях Уповноваженого Верховної Ради України з прав людини з питань додержання конституційного права людини і громадянина на доступ до інформації [2, с. 178].

Виходячи із цього, в аналізованому вище рішенні суду [12] розпорядник інформації був зобов'язаний обґрунтовувати обмеження у доступі згідно переліку підстав, які становлять зміст «трискладового тесту». Зокрема, згідно з позицією Суду, з відмови у доступі до публічної інформації повинно вбачатися: «якому з перелічених у п. 1 ч. 2 ст. 6 Закону України «Про доступ до публічної інформації» інтересів відповідає обмеження, а також чому обмеження доступу відповідає зазначеному інтересу (інтересам); у чому конкретно полягає шкода правомірному інтересу (інтересам); яким є причинно-наслідковий зв'язок між наданням доступу та можливим настанням шкоди; чому ця шкода є істотною; яка ймовірність настання шкоди внаслідок надання доступу до інформації; чому шкода від надання інформації переважає суспільний інтерес в її отриманні» [12]. Однак, констатуємо, що в своїх остаточних висновках Суд лише приймає рішення щодо обґрунтованості та не визначається з обов'язковістю компенсації втрачених інформаційних можливостей.

В іншому аналізованому рішенні [11] Верховний Суд звертав увагу на альтернативу отримання інформації аналогічної за змістом й значенням для користувача з інших джерел, що можна визнати компенсаційним механізмом, який супроводжує заходи забезпечення інформаційної безпеки, які, у свою чергу, проводяться із застосуванням «трискладового тесту». Також слід додати, що й Постанова Пленуму вищого адміністративного суду України від 29.09.2016 № 10 «Про практику застосування адміністративними судами законодавства про доступ до публічної інформації» [9] вимагає від розпорядників враховувати подібні вимоги.

Також вважаємо, що обмеження доступу до публічної інформації, заборона на поширення якої встановлена безпосередньо Законом, має відбуватися лише після застосування «трискладового тесту». Побічним аргументом цього є зазначене вище рішення [12], в якому «незастосування «трискладового тесту» під час обмеження доступу до інформації» призвело до визнання обмеження неправомірним. При цьому врахуємо, що така позиція зобов'язує встановити правовий статус відповідних «вtrat» як шкоди, що має бути компенсована.

У рішенні ЄСПЛ [15] наведено подібні міркування, однак застосовано й принцип «порівняння» визначених обсягів, який викладено у формулі: «права слід розуміти широко, а винятки чи обмеження (прав) – тлумачити

вузько» [15]. На нашу думку, такий підхід свідчить переважно про сприйняття «трискладового тесту» як основного засобу для обґрунтування не стільки самих механізмів обмеження права, скільки засобу обґрунтування обсягів компенсуючих заходів.

Отже, за позицією національних судів та ЄСПЛ, дії суб'єкта інформаційної безпеки як правозастосовувача мають бути спрямовані на захист певного охоронюваного законом інтересу (у т.ч. національного), а судів – на визначення «пропорційності» дій правозастосовувача як ненадмірності обмежувальних заходів забезпечення інформаційної безпеки із встановленням у кожному рішенні «балансу» між визначеним охоронюваним інтересом, ймовірністю шкоди (втрат) від інформаційної діяльності (реалізації та/або не реалізації права на інформацію), а також втратами особи від здійснюваних обмежувальних заходів. Побічно суди, обґрунтовуючи через пропорційність правомірність обмежень, мають відокремити інформацію (інформаційну діяльність), яка й становить фактичний зміст «інтересу» до неї, чим встановити для суб'єкта інформаційної безпеки «межі» його дій – визначити зміст інформації який для особи не меже «втратитися», а для суб'єкта інформаційної діяльності – вичерпний перелік видів такої діяльності, що не може піддаватися додатковому обмеженню через регулювання.

Реалізуючи власний обов'язок щодо «компенсації» втрачених особою інформаційних можливостей держава за допомогою категорії «суспільний інтерес до конкретної інформації» розширює обсяги правових можливостей у різних площинах, зокрема: надає можливість участі у публічній дискусії з актуальних питань чинного режиму забезпечення національної безпеки; надає тлумачення причин, які спонукали правозастосовувача (державний орган, орган місцевого самоврядування, його службова чи посадова особа) до обмежень; посилює прозорість процесу підготовки і прийняття рішень у сфері забезпечення інформаційної безпеки як підконтрольність влади суспільству загалом; надає можливість вторинного контролю за витрачанням бюджетних коштів та інших ресурсів держави на забезпечення інформаційної безпеки; нормативно визначає ризики завдання шкоди громадському здоров'ю, безпеці і порядку; створює умови запобігання їм та їх наслідкам; протидіє введенню суспільства в оману через розповсюдження неправдивої чи викривленої інформації, фейків тощо.

