Теоретико-правові основи юридичної відповідальності за правопорушення в інформаційній сфері

Чистоклетов Л. Г.[1], Несторко Я. Б.[2]

Опубліковано	Секція	УДК
30.01.2026	Право	34.03:347:007

DOI: https://doi.org/10.5281/zenodo.19946344

Анотація. У статті досліджено теоретико-правові засади юридичної відповідальності за правопорушення в інформаційній сфері в умовах розвитку інформаційного суспільства, цифровізації та сучасних воєнних викликів. На основі аналізу чинного законодавства України, зокрема Конституції України, Закону України «Про інформацію», Закону України «Про доступ до публічної інформації», Кримінального кодексу України та Кодексу України про адміністративні правопорушення, а також міжнародних правових актів, зокрема Конвенції про кіберзлочинність, розкрито сутність інформації як правової категорії та визначено її місце у системі суспільних відносин.

У ході дослідження встановлено, що інформація виступає не лише ресурсом, але й стратегічним фактором впливу, який визначає ефективність функціонування держави, рівень захищеності прав і свобод людини та стабільність суспільства. Обґрунтовано, що правове регулювання інформаційних відносин має комплексний характер і спрямоване на забезпечення балансу між реалізацією права на інформацію та необхідністю її обмеження в інтересах національної безпеки, громадського порядку та захисту прав інших осіб.

Проаналізовано поняття та ознаки інформаційних правопорушень, які визначаються як протиправні, суспільно небезпечні та винні діяння, що здійснюються у сфері інформаційної діяльності або з використанням інформаційних технологій і порушують встановлений порядок інформаційних відносин. Встановлено, що характерною рисою таких правопорушень є їх тісний зв'язок із процесами створення, оброблення, зберігання та поширення інформації, а також із функціонуванням інформаційно-комунікаційних систем.

Визначено, що система юридичної відповідальності за правопорушення в інформаційній сфері має міжгалузевий характер і включає кримінальну, адміністративну, цивільно-правову та дисциплінарну відповідальність. Доведено, що кримінальна відповідальність застосовується за найбільш суспільно небезпечні діяння, пов'язані з несанкціонованим втручанням у роботу інформаційних систем, тоді як адміністративна відповідальність виконує превентивну функцію і спрямована на припинення менш небезпечних порушень. Водночас цивільно-правова відповідальність забезпечує відшкодування завданої шкоди, а дисциплінарна – дотримання правил інформаційної діяльності у межах трудових відносин.

[1] доктор юридичних наук, професор, Навчально-науковий інститут права, психології та інноваційної освіти Національного університету «Львівська політехніка», https://orcid.org/0000-0002-3306-1593
[2] здобувачка, Навчально-науковий інститут права, психології та інноваційної освіти Національного університету «Львівська політехніка» https://orcid.org/0009-0004-5613-8866

Особливу увагу приділено питанням захисту персональних даних, які в умовах цифровізації набувають особливого значення. Встановлено, що порушення порядку обробки персональних даних є одним із найбільш поширених видів правопорушень у цій сфері та потребує належного правового регулювання і контролю.

Окремо досліджено вплив сучасних викликів, зокрема дезінформації, пропаганди та інформаційних операцій, які особливо актуалізуються в умовах російсько-української війни. Обґрунтовано, що інформаційна сфера фактично перетворюється на окремий фронт, а поширення недостовірної інформації становить загрозу національній безпеці та демократичним процесам. У зв'язку з цим підкреслено необхідність удосконалення механізмів юридичної відповідальності та впровадження комплексної системи протидії інформаційним загрозам.

Проаналізовано також міжнародний досвід, зокрема європейські підходи до протидії інформаційним правопорушенням, які базуються на поєднанні правових, організаційних і технологічних інструментів. Встановлено, що їх адаптація в Україні є важливим кроком для підвищення ефективності захисту інформаційного простору держави.

Ключові слова: інформаційна сфера, інформаційні правовідносини, інформаційні правопорушення, юридична відповідальність, інформаційне право, інформаційна безпека, кіберзлочинність, дезінформація, персональні дані, цифрові технології, національна безпека, правове регулювання, інформаційне суспільство.

Theoretical and legal foundations of legal liability for offenses in the information sphere

Abstract. The article examines the theoretical and legal foundations of legal liability for offenses in the information sphere under conditions of the development of the information society, digitalization, and modern wartime challenges. Based on the analysis of the current legislation of Ukraine, in particular the Constitution of Ukraine, the Law of Ukraine "On Information", the Law of Ukraine "On Access to Public Information", the Criminal Code of Ukraine, and the Code of Ukraine on Administrative Offenses, as well as international legal acts, including the Convention on Cybercrime, the essence of information as a legal category is раскрыто and its place within the system of social relations is determined.

