

УДК 342.7

DOI <https://doi.org/10.32782/ln.2024.23.72>**Мазепа С.О.**

*кандидат юридичних наук, доцент,
доцент кафедри кримінального права та
процесу
Західноукраїнського національного
університету,
міжнародний дослідник
Оснабрюцького університету
ORCID ID: 0000-0003-1282-9089*

АДМІНІСТРАТИВНО-ПРАВОВІ ІНСТРУМЕНТИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Вступ. У сучасних умовах питання забезпечення інформаційної безпеки в Україні є надзвичайно важливим, що в першу чергу пов'язано з необхідністю протидіяти незаконним втручанням в інформаційний простір України, зберегти інформаційні ресурси, захистити населення від негативного інформаційного впливу інших держав, певних політичних сил і суспільних груп тощо. Крім того, європейська інтеграція є стратегічно визначним пріоритетом зовнішньої політики України, оскільки вимагає вдосконалення правової та регуляторної бази інформаційної безпеки України, яка відповідала б не тільки міжнародним стандартам, а й, перш за все, національним інтересам України в інформаційній сфері. Ці положення відображені в Стратегії інформаційної безпеки України, оскільки в ній визначено, з якими актуальними викликами та загрозами стикається національна безпека України в інформаційній сфері, які стратегічні цілі існують для боротьби з цими загрозами, як захищаються права людини та персональні дані [1].

Положення цього документа визначають, що метою стратегії є зміцнення спроможності забезпечувати інформаційну безпеку держави та її інформаційного простору, підтримка соціальної та політичної стабільності за допомогою інформаційних засобів і заходів, обо-

рона країни, захист державного суверенітету, територіальної цілісності України, демократичного конституційного ладу та забезпечення прав і свобод усіх громадян.

Крім того, у Стратегії названо основні глобальні загрози інформаційній безпеці держави: зростання кількості глобальних дезінформаційних кампаній; інформаційна політика Російської Федерації, яка загрожує не тільки Україні, а й іншим демократичним державам; ступінь впливу соціальних мереж на інформаційний простір; брак медіакомпетентності (медіакультури) в умовах стрімкого розвитку цифрових технологій. Незважаючи на зовнішні загрози, існують також внутрішні виклики та загрози, такі як: обмежена здатність реагувати на дезінформаційні кампанії; неповна система стратегічних комунікацій; необхідність регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів; спроби маніпулювання громадянами України щодо європейської та євроатлантичної інтеграції України; доступ до інформації на місцевому рівні; недостатній рівень інформаційної грамотності. Окрім викликів, безпосередньо згаданих у Стратегії, недосконалість українського законодавства в інформаційній сфері та його невідповідність сучасним вимогам є ще одним викликом для українського суспіль-

ства. Для реалізації цієї стратегії уряду було доручено вдосконалити правове та регуляторне поле шляхом систематичного перегляду та внесення змін до відповідних законодавчих та інших нормативно-правових актів у сфері інформації.

Метою статті є з'ясування особливостей та проблем забезпечення інформаційної безпеки, зокрема, висвітлення особливостей адміністративної відповідальності за правопорушення в інформаційній сфері, виявлення недоліків та визначення перспектив.

1. Щодо питання визначення понять інформаційна безпека, інформаційна сфера та інформаційне правопорушення, та їх адаптації до сучасних викликів інформаційної безпеки

Існує багато наукових досліджень, присвячених забезпеченню інформаційної безпеки в Україні, значна частина з яких присвячена розвитку в галузі права. Особливо важливо згадати деяких вчених, роботи яких були проаналізовані під час підготовки цієї статті. Наприклад, Белевцева описує деякі особливості правового регулювання інформаційних ресурсів [2]. Автор вказує на деякі недоліки в сфері інформаційної безпеки, зокрема на неповну розробку правової бази, яка забезпечує правове регулювання даної сфери. Перун у своїй роботі показує особливості адміністративного та правового механізму забезпечення інформаційної безпеки в Україні [3]. У рамках дослідження особливостей та проблем правового регулювання у сфері інформаційної безпеки в Україні було доцільно розглянути оприлюднені питання. Турчак комплексно розглядає механізми інформаційної безпеки України як складову державної безпеки України [4]. Зрозуміло, що інформаційна безпека передбачає не тільки захист інформації від несанкціонованого доступу, але й, перш за все, запобігання несанкціонованому доступу, використанню, розкриттю, зміні, перевірці, запису або знищенню інформації. Отже, інформаційна безпека охоплює дуже багато сфер застосування, таких як криптографія,