У випадках обмеження права на інформацію шляхом її віднесення до категорії обмеженого доступу дія компенсаційного механізму не має зазнавати змін та також має відповідати умовам пропорційності й вимог проходження «трискладового тесту» як «правового орієнтиру», про що, зокрема, вказував Суд в аналізованому вище рішенні [12]. Таким чином, у практиці правозастосування, «таємність» компенсується абстрактністю категорії відомостей, які конкретизуючись отримують статус «для службового користування».

Висновки. Чинне законодавство у сфері забезпечення інформаційної безпеки та правова теорія загалом вбачають можливим застосування в інтересах національної (інформаційної) безпеки обмеження права на інформацію, у т.ч. без додаткових умов та вимог обґрунтування такої можливості, що ставить відповідні заходи в один ряд з іншими заходами забезпечення національної безпеки, однак, фіксують й отримання суб'єктами інформаційної діяльності певної шкоди - «витрат», які слід «компенсувати» у загальному процесі як відшкодування шкоди майнового (немайнового) характеру, так і усунення перешкод у реалізації охоронюваного законом «інтересу».

Проаналізована судовою практикою щодо забезпечення громадського порядку та безпеки, національної безпеки та оборони України з 2019 року по теперішній час засвідчила напрацювання компенсаційних механізмів через оскарження актів, дій чи бездіяльності Верховної Ради України, Президента України, Вищої ради правосуддя, Вищої кваліфікаційної комісії суддів України, органів, які обирають (призначають), звільняють, оцінюють членів Вищої ради правосуддя, у межах якого «вимагалось» обґрунтування застосованого обмеження права на інформацію.

Від органів правозастосування, які виконують функції забезпечення інформаційної безпеки, Суд вимагає пропорційності регулювання інформаційної діяльності й обґрунтованості рішень щодо «найменших втрат» суб'єктів інформаційної діяльності дотриманням «трискладового тесту».

Подальші наукові розвідки проблеми обов'язку держави щодо «компенсації» втрачених особою інформаційних можливостей доцільно спрямувати на розробку окремих засобів «трискладового тесту», зокрема в аспекті обрання органом правозастосування засобу, який забезпечить як мінімальність «втрат» від обмеження права на інформацію, так і належну його правову оцінку Судом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Корчевна Л. О. Компенсація моральної шкоди, завданої порушенням особистих немайнових прав, у цивільному праві України : автореф. дис. ... канд. юрид. наук : 12.00.03 ; Університет внутрішніх справ. Х., 1998. 24 с.
2. Олексіюк Т., Опришко Л., Буртник Х., Барвіцький В., Кабанов О. Рекомендації Уповноваженого Верховної Ради України з прав людини з питань додержання конституційного права людини і громадянина на доступ до інформації. Strasbourg CEDEX. 2020. 336с. URL:<https://rm.coe.int/recommendations-final-10-02-21/1680a165f7>
3. Постанова Верховного Суду у складі колегії суддів Касаційного адміністративного суду від 21 жовтня 2021 року у справі № 520/118/20 URL: <https://reyestr.court.gov.ua/Review/100471040>
4. Постанова Верховного Суду у справі № 9901/26/21 від 06 жовтня 2021 року. URL: <https://reyestr.court.gov.ua/Review/101424457>
5. Постанова Другого апеляційного адміністративного суду від 07 липня 2020 року у справі № 520/118/20. URL:<https://reyestr.court.gov.ua/Review/90234393>
6. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17>.
7. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL:<https://zakon.rada.gov.ua/laws/show/2469-19#n111>
8. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.07 р. № 537-V. Відомості Верховної Ради України. 2007. № 12. Ст.102.
9. Про практику застосування адміністративними судами законодавства про доступ до публічної інформації : Постанова Пленуму Вищого адміністративного суду України від 29 вересня 2016 року № 10.
10. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
11. Рішення Верховного Суду у складі колегії суддів Касаційного адміністративного суду від 26 квітня 2021 року у справі № 9901/22/21. URL: <https://reyestr.court.gov.ua/Review/96591995>
12. Рішення Львівського окружного адміністративного суду від 06 травня 2020 року у справі № 380/2525/20. URL: <https://zakononline.com.ua/court-decisions/show/89248574>
13. Рішення Харківського окружного адміністративного суду від 10 березня 2020 року у справі № 520/118/20. URL: <https://reyestr.court.gov.ua/Review/88173959>
14. Фурашев В. М. Сутність та визначення поняття «інформаційна безпека» і «безпека інформації». *Правова інформатика*, 2012. № 2(34). С. 51–59. URL:<https://ippi.org.ua/sites/default/files/12fvmbbi.pdf>
15. Brian Leonard FRIEND v the United Kingdom 16072/06 (2009) ECHR 2068 (24 November 2009). URL: <http://www.bailii.org/eu/cases/ECHR/2009/2068.html>

REFERENCES:

1. Korchevna, L. (1998). Compensation for Non-Pecuniary Damage Caused by Violation of Personal Non-Property Rights in the Civil Law of Ukraine [Kompensazia moralnoi shkodi, zavdanoi porucheniam osobistick nemaimovick prav, u zivilnomu pravi Ukraini]. Thesis abstract of the candidate of legal sciences – Avtoreferat disertazii kandidata uridichnick nauk: 12.00.03 ; University of Internal Affairs. Kharkiv., 24 p. [in Ukrainian]
2. Oleksiyuk, T., Opryshko, L., Burtnyk, H., Barvitsky, V., Kabanov, O. (2020). Recommendations of the Ukrainian Parliament Commissioner for Human Rights on the observance of the constitutional right of a person and citizen to access to information [Rekomendazii Upovnovagenogo Verckovnoi Radi Ukraini z prav ludini z pitan doderjania konstituziinogo prava ludini i gromadianina na dostup do informazii]. Strasbourg CEDEX. 336p. Retrieved from: <https://rm.coe.int/recommendations-final-10-02-21/1680a165f7>. [in Ukrainian]
3. Resolution of the Supreme Court as part of the panel of judges of the Administrative Court of Cassation of October 21, 2021 in case No. 520/118/20. [Postanova Verckovnogo Sudu u skladi suddiv Kasaziynogo administrativnogo sudu vid 21 jovntnia 2021 roku u spravi № 520/118/20]. Retrieved from: <https://reyestr.court.gov.ua/Review/100471040>
4. Resolution of the Supreme Court in case No. 9901/26/21 of October 06, 2021 [Postanova Verckovnogo Sudu u spravi № 9901/26/21 vid 06 jovntnia 2021 roku]. Retrieved from: <https://reyestr.court.gov.ua/Review/101424457>
5. Resolution of the Second Administrative Court of Appeal of July 07, 2020 in case No. 520/118/20 [Postanova Drugogo apeliazijnogo sudu vid 07 lipnia 2020 roku u spravi № 520/118/20]. Retrieved from: <https://reyestr.court.gov.ua/Review/90234393>
6. On access to public information [Pro dustup do publicnoi informazii]. Law of Ukraine of January 13, 2011, No. 2939-VI. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2939-17>.
7. On the national security of Ukraine. [Pro nationalnu bezpeku Ukraini], Law of Ukraine No. 2469-VIII (2018) (Ukraine). Retrieved from: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
8. On the Basic Principles of Information Society Development in Ukraine for 2007-2015 [Pro osnovni zasady rozvitku informaziynogo suspilstva v Ukraini na 2007-2015 roki], Law of Ukraine No. 537-V (2007) (Ukraine). Retrieved from: <https://zakon.rada.gov.ua/laws/show/537-16#Text>
9. On the practice of application of legislation on access to public information by administrative

- courts [Pro praktiku zastosuvania administrativnimi sudami zakonodavstva pro dostup do publichnoi informazii]: Resolution of the Plenum of the Higher Administrative Court of Ukraine of September 29, 2016, No. 10.
10. On the Decision of the National Security and Defense Council of Ukraine of October 15, 2021 “On the Information Security Strategy” [Pro richennya Rady nazionalnoi bezpeki i oboroni Ukraini vid 15 jovtnia 2021 roku “Pro Strategiu informazynoy bezpeki Ukraini”], Decree of the President of Ukraine No. 685/2021 (2021) (Ukraine). Retrieved from: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
 11. Decision of the Supreme Court composed of the panel of judges of the Administrative Court of Cassation dated April 26, 2021 in case 9901/22/21 [Richenia Verckovnogo Sudu u skladi suddiv Kasaziynogo administrativnogo sudu vid 26 kvitnia 2021 roku u spravi 9901/22/21]. Retrieved from: <https://reyestr.court.gov.ua/Review/96591995>
 12. Decision of the Lviv District Administrative Court of May 06, 2020 in case No. 380/2525/20 [Richenia Lvivskogo okrujnogo administrativnogo sudu vid 06 travnia 2020 roku u spravi № 380/2525/20]. Retrieved from: <https://zakononline.com.ua/court-decisions/show/89248574>
 13. Decision of the Kharkiv District Administrative Court of March 10, 2020 in case No. 520/118/20 [Richenia Kharkivskogo okrujnogo administrativnogo sudu vid 10 bereznia 2020 roku u spravi № 520/118/20]. Retrieved from: <https://reyestr.court.gov.ua/Review/88173959>
 14. Furashev, V. (2012). The essence and definition of the concepts of “information security” and “information security” [Sutnist ta viznachennia poniat “informaziynaia bezpeka” i “bezpeka informazii”]. *Legal Informatics – Pravova informatika*, 51–53. Retrieved from: <https://ippi.org.ua/sites/default/files/12fvmbbi.pdf>. [in Ukrainian]
 15. Brian Leonard FRIEND v the United Kingdom 16072/06 (2009) ECHR 2068 (24 November 2009). Retrieved from: <http://www.bailii.org/eu/cases/ECHR/2009/2068.html>. [in English].

Дата надходження статті: 20.06.2025

Дата прийняття статті: 20.07.2025

Опубліковано: 10.10.2025