The study establishes that information acts not only as a resource but also as a strategic factor influencing the effectiveness of state functioning, the level of protection of human rights and freedoms, and the stability of society. It is substantiated that the legal regulation of information relations is complex in nature and aimed at ensuring a balance between the exercise of the right to information and the necessity of its restriction in the interests of national security, public order, and the protection of the rights of others.

The concept and characteristics of information offenses are analyzed, which are defined as unlawful, socially dangerous, and culpable acts (actions or omissions) committed in the field of information activity or using information technologies, and which violate the established order of information relations. It is determined that a distinctive feature of such offenses is their close connection with the processes of creation, processing, storage, and dissemination of information, as well as with the functioning of information and communication systems.

It is established that the system of legal liability for offenses in the information sphere has an interdisciplinary nature and includes criminal, administrative, civil, and disciplinary liability. It is proven that criminal liability is applied to the most socially dangerous acts related to unauthorized interference in the functioning of information systems, while administrative liability performs a preventive function and is aimed at stopping less dangerous violations. At the same time, civil liability ensures compensation for damage caused, and disciplinary liability ensures compliance with the rules of information activity within labor relations.

Particular attention is paid to the issues of personal data protection, which have become especially significant in the context of digitalization. It is established that violations of personal data processing procedures are among the most common types of offenses in this sphere and require proper legal regulation and control.

The influence of modern challenges, including disinformation, propaganda, and information operations, which have become particularly relevant in the context of the Russian-Ukrainian war, is also examined. It is substantiated that the information sphere is effectively transforming into a separate front, while the dissemination of false information poses a threat to national security and democratic processes. In this regard, the need to improve mechanisms of legal liability and to implement a comprehensive system for countering information threats is emphasized.

International experience is also analyzed, in particular European approaches to combating information offenses, which are based on a combination of legal, organizational, and technological tools. It is determined that their adaptation in Ukraine is an important step towards increasing the effectiveness of protecting the national information space.

Keywords: information sphere, information legal relations, information offenses, legal liability, information law, information security, cybercrime, disinformation, personal data, digital technologies, national security, legal regulation, information society.

Вступ

У сучасних умовах розвитку інформаційного суспільства інформація перетворюється на один із ключових ресурсів, що визначає ефективність функціонування держави, рівень забезпечення прав і свобод людини та стабільність суспільства. Активне впровадження цифрових технологій, розширення інформаційного простору та зростання обсягів обробки даних зумовлюють появу нових видів правопорушень у сфері інформаційних відносин, що ускладнює їх правове регулювання.

Особливої актуальності ця проблема набуває в умовах воєнного стану та збройної агресії, коли інформаційна сфера фактично перетворюється на окремий фронт, а інформація використовується як інструмент впливу на суспільну свідомість і національну безпеку. Поширення дезінформації, пропаганди, незаконне використання інформаційних ресурсів та порушення порядку обробки персональних даних створюють додаткові загрози, які потребують ефективного правового реагування.

Водночас аналіз чинного законодавства свідчить про наявність низки проблем, зокрема фрагментарність нормативно-правового регулювання, дублювання окремих норм, а також невідповідність темпів його розвитку динаміці інформаційних технологій. Це ускладнює застосування юридичної відповідальності та знижує ефективність захисту інформаційних правовідносин.

Крім того, інформаційні правопорушення мають комплексний і міжгалузевий характер, що зумовлює необхідність їх дослідження крізь призму різних галузей права, а також з урахуванням міжнародного досвіду. У зв'язку з цим виникає потреба у поглибленому теоретико-правовому аналізі юридичної відповідальності за правопорушення в інформаційній сфері з метою вдосконалення механізмів правового регулювання та підвищення їх ефективності.

Щодо аналіз дослідження проблеми то окремі аспекти юридичної відповідальності за правопорушення в інформаційній сфері, інформаційного права, інформаційної безпеки, а також правового регулювання інформаційних відносин досліджували у своїх працях О. О. Тихомиров, О. К. Тугарова, І. В. Арістова, О. А. Баранов, О. П. Дзьобань, А. В. Кирилюк, І. С. Жевелєва, О. Марін, Н. Глущенко, А. Головач, О. А. Заярний, А. О. Кодинець, В. П. Бакало, О. В. Коба, В. Іванцов, В. Бахмат, Р. Дем'янюк та інші науковці. Їхні наукові праці сформували теоретичну основу для розуміння сутності інформаційних правопорушень, визначення їх ознак і класифікації, а також дослідження системи

юридичної відповідальності, що включає кримінальну, адміністративну, цивільно-правову та дисциплінарну відповідальність. Значна увага у наукових дослідженнях приділяється питанням кваліфікації правопорушень у сфері використання інформаційно-комунікаційних технологій, проблемам адміністративної відповідальності та особливостям цивільно-правового захисту інформаційних правовідносин.

Метою статті є комплексний аналіз теоретико-правових засад юридичної відповідальності за правопорушення в інформаційній сфері, визначення їх сутності, ознак та видів, а також дослідження особливостей правового регулювання інформаційних відносин у сучасних умовах розвитку цифрових технологій та воєнних викликів.

Результати

У сучасному інформаційному суспільстві інформація виступає одним із ключових ресурсів, що визначає рівень розвитку держави, ефективність функціонування її інститутів та ступінь захищеності прав і свобод людини. Саме тому питання правового регулювання інформаційних відносин набуває особливої актуальності, адже належне функціонування інформаційної сфери є важливою передумовою стабільності суспільства.

Відповідно до Закону України «Про інформацію», інформація визначається як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Таке широке розуміння інформації свідчить про її універсальний характер та застосування у різних сферах суспільного життя. Водночас важливим є забезпечення належного рівня її захисту, який розглядається як сукупність правових, організаційних, технічних та інших заходів, спрямованих на збереження, цілісність інформації та регулювання доступу до неї.

Законодавство також гарантує кожному право на інформацію, яке забезпечується створенням відповідних механізмів доступу до інформаційних ресурсів, відкритістю діяльності органів державної влади, а також здійсненням контролю за дотриманням інформаційного законодавства. Важливо, що право на інформацію не є абсолютним і може бути обмежене законом з метою забезпечення національної безпеки, громадського порядку, захисту прав інших осіб та інших суспільно значущих інтересів [1].

Водночас порушення встановлених меж реалізації цього права зумовлює виникнення правопорушень в інформаційній сфері, що потребують детального правового аналізу.

Суттєвий вплив на формування сучасного розуміння правопорушень у сфері інформаційних технологій справили міжнародні правові акти, зокрема Європейська конвенція про кіберзлочинність 2001 року, яка визначила основні групи правопорушень у сфері комп'ютерних систем і мереж. Україна, приєднавшись до цієї Конвенції, імплементувала її положення у національне законодавство, що сприяло виокремленню відповідних правопорушень у кримінальному праві [2].

Загалом інформаційне правопорушення визначається як протиправне, суспільно небезпечне, винне діяння (дія або бездіяльність), що здійснюється у сфері інформаційної діяльності або з використанням інформаційних технологій і порушує встановлений порядок інформаційних відносин . Такі правопорушення можуть проявлятися у різних формах, зокрема у незаконному доступі до інформації, її поширенні, приховуванні або спотворенні.

Характерною особливістю цих правопорушень є їх безпосередній зв'язок з інформаційними процесами, включаючи створення, оброблення, зберігання та поширення інформації, а також використання інформаційно-комунікаційних

технологій. Саме ця ознака дозволяє виділити їх у самостійну групу правопорушень [3, с. 53-54].

Важливим аспектом є також питання так званої «інформаційної відповідальності». Під юридичною відповідальністю розуміється правовідношення між державою та особою, яка вчинила правопорушення, у межах якого застосовуються передбачені законом санкції. Вона виконує стимулюючу, компенсаційну, превентивну та каральну функції.

Нормативною основою відповідальності є законодавство України, зокрема ст. 24 Закону України «Про доступ до публічної інформації», яка передбачає відповідальність за ненадання інформації, безпідставну відмову, надання недостовірної чи неповної інформації та інші порушення [4].

Також важливо, що право на інформацію має конституційне підґрунтя, оскільки відповідно до ст. 34 Конституції України кожному гарантується свобода збирання, зберігання, використання та поширення інформації. Реалізація цього права забезпечується системою спеціальних нормативно-правових актів, які не лише визначають порядок доступу до інформації, а й встановлюють відповідальність за порушення встановлених правил [5].

Подальший розвиток нормативного регулювання проявляється у закріпленні видів юридичної відповідальності на рівні галузевого законодавства. Зокрема, відповідно до ч. 1 ст. 27 Закону України «Про інформацію», порушення законодавства у цій сфері тягне дисциплінарну, цивільну, адміністративну або кримінальну відповідальність [1]. Це свідчить про комплексний, міжгалузевий характер відповідальності, оскільки вона реалізується через норми різних галузей права залежно від характеру вчиненого правопорушення.

Кримінальна відповідальність у сфері інформаційних технологій займає особливе місце в системі юридичної відповідальності, оскільки є найбільш суворим засобом державного реагування на правопорушення. Вона спрямована на охорону інформаційних правовідносин і застосовується за вчинення суспільно небезпечних діянь у цій сфері. Важливо розмежовувати кримінальну відповідальність і покарання, оскільки покарання є лише формою її реалізації. Кримінальна відповідальність виникає з моменту вчинення правопорушення, тоді як покарання визначається судом і полягає у конкретних обмеженнях прав і свобод особи [6, с. 118].

Основним нормативно-правовим актом, що встановлює кримінальну відповідальність за правопорушення у сфері інформаційних технологій, є Кримінальний кодекс України. Зокрема, розділ XVI Особливої частини визначає відповідальність за несанкціоноване втручання в роботу комп'ютерів, мереж та інформаційних систем, створення та розповсюдження шкідливих програм, незаконний збут або використання інформації з обмеженим доступом. Норми Кодексу встановлюють види покарань залежно від тяжкості правопорушення, що забезпечує правовий захист інформаційної безпеки держави та громадян [7].

Окрему увагу слід приділити класифікації за наслідками, оскільки вони можуть варіюватися від незначного втручання до заподіяння істотної шкоди, включаючи порушення функціонування інформаційних систем, втрату або спотворення даних. Також важливим є поділ за мотивами вчинення, які можуть мати корисливий, політичний або інший характер .

Важливим елементом правильної кваліфікації таких правопорушень є встановлення їх складу, який включає об'єкт, об'єктивну сторону, суб'єкт та суб'єктивну сторону. Зокрема, об'єктом виступає встановлений порядок функціонування інформаційних систем і мереж, а суб'єктом - фізична осудна особа, яка досягла встановленого законом віку. При цьому значну роль відіграє аналіз суб'єктивної сторони, зокрема форми вини та мети вчинення діяння .

Кримінальні правопорушення у сфері інформаційних технологій дедалі частіше використовуються як засіб вчинення більш тяжких злочинів, зокрема тих, що посягають на національну безпеку. Це обумовлює підвищену увагу до їх кваліфікації та необхідність удосконалення кримінально-правових норм у цій сфері [8, с. 78-79].

Важливим є вплив інформаційної діяльності на процеси прийняття рішень у суспільстві. Використання недостовірної або маніпулятивної інформації здатне спотворювати суспільну свідомість, що, у свою чергу, впливає на реалізацію принципів демократії та народовладдя. Це підкреслює важливість забезпечення належного рівня правового контролю у сфері поширення інформації .

Сучасні події свідчать про те, що інформаційний вплив може використовуватися як інструмент досягнення політичних і навіть військових цілей. Це зумовлює необхідність формування нових підходів до кримінально-правового реагування на такі дії, зокрема шляхом розширення переліку кримінально караних діянь у сфері інформаційних відносин [9, с. 251-253].

Водночас поряд із кримінальною відповідальністю за більш тяжкі правопорушення в інформаційній сфері важливу роль відіграє адміністративна відповідальність, яка застосовується до менш суспільно небезпечних діянь.

Правову основу такої відповідальності становить Кодекс України про адміністративні правопорушення, який визначає перелік відповідних правопорушень і заходи впливу за їх вчинення. Зокрема, Кодекс передбачає відповідальність за порушення права на інформацію та неправомірну відмову в її наданні (ст. 212-3 КУпАП), порушення законодавства про захист персональних даних (ст. 188-39 КУпАП), а також інші правопорушення, пов’язані з недотриманням встановленого порядку збирання, зберігання, використання та поширення інформації [10].

Адміністративна відповідальність у цій сфері виступає важливим інструментом охорони інформаційних правовідносин і спрямована на попередження та припинення правопорушень. Вона є формою реагування держави на протиправні діяння, які порушують встановлений порядок здійснення інформаційної діяльності. При цьому суб’єктами таких правопорушень можуть бути як фізичні, так і юридичні особи, а об’єктом – суспільні відносини, пов’язані із забезпеченням інформаційної безпеки, доступу до інформації, захисту персональних даних та інших інформаційних інтересів.

Особливістю адміністративної відповідальності є те, що вона реалізується через застосування уповноваженими органами державної влади передбачених законом заходів впливу. Такі заходи мають на меті не лише покарання, але й запобігання подальшим правопорушенням, що підкреслює її превентивний характер у системі юридичної відповідальності.

Водночас аналіз сучасного стану правового регулювання свідчить про наявність певних проблем, зокрема фрагментарність нормативної бази та невідповідність темпів розвитку законодавства динаміці інформаційного суспільства. Це ускладнює ефективне застосування адміністративної відповідальності та вимагає подальшого вдосконалення правових механізмів у цій сфері [11, с. 288].

З урахуванням зазначених особливостей адміністративних правопорушень у сфері інформації, окремої уваги потребують діяння, пов’язані з обробкою та захистом персональних даних.

Відповідно до ст. 32 Конституції України, ніхто не може зазнавати втручання в його особисте і сімейне життя, а збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди не допускається, за винятком випадків, визначених законом [5].

У розвиток зазначених положень законодавство України встановлює чіткі вимоги до обробки персональних даних. Зокрема, така обробка повинна здійснюватися виключно з визначеною метою та на законних підставах, а володілець персональних

даних зобов'язаний забезпечити їх належний захист від незаконного доступу, втрати чи пошкодження.

Порушення цих вимог тягне за собою адміністративну відповідальність, зокрема у випадках недотримання порядку обробки персональних даних, невиконання законних вимог уповноважених органів або неналежного забезпечення їх захисту. Найпоширенішими правопорушеннями є незаконне розголошення персональних даних, їх розміщення у відкритому доступі без правових підстав, а також передача інформації третім особам без відповідних повноважень.

Сучасний розвиток цифрових технологій і розширення інформаційної сфери призводять до появи нових видів правопорушень, при цьому законодавство не завжди встигає адаптуватися до цих змін. Унаслідок цього адміністративні правопорушення залишаються найбільш поширеними у сфері інформаційних відносин.

Водночас проблемою залишається недосконалість законодавчого регулювання, зокрема відсутність санкцій за окремі правопорушення або дублювання норм у різних актах, що ускладнює їх застосування.

Крім того, законодавство передбачає випадки, коли діяння не визнається правопорушенням, зокрема за наявності стану крайньої необхідності, коли шкода є меншою, ніж відвернена небезпека. Це має особливе значення для інформаційної сфери [12, с. 119-120].

Поряд із адміністративною відповідальністю важливе значення у системі юридичної відповідальності за правопорушення в інформаційній сфері має цивільно-правова відповідальність, яка спрямована насамперед на відновлення порушених прав та компенсацію завданої шкоди. Її застосування пов'язане з наявністю цивільного правопорушення, яке породжує правовідносини між потерпілою особою та правопорушником щодо відшкодування шкоди .

У науковій доктрині підставою цивільно-правової відповідальності визнається порушення суб'єктивних цивільних прав, як майнових, так і немайнових. Водночас для притягнення до відповідальності необхідна наявність певних умов, серед яких виділяють протиправну поведінку, шкоду, причинний зв'язок між діями порушника та наслідками, а також вину. Саме ці елементи дозволяють встановити факт правопорушення та обґрунтувати обов'язок відшкодування шкоди.

Крім того, специфікою цивільно-правової відповідальності в інформаційній сфері є наявність випадків звільнення від відповідальності. Зокрема, не підлягають відшкодуванню оціночні судження, а також інформація, поширена журналістом за умови добросовісності та належної перевірки. Такі положення спрямовані на забезпечення балансу між захистом прав особи та свободою вираження поглядів [14, с. 58-60].

Зазначені підходи знаходять своє нормативне закріплення у положеннях Цивільного кодексу України. Зокрема, відповідно до ст. 16 гарантується право на захист цивільних прав, у тому числі пов'язаних з інформаційними відносинами, ст. 1166 встановлює загальні підстави відшкодування майнової шкоди, а ст. 1176 визначає особливості відповідальності за шкоду, завдану незаконними рішеннями органів державної влади. Крім того, положення цивільного законодавства застосовуються у випадках неправомірного використання, поширення або пошкодження інформації, що забезпечує захист особистих немайнових прав, у тому числі у цифровому середовищі [15].

Як зазначається у наукових дослідженнях, інформаційні правопорушення досить часто вчиняються працівниками підприємств, установ чи організацій під час виконання ними своїх службових обов'язків . У таких випадках, незалежно від можливості притягнення особи до інших видів юридичної відповідальності, зберігається можливість застосування дисциплінарної відповідальності в межах трудових правовