

УДК 342.7

DOI <https://doi.org/10.24144/2788-6018.2025.04.3.72>

ІНФОРМАЦІЙНЕ ПРАВОПОРУШЕННЯ: ДО ПИТАННЯ ФОРМАЛІЗАЦІЇ ПРАВОВОЇ КАТЕГОРІЇ

Мазепа С.,

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

Мазепа С. Інформаційне правопорушення: до питання формалізації правової категорії.

Вказується, у законодавстві вже існує поняття кіберзлочину та комп'ютерного правопорушення, які охоплюють цифрову специфіку: обробку персональних даних; кібератаки; втручання в роботу систем; розповсюдження фейків або deepfake. Проте ці категорії не включають специфіку і характер інформації, з якою вчиняються діяння.

Стаття присвячена теоретико-правовому аналізу феномену інформаційного правопорушення, що в умовах цифрової трансформації суспільства набуває все більшої актуальності. У роботі розкрито передумови формування нової юридичної категорії – «інформаційне правопорушення» – як комплексного явища, що охоплює широкий спектр протиправних діянь, пов'язаних із створенням, обробкою, передачею, зберіганням, зміною або знищенням інформації незалежно від її форми. Авторка досліджує розвиток міжнародного та національного законодавства у сфері кібербезпеки, інформаційних технологій та захисту персональних даних, зокрема аналізує положення Будапештської конвенції про кіберзлочинність, імплементацію її норм у Кримінальний кодекс України, а також зміст інших законодавчих актів, що формують основу інформаційного законодавства. Окрему увагу приділено сучасним викликам, зумовленим використанням штучного інтелекту у сфері правозастосування, а також загрозам, що виникають у зв'язку з цим – порушенням права на приватність, витоку персональних даних, зниженню рівня довіри до правоохоронних органів. У статті запропоновано авторське бачення структури інформаційного правопорушення, визначено його об'єктивні та суб'єктивні ознаки, охарактеризовано його об'єкт як сукупність суспільних інформаційних відносин, що охороняються законом. Наголошено на міжгалузевому характері інформаційного права як підґрунтя для формування ефективної правової політики у сфері інформаційної безпеки. Запропоноване визначення інформаційного правопорушення покликане слугувати підґрунтям для подальших наукових досліджень та удосконалення правового регулювання у зазначеній сфері.

У статті автор розмірковує над доцільністю виокремлення інформаційної відповідальності як самостійного правового явища, що формується на перетині класичних галузей права, але має власні підстави, механізми впливу та форми реалізації в умовах цифрової трансформації суспільства.

Ключові слова: інформаційне правопорушення, інформаційна безпека, штучний інтелект, інформаційне законодавство, кіберзлочини, юридична відповідальність.

Mazepa S. Information offense: on the issue of formalization of the legal category.

It is indicated that the legislation already includes the concepts of cybercrime and computer offense, which cover digital specifics: processing of personal data; cyberattacks; interference with the operation of systems; distribution of fakes or deepfake. However, these categories do not include the specifics and nature of the information with which the acts are committed.

The article is devoted to the theoretical and legal analysis of the phenomenon of information offence, which is gaining increasing relevance in the context of digital transformation of society. The study reveals the prerequisites for the formation of a new legal category – “information offence” – as a complex phenomenon encompassing a wide range of unlawful acts related to the creation, processing, transmission, storage, or destruction of information, regardless of its form. The author explores the development of international and national legislation in the fields of cybersecurity, information technologies, and personal data protection, in particular by analyzing the provisions of the Budapest Convention on Cybercrime, its implementation in the Criminal Code of Ukraine, and other legislative acts that constitute the foundation of information law. Special attention is paid to the contemporary challenges posed by the use of artificial intelligence in law enforcement, as well as the threats arising

from it – including violations of privacy rights, data breaches, and a decline in public trust towards law enforcement authorities. The article offers the author's vision of the structure of an information offence, identifies its objective and subjective elements, and defines its object as the totality of legally protected social relations involving information. Emphasis is placed on the interdisciplinary nature of information law as the basis for shaping effective legal policy in the field of information security. The proposed definition of information offence is intended to serve as a foundation for further academic research and legal development in this domain.

The author reflects on the appropriateness of distinguishing informational liability as an independent legal phenomenon that emerges at the intersection of traditional branches of law but possesses its own grounds, mechanisms of influence, and forms of implementation in the context of digital transformation of society.

Key words: information offence, information security, artificial intelligence, information legislation, cybercrime, legal liability.

Постановка питання. Війна, пандемія, інформаційні операції та пропаганда, штучний інтелект та зміна клімату – це теми які хвилюють суспільство останні кілька років. Вираз «Хто володіє інформацією, той володіє світом» набирає нових обертів. Авторка останні кілька років присвятила дослідженню новел законодавства в контексті інформаційних правопорушень. Чимало праць було присвячено забороненим видам висловлювань в контексті російсько-української війни, раніше фокус уваги був зосереджений на розголошенні певних видів таємниці. Вітчизняні та зарубіжні вчені опублікували чимало цікавих досліджень у цій сфері, але ми здійснимо спробу висвітлити свіжий погляд на поняття інформаційного правопорушення в сучасних умовах.

Метою статті є аналіз існуючих положень щодо визначення інформаційного правопорушення та формування нового підходу із врахуванням сучасних умов розвитку інформаційного суспільства.

Виклад основного матеріалу. Вчені-юристи безперервно працюють над удосконаленням класифікації правопорушень за різними критеріями. На сьогодні існує чимало категорій, як от майнові, насильницькі, корупційні тощо. Проте виокремлення такої категорії як інформаційні правопорушення зазнає критики. У законодавстві вже існує поняття кіберзлочину та комп'ютерного правопорушення, які охоплюють цифрову специфіку: обробку персональних даних; кібератаки; втручання в роботу систем; розповсюдження фейків або deepfake. Проте ці категорії не включають специфіку і характер інформації, з якою вчиняються діяння. Тому важливим є роз'яснення поняття інформаційне правопорушення, яке включає в себе увесь спектр протиправних діянь, пов'язаних із інформацією.

Значним етапом у формуванні міжнародно-правових механізмів протидії правопорушенням у сфері інформаційних технологій стало підписання у 2001 році Конвенції Ради Європи про кіберзлочинність (м. Будапешт), яка покликана забезпечити уніфікацію кримінально-правових підходів та поглиблення співпраці між державами щодо боротьби з найбільш небезпечними діяннями у сфері комп'ютерних систем і мереж, так званими «кіберзлочинами» [1]. Конвенція визначає чотири основні групи правопорушень, які повинні підлягати криміналізації в національних законодавствах держав-учасниць, а саме: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; злочини, пов'язані з використанням комп'ютерів як засобу вчинення злочину; правопорушення, пов'язані зі змістом інформації (зокрема, поширенням забороненого контенту); порушення авторських та суміжних прав у цифровому середовищі.

Україна приєдналася до Конвенції, ратифікувавши її у 2005 році. Наслідком її імплементації стало формування Розділу XVI Кримінального кодексу України – «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», що є першим вітчизняним кодифікованим підходом до криміналізації інформаційних правопорушень [2]. Підписання Будапештської конвенції можна розглядати як реакцію міжнародної спільноти на глобальну кіберзагрозу, а також як перший крок до інституалізації інформаційних правопорушень у межах кримінального права. Таким чином, кіберзлочини стали тією частиною інформаційних правопорушень, яка вже отримала нормативне визнання на міжнародному рівні та стала основою для подальшого розвитку кримінально-правового захисту інформаційної сфери.

Але, крім кіберзлочинів, існує чимало інформаційних правопорушень, за які передбачено інші види юридичної відповідальності. Сьогодні сформовано ґрунтовний законодавчий масив щодо регулювання інформаційної безпеки країни, проте із використанням інструментів штучного інтелекту, практично щодня виникають питання, які потребують законодавчого регулювання. Також із зростанням кількості користувачів всесвітньої мережі «Інтернет» паралельно зростає потенційна можливість стати жертвою використання інформаційних технологій у злочинних цілях [4, с. 85]. Із розвитком інформаційних технологій це явище перетворилося на глобальну проблему, поставивши

під загрозу не лише окремо взятих користувачів всесвітньої мережі «Інтернет», а й інформаційну безпеку цілих держав, оскільки і держава, і громадяни стають уразливими [5].

Вважаємо за доцільне спиратися на напрацювання провідних вчених із кримінального та адміністративного права, які працювали над вдосконаленням самого поняття правопорушення в тій чи іншій галузі. Так, під загальним поняттям "кримінальне правопорушення", що фактично виконує в кримінальному законодавстві України функцію відправної, визначальної категорії кримінального права, слід розуміти на думку М. Панова, С. Харитонова: передбачене Кримінальним кодексом України суспільно небезпечне, винне, кримінально каране діяння (дія чи бездіяльність), вчинене суб'єктом злочину. Це поняття посідає особливе місце в системі понять апарату кримінального права. Воно виконує консолідуючу функцію, оскільки визначає (на рівні загального) зміст понять "кримінальний проступок" і "злочин", що є видами кримінального правопорушення, а також поняття конкретних видів кримінальних правопорушень, визначених у кримінально-правових нормах, передбачених у статтях (частинах статей) Особливої частини КК України. Це поняття має слугувати базовою й установчою категорією у кримінальному правотворенні та правозастосовній діяльності.

М. Новицька у своїй роботі узагальнила позиції провідних вчених-адміністративістів та визначила що, згідно адміністративне правопорушення (проступок) є діянням, вчиненим відповідним суб'єктом, що порушує встановлені чинним законодавством заборони і тягне за собою покарання у вигляді адміністративних стягнень, визначених законом, поняття «адміністративне правопорушення» й «адміністративний проступок» можна застосовувати як синоніми, оскільки таку позицію зафіксовано і законодавцем [7, с. 390].

Для того, щоб сформувати поняття інформаційного правопорушення, спочатку потрібно розглянути поняття інформаційного законодавства та його можливу кодифікацію. Так, ряд вчених, Р. Калюжний, В. Гавловський, В. Цимбалюк, М. Гуцалюк зробили спробу аналізу правового регулювання інформаційних відносин в Україні та міжнародної практики, який дозволяє доктринально визначити низку основоположних методологічних, принципових положень інформаційного законодавства, яке виступає публічно-правовою основою такої юридичної інституції, як інформаційне право: основний об'єкт регулювання - суспільні інформаційні відносини; основний предмет суспільних відносин - інформація (відомості, дані, знання, таємниця тощо); метод правового регулювання - системне комплексне застосування методів конституційного, цивільного, адміністративного, трудового та кримінального права (що визначає міжгалузевий характер публічно-правового регулювання) та застосування методів приватно-правового регулювання (на рівні правочинів, угод, звичаїв, традицій, норм суспільної моралі, професійної, ділової етики); за правовою природою походження, як міжгалузевий комплексний інститут національного права України має приватно правову і публічно-правову природу; через предмет суспільних відносин інформаційне право має зв'язок з іншими міжгалузевими інститутами права: авторським правом, правом власності, правом інтелектуальної власності тощо, та утворює з ними складну, велику, агреговану гіперсистему права. Як констатацію факту, слід зазначити, що сучасне інформаційне законодавство України має характер змішаної системи права: зберігши галузевий підхід традиційної континентальної системи права, воно стало на шлях публічно-правового нормотворення за доктриною загального права (англо-американської системи права), коли окремі проблеми на законодавчому рівні вирішуються на рівні окремих законів [8, с. 18]. Крім того, зазначено, що виокремлення окремою галузі права – як інформаційне право, потребує формування поняття інформаційного правопорушення.

Крім цього, допоміжним буде аналіз складу правопорушення, який є типовим для більшості видів правопорушень у різних галузях. Традиційно, склад правопорушень має об'єктивні та суб'єктивні ознаки. Факт правопорушення може містити безліч різноманітних ознак, які визначають його як конкретну реальну життєву ситуацію. Проте не всі фактичні ознаки мають значення для встановлення відповідності вчиненого протиправного діяння певній правовій нормі, що передбачає те чи інше правопорушення, а також визначення виду й міри покарання. Для цього правовою нормою закріплюється сукупність обов'язкових ознак (елементів), які загалом становлять юридичний склад правопорушення [9, с. 15]. М. Баран зазначає, що правове регулювання юридичної відповідальності за порушення інформаційної безпеки у межах спеціальних законів, що обумовлюють запровадження та дію юрисдикційних правових механізмів, є незавершеним та системним. Принциповою особливістю юридичної відповідальності у сфері забезпечення інформаційної безпеки в умовах воєнного стану є її підвищений та обмежений у часі характер, домінування компенсаторної та охоронної функцій [10, с. 5].

Об'єктом інформаційного правопорушення є суспільні відносини у сфері створення, збирання, зберігання, обробки, передачі, захисту, зміни, використання та знищення інформації, які охороняються нормами права. Для того, щоб заглибитись в деталі ми проаналізували інформаційне законодавство (Закон України «Про інформацію» (1992), «Про захист інформації в інформаційно-комуні-

каційних системах» (1994), «Про державну таємницю» (1994), «Про захист персональних даних» (2010), «Про доступ до публічної інформації» (2011), «Про електронні документи та електронний документообіг» (2003), «Про електронну ідентифікацію та електронні довірчі послуги» (2017), «Про електронні комунікації» (2020)).

Також для формування юридичного поняття інформаційного правопорушення має значення об'єктивна сторона, тобто видима сторона правопорушення. Діяння (дія, чи бездіяльність) має бути пов'язане з інформацією. Іншими словами, це всі вищеперераховані діяння щодо інформації. Вважаємо за доцільне включити сюди також все що скоєно за допомогою гаджету або в самому гаджеті. Суб'єкт та суб'єктивна сторона, це відповідно фізична осудна особа та її ставлення вчиненого.

У загальному вигляді інформаційні правопорушення поділяються залежно від ступеня суспільної небезпеки на проступки та злочини. Відповідно, юридична відповідальність за них може бути: адміністративною, кримінальною, цивільно-правовою або дисциплінарною. Особливої актуальності набуває проблема захисту персональних даних та конфіденційної інформації, яка обробляється в автоматизованих системах. Інформаційні делікти в цій сфері включають: знищення або спотворення інформації, несанкціонований доступ, копіювання, використання, модифікацію або блокування інформації. Класифікація таких порушень базується на характері дій та загрози, яку вони створюють для інформаційної безпеки.

Багато дискусій виникає щодо нового закону «Про медіа» [18], в центрі уваги положення відсутності відповідальності за поширення інформації, що містить таємницю, яка спеціально охороняється законом, якщо ці відомості не було отримано незаконним шляхом. Детальний аналіз цього питання буде представлений у нашому наступному дослідженні. Юридична відповідальність у сфері інформаційних правопорушень передбачає наявність певних обов'язкових умов: суб'єкта-правопорушника, суб'єкта-потерпілого, закону, що регламентує відповідну поведінку, охоронної норми, а також юридичного факту правопорушення. Доцільно включити в законодавство деталізацію щодо поширення інформації через медіа, це має здійснюватися лише з дотриманням вимог спеціального законодавства, яке регламентує обіг відповідного виду інформації.

Водночас у кіберпросторі складно ідентифікувати зовнішні ознаки протиправної поведінки, особливо в разі поширення вірусів або використання анонімних технічних засобів. Такі дії, попри відсутність видимого наміру, все одно мають конкретного правопорушника, що створив або запустив шкідливе ПЗ.

Значна увага приділяється питанню природи так званих «інформаційних санкцій», що застосовуються до порушників інформаційного законодавства – наприклад, у вигляді анулювання ліцензії мовника або обмеження доступу до інформаційних ресурсів. У науці існує дискусія щодо їхнього статусу: частина фахівців розглядає їх як елемент нової, «інформаційної» відповідальності, інші – як різновид адміністративної. На практиці інформаційні правопорушення охоплюються нормами різних галузей права. Кримінальні – зазвичай пов'язані з несанкціонованим втручанням у роботу систем, порушенням таємниці, розповсюдженням шкідливого ПЗ тощо. Адміністративні охоплюють порушення порядку збору, обробки, зберігання та надання інформації, зокрема персональних даних, а також правопорушення у сфері ЗМІ, реклами, виборчих кампаній. Цивільно-правова відповідальність має майновий характер і стосується як договірних, так і позадоговірних зобов'язань (наприклад, компенсація за поширення недостовірної інформації чи за ненадання важливої інформації).

Наявність нових інформаційних реалій вимагає від правової науки систематизації та оновлення підходів до класифікації інформаційних деліктів. Очевидним є необхідність розробки єдиного комплексного інституту інформаційної відповідальності, який враховуватиме специфіку предмету порушення – інформації як нематеріального ресурсу – та особливості її правового режиму.

Отже, інформаційне правопорушення є специфічним типом делікту, який у сучасному суспільстві вимагає нових підходів до класифікації, регламентації та відповідальності. Відсутність кодифікованого акту, що унормовував би цю категорію, гальмує ефективність правозастосування та створює ризики юридичної невизначеності. Тому формування єдиного концептуального підходу до поняття, структури та видів інформаційної відповідальності є одним із ключових завдань сучасної правової науки.

Висновок. Отже, наукове й нормативне виокремлення інформаційних правопорушень є необхідним кроком у розвитку сучасної правової доктрини та практики, що дозволяє забезпечити належний рівень охорони прав людини, інформаційного суверенітету та кібербезпеки в умовах цифрової доби. Аналізуючи різні підходи до формулювання поняття правопорушення в різних галузях, прийшли до висновку що інформаційне правопорушення – це протиправне діяння (дія або бездіяльність), пов'язане з інформацією як основним предметом посягання або засобом скоєн-

ня правопорушення, яке завдає або створює загрозу заподіяння шкоди охоронюваним законом суспільним відносинам у сфері створення, збирання, обробки, передачі, зберігання, зміни, знищення чи захисту інформації незалежно від форми її існування. Такий підхід дозволяє не лише систематизувати правопорушення у сфері інформації, а й ефективно реагувати на нові виклики, пов'язані з розвитком цифрових технологій, штучного інтелекту, кіберзагроз і гібридних інформаційних впливів. Нагальною залишається потреба в гармонізації нормативного поля, узгодженні термінології, формуванні єдиної правової позиції та розробці спеціальних механізмів відповідальності у сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конвенція про кіберзлочинність, підписана в місті Будапешт 23 листопада 2001 року. Ратифікована Законом України від 07 вересня 2005 року № 2824 IV. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 26.01.2025).
2. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131. URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 26.01.2025).
3. Hilgendorf E. Digitization and the Law. Nomos Verlagsgesellschaft mbH & Co. KG, 2018.
4. Федоренко Т.В., Садковський С.П. Юридична відповідальність в інформаційній сфері: поняття та особливості. *Часопис Київського університету права*. 2022. № 2–4. С. 82–85.
5. Про захист персональних даних: Закон України від 01 черв. 2010 р. № 2297 VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 26.07.2025).
6. Панов М., Харитонов С. Кримінальне правопорушення: поняття та його види. *Право України*. 2021. № 3. С. 27–59.
7. Новицька М. «Адміністративне правопорушення» та суміжні поняття: аналіз співвідношення. *Юридичний вісник*. 2020. № 1. С. 384–390.
8. Калюжний Р. та ін. Питання концепції реформування інформаційного законодавства України. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2000. С. 17–21.
9. Тихомиров О.О., Тугарова О.К. Юридична відповідальність за правопорушення в інформаційній сфері: навч. посіб. Київ: Нац. акад. СБУ. – 2015.
10. Баран М.В. Адміністративно-правове забезпечення інформаційної безпеки в Україні: дис. ... д-ра філософії : 081 Право. Львівський державний університет внутрішніх справ. Львів, 2022.
11. Мазепа С О. Як Україна протистоїть ворогу на інформаційному фронті? *Наукові заходи Юридичного факультету Західноукраїнського національного університету*. 2023. С. 344–345.
12. Про інформацію: Закон України від 02 жовт. 1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 26.02.2025).
13. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 26.02.2025).
14. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314. URL: <https://zakon.rada.gov.ua/laws/show/2939-17> (дата звернення: 26.02.2025).
15. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 26.0.2025).
16. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93. URL: <https://zakon.rada.gov.ua/laws/show/3855-12> (дата звернення: 26.07.2025).
17. Про електронні документи та електронний документообіг: Закон України від 22 трав. 2003 р. № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: <https://zakon.rada.gov.ua/laws/show/851-15> (дата звернення: 26.07.2025).
18. Про медіа: Закон України від 13.12.2022 р. № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text> (дата звернення: 12.03.2025).