комп'ютери, кіберкриміналістика, соціальні онлайн-медіа тощо.

Борисов зазначає, що національна законодавча система чітко не визначає ані цілі та актуальні завдання інформаційної безпеки України, ані компетенції в цій сфері та засоби правового регулювання, які б забезпечували адекватний та збалансований правовий вплив на відповідні правовідносини [5]. Водночас автор вказує на важливість і необхідність належного законодавчого забезпечення при формуванні правової системи та забезпеченні функціонування механізму правового регулювання інформаційної безпеки. Відповідно, автор зазначає, що створення належного правового поля інформаційної безпеки в Україні є важливою передумовою та пріоритетним кроком для впровадження ефективного правового регулювання забезпечення інформаційної безпеки в Україні.

У повсякденному спілкуванні та в засобах масової інформації часто зустрічаються такі поняття, як інформаційний простір, інформаційна інфраструктура, інформаційна сфера, інформаційна діяльність, інформаційний потенціал, інформаційна реальність, інформаційна дійсність, сфера інформатизації, інфосфера і навіть кіберпростір, кіберсфера та подібні, які для пересічного громадянина фактично є синонімами і відображають соціальні процеси, пов'язані з обміном інформацією та інформатизацією. Логічно було б розпочати аналіз з категорії, яка тим чи іншим чином здатна об'єднати поширені в інформаційному праві поняття та охопити суть предмета правового регулювання інформаційних відносин, враховуючи теоретичні та методологічні передумови для визначення поняття «інформаційна сфера». Визначення інформаційної сфери широко поширене як у загальному мовленні, так і в медійній риторичі, науковій термінології, законодавчих актах тощо. Однак слід зазначити, що на сьогодні не існує єдиного тлумачення цього поняття.

Загальноновизнано, що діяльність, пов'язана з інформацією та інформаційними процесами,

регулюється нормами інформаційного права. Отже, логічно, що систематичне та глибоке дослідження теоретичних і методологічних основ інформаційного права, його наукових проблем у різних напрямках та відповідності інформаційного законодавства сучасним суспільним вимогам є однією з найважливіших передумов успішного формування інформаційної сфери та правового забезпечення цього процесу. Для опису різних концепцій, що представляють сферу інформації, у науковій літературі при дослідженнях у різних галузях знань і діяльності зазвичай використовуються такі терміни: інформаційний простір, інформаційне поле, інформаційна сфера.

Однак на даний момент, незважаючи на широке використання терміна «інформаційний простір», існує кілька інших визначень поняття інформаційного простору. «Інформаційна сфера – це сфера обміну інформацією (виробництво – розподіл – споживання), в якій суб'єкти реалізують свої потреби та можливості щодо інформації» – таке визначення запропонували відомі дослідники в галузі інформаційного права Бачіло, Лопатін та Федотов. І якщо саме визначення є досить загальним, то воно уточнюється подальшими поясненнями авторів. Отже, до основних об'єктів інформаційної сфери належать: інформація, включаючи інформаційні ресурси, що зберігаються на відповідних носіях інформації, а також інформаційна інфраструктура, що охоплює декілька інформаційних систем: організаційні структури, інформаційно-телекомунікаційні структури, інформаційні, комп'ютерні та телекомунікаційні технології, медіасистеми.

Зрозуміло, що перелічений авторами перелік елементів інформаційної інфраструктури далеко не повний. Важливою складовою цього комплексу правил є інформаційне право. Однак найбільшим недоліком цього визначення є те, що воно замінюється іншим поняттям – «сфера», визначення якого не наводиться. Слід погодитися з визначенням

Арістової [6], яка в своєму тлумаченні підкреслює особливість інформаційної сфери як сфери, в якій здійснюється інформаційна діяльність (збір, виробництво, зберігання, використання, поширення інформації), та відповідні види діяльності, що забезпечують інформаційну діяльність. Подібну наукову точку зору представляє Беляков [7], який стверджує, що інформаційне середовище можна визначити як сукупність інформаційних ресурсів у поєднанні із засобами, методами та умовами, що забезпечують їх активацію та активне використання. Ряд науковців визначили, що інформаційна сфера складається з сукупності інформації та інформаційної інфраструктури суспільства, а також соціальних відносин, предметом яких є інформація та інформаційна інфраструктура. Це визначення пізніше було уточнене як інформаційне середовище у сукупності таких елементів: 1) суб'єктів інформаційної взаємодії або впливу; 2) сама інформація, призначена для використання суб'єктами інформаційної сфери; 3) інформаційна інфраструктура, що забезпечує обмін інформацією між суб'єктами; 4) соціальні відносини, що виникають у зв'язку з утворенням, передачею, розповсюдженням і збереженням інформації.

І в кожному випадку в визначеннях або виключається інформаційна інфраструктура або інформаційні ресурси з моделі інформаційної сфери, або не охоплюються всі етапи інформаційного обміну, або не враховується питання регулювання інформаційної діяльності. Особливу увагу слід звернути на тлумачення поняття, сформульоване у спільній монографії «Правова відповідальність за злочини в інформаційній сфері та основи інформаційної деліктології: монографія»: «Інформаційна сфера – це сукупність інформаційних ресурсів, інформаційної інфраструктури, суб'єктів, які здійснюють інформаційний обмін, тобто їх створення, розповсюдження (передачу), зберігання, використання та знищення, і забезпечують цей обмін, що виникають з цього соціальних відносин, системи

правового забезпечення, а також інституційної системи державного управління цим середовищем». Водночас можна підтримати думку А. Селезньової про те, що інформаційна сфера тісно пов'язана з іншими сферами суспільної діяльності, але водночас характеризується галузевою приналежністю, що визначає її автономність щодо інших сфер [8].

Складність інформаційного права та міжгалузевий зміст існуючого інформаційного законодавства вимагають глибокого дослідження аналізу інституту правової відповідальності за правопорушення в інформаційній сфері з метою забезпечення інформаційної безпеки особи, держави та суспільства шляхом вдосконалення механізму регулювання соціальних відносин, що виникають у процесі інформаційної діяльності (інформаційних відносин), що має ключове значення для розвитку інформаційного права.

2. Адміністративна відповідальність як інструмент забезпечення інформаційної безпеки: концепція, особливості, ефективність застосування

Серед правових інструментів забезпечення інформаційної безпеки та боротьби з інформаційними правопорушеннями адміністративна відповідальність займає центральне місце в системі заходів захисту соціальних відносин в інформаційній сфері, оскільки норми адміністративної відповідальності спрямовані на запобігання та припинення протиправних втручань у правовідносини, що охороняються законом.

Водночас, як справедливо зазначає Перун, законодавство про адміністративну відповідальність «не встигає» за стрімкими процесами розвитку інформаційного суспільства, що негативно позначається на стані правопорядку в суспільстві та вимагає подальшого наукового розвитку [3]. Вищезазначений автор проаналізував усі адміністративні правопорушення у сфері інформаційної безпеки, що містяться в Кодексі України про адміністративні правопорушення (далі – КпАПУ), та розділив їх на три групи, а саме: 1) забез-

печення доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; 2) забезпечення обмеження доступу до певної інформації, поширення якої може негативно вплинути на права і свободи громадян, законну діяльність юридичних осіб або національну безпеку; 3) забезпечення безпеки в сфері медіаінформації. Автор також зазначає, що нормативно-правове забезпечення адміністративної відповідальності у сфері інформаційної безпеки є недостатнім для охоплення сукупності соціальних відносин в інформаційній сфері, зокрема, норми Кодексу про адміністративні правопорушення не регулюють питання визначення відповідальності за зміст і якість медіа-контенту телерадіоорганізацій [11].

Інший науковець, Волкова, аналізуючи законодавство, що встановлює адміністративну відповідальність за правопорушення в інформаційній сфері, та матеріалів практики розгляду справ про такого роду правопорушення дійшла висновку, що існують певні прогалини в адміністративно-правовому регулюванні відносин у сфері забезпечення інформаційних прав і свобод, що створює перешкоди для притягнення до відповідальності, а також для виявлення та запобігання такого роду правопорушенням [10]. Можна поділити думку автора, що законодавство про адміністративні правопорушення досі не містить повного переліку законів, які передбачають адміністративну відповідальність за правопорушення у сфері інформації. Кодекс України про адміністративні правопорушення побудований таким чином, що більшість елементів інформаційних правопорушень містяться в різних розділах Кодексу, що значно ускладнює захист правових відносин у сфері інформації. Відповідно до вищезазначених пропозицій, доцільним вважається введення до Кодексу окремого розділу про боротьбу з відмиванням грошей, в якому будуть регулюватися всі адміністративні правопорушення у сфері інформації. Ми пропонуємо,

наприклад, об'єднати низку правопорушень у сфері інформації в єдиному розділі під назвою «Адміністративні правопорушення у сфері інформації», який може містити такі правопорушення:

- ненадання інформації для проведення колективних переговорів та контролю за виконанням колективних договорів (ст. 41-3);
- використання засобів комунікації в цілях, що суперечать інтересам держави, порушують громадський порядок та ображають честь і гідність громадян (ст. 148-3);
- приховування інформації про діяльність емітента (ст. 163-5);
- незаконне використання інсайдерської інформації (ст. 163-9);
- порушення процедури внесення змін до системи зберігання документів про цінні папери (ст. 163-10);
- порушення процедури розкриття інформації на фондовій біржі (ст. 163-11);
- недобросовісна конкуренція (ст. 164-3);
- поширення неправдивих чуток (ст. 173-1);
- розголошення інформації про заходи безпеки щодо особи, яка перебуває під охороною (ст. 185-11);
- невиконання законних вимог посадових осіб Державної служби спеціального зв'язку та інформаційної безпеки України (ст. 188-31);
- порушення законодавства у сфері захисту персональних даних (ст. 188-39)
- невиконання законних вимог посадових осіб спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних (ст. 188-40)
- порушення закону про державну таємницю (ст. 212-2)
- порушення права на інформацію (ст. 212-3);
- порушення порядку реєстрації, зберігання та використання документів та інших носіїв інформації, що містять конфіденційну інформацію, яка є власністю держави (ст. 212-5);
- незаконний доступ до інформації в (автоматизованих) інформаційних системах, незаконне виготовлення або розповсюдження

копій баз даних (автоматизованих) інформаційних систем (ст. 212-6) та ряд інших злочинів у сфері інформації [11].

Ще однією проблемою у сфері інформаційної безпеки людини є недостатній захист персональних даних та неефективність органу, уповноваженого контролювати захист персональних даних. Особливе занепокоєння викликає ситуація щодо положень українського законодавства, що регулюють відповідальність за порушення норм захисту персональних даних. Наразі в українському законодавстві не повністю визначено поняття «захист персональних даних», критерії, яким повинен відповідати такий захист, та вимоги до власника і адміністратора щодо визначення рівня захисту; фактичні підстави відповідальності за порушення при обробці персональних даних є нечіткими. Слід також зазначити, що виключно адміністративні санкції як засіб покарання за порушення норм щодо захисту персональних даних є недостатніми; інституційна система переслідування порушень законодавства про захист персональних даних, яка наразі здійснюється Секретаріатом Уповноваженого з прав людини «Верховної Ради» (Верховної Ради) України, є недостатньо ефективною. Однак ми пропонуємо запровадити окремий орган або посаду для захисту персональних даних – інформаційного, можливо, уповноваженого з питань захисту даних. Також, країна потребує окремого закону про медіа, де центральними мають бути питання регулювання, нагляду та відповідальності.

Висновки.

Підсумовуючи, можна сказати, що інститут адміністративної відповідальності за правопорушення в інформаційній сфері не є належним інструментом забезпечення інформаційної безпеки в Україні і все ще перебуває на стадії становлення. Ми також вважаємо за необхідне законодавчо врегулювати поняття «інформаційна сфера» та «правопорушення в інформаційній сфері» та, з метою раціоналізації правового регулювання адміністративної відповідальності, об'єднати всі правопору-

шення в інформаційній сфері в окрему главу Закону про адміністративні правопорушення в КпАП. Особливе занепокоєння викликає ситуація щодо положень українського законодавства, що регулюють відповідальність за порушення норм захисту персональних даних. Наразі в українському законодавстві не повністю визначено поняття «захист персональних даних», критерії, яким повинен відповідати такий захист, та вимоги до власника і адміністратора щодо визначення рівня захисту; фактичні підстави відповідальності за порушення при обробці персональних даних є нечіткими. Слід також зазначити, що виключно адміністративні санкції як засіб

покарання за порушення норм щодо захисту персональних даних є недостатніми; інституційна система переслідування порушень законодавства про захист персональних даних, яка наразі здійснюється Секретаріатом Уповноваженого з прав людини «Верховної Ради» (Верховної Ради) України, є недостатньо ефективною. Однак ми пропонуємо запровадити окремий орган або посаду для захисту персональних даних – інформаційного, можливо, уповноваженого з питань захисту даних. Також, країна потребує окремого закону про медіа, де центральними мають бути питання регулювання, нагляду та відповідальності.

Анотація

У статті проаналізовано сучасні наукові підходи до розуміння змісту інформаційного права та запропоновано авторське бачення ролі адміністративно-правових інструментів у протидії гібридним загрозам в інформаційній сфері. Особливу увагу приділено оцінці ефективності адміністративної відповідальності як одного з ключових механізмів забезпечення інформаційної безпеки держави. Висвітлено проблемні аспекти чинного законодавства, зокрема нечіткість правового визначення понять «інформаційна сфера» та «правопорушення в інформаційній сфері», що ускладнює належну кваліфікацію правопорушень і послаблює превентивну функцію права. Автор наголошує, що інститут адміністративної відповідальності за правопорушення в інформаційній сфері перебуває на етапі становлення та вимагає комплексного перегляду. З метою підвищення ефективності правового регулювання пропонується кодифікувати норми про відповідальність за інформаційні правопорушення в окремій главі КУпАП, що сприятиме узгодженості правозастосування та забезпеченню належного реагування на кіберінциденти, дезінформацію й інші прояви гібридної агресії.

Наразі в українському законодавстві не повністю визначено поняття «захист персональних даних», критерії, яким повинен відповідати такий захист, та вимоги до власника і адміністратора щодо визначення рівня захисту; фактичні підстави відповідальності за порушення при обробці персональних даних є нечіткими. Слід також зазначити, що виключно адміністративні санкції як засіб покарання за порушення норм щодо захисту персональних даних є недостатніми; інституційна система переслідування порушень законодавства про захист персональних даних, яка наразі здійснюється Секретаріатом Уповноваженого з прав людини Верховної Ради України, є недостатньо ефективною. Однак ми пропонуємо запровадити окремий орган або посаду для захисту персональних даних – інформаційного, можливо, уповноваженого з питань захисту даних. Також, країна потребує окремого закону про медіа, де центральними мають бути питання регулювання, нагляду та відповідальності.

Ключові слова: інформаційна безпека, юридична відповідальність, інформаційні правопорушення, адміністративно-правовий аспект, кібербезпека.

Summary

The article analyzes contemporary scholarly approaches to the development of information law and offers an original assessment of the effectiveness of administrative-legal instruments in countering hybrid threats in the information sphere. Particular attention is paid to evaluating the role of administrative liability as a key mechanism for ensuring national information security. The study highlights the deficiencies of the current legal framework, especially the lack of clear definitions for the concepts of “information sphere” and “information-related offenses,” which hampers proper legal qualification and weakens the preventive function of administrative law. The author emphasizes that the institution of administrative liability for offenses in the information domain remains underdeveloped and requires a comprehensive reform. In order to enhance the efficiency and coherence of legal regulation, it is proposed to codify administrative liability for information-related offenses within a separate chapter of the Code of Ukraine on Administrative Offenses. Such codification would contribute to the consistency of law enforcement practices and provide an adequate legal response to cyber incidents, disinformation, and other manifestations of hybrid aggression.

Currently, Ukrainian legislation does not provide a comprehensive definition of «personal data protection,» nor does it establish clear criteria that such protection must meet or requirements for data controllers and processors regarding the determination of protection levels. The legal grounds for liability in cases of violations during personal data processing remain vague and insufficiently defined. It should also be noted that relying solely on administrative sanctions as a punitive measure for breaches of personal data protection norms is inadequate. The institutional framework for enforcing personal data protection legislation – currently managed by the Secretariat of the Ukrainian Parliament Commissioner for Human Rights – is not sufficiently effective.

We therefore propose the establishment of a dedicated authority or position responsible for personal data protection – potentially an Information Commissioner or a Data Protection Commissioner. Additionally, the country requires a distinct Media Law, with a strong emphasis on regulation, oversight, and accountability as central components.

Key words: information security, legal liability, information-related offenses, administrative and legal framework, cybersecurity.

Список використаних джерел:

1. Стратегія інформаційної безпеки : Указ Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n7> (дата звернення: 15.01.2022).
2. Белєвцева В. В. Правовий режим інформаційних ресурсів. Інформація і право. 2011. №. 3. С. 41-46.
3. Перун Т. С. Адміністративна відповідальність у системі заходів забезпечення інформаційної безпеки. IT-право: проблеми і перспективи розвитку в Україні (Друга міжнародна щорічна конференція). URL: <http://aphd.ua/publication-358> (дата звернення: 19.01.2022).
4. What is Information Security? URL: <https://www.geeksforgeeks.org/what-is-information-security> (дата звернення: 19.01.2022).
5. Борисов О. Особливості правового режиму забезпечення інформаційної безпеки України, зумовлені Конституцією України. Інформація і право. 2021. №. 3 (38). С. 155-161.
6. Аристова І. В., Чернадчук В. Д. Концепція інформаційних правовідносин: сутність і особливості використання у сфері банківської діяльності. Інформація і право. 2012. № 3. С. 47–57.
7. Беляков К. І. Інформатизація в Україні: проблеми організаційного, правового і наукового забезпечення : монографія. Київ : КВІЦ, 2008. 576 с.
8. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформа-

ційної деліктології : монографія / І. В. Аристова, А. А. Баранов, О. П. Дзобань та ін. ; за заг. ред. проф. К. І. Беякова. Київ : КВІЦ, 2019. 23 с.

9. Правдюк, С. А. Класифікація інформаційних правопорушень. № 4 (2013), Аналітично-порівняльне право. с. 209–211.
10. Волкова, А. Особливості юридичної відповідальності за правопорушення в інформаційній сфері. Правова інформатика. 2014. №. 1. С. 72-80.
11. Кодекс України про адміністративні правопорушення: Закон України від 18 грудня 1984 р. № 8073-X (на підставі – 1965-IX). URL: <https://zakon.rada.gov.ua/laws/show/80731-10?lang=en#Text> (дата звернення: 14 січня 2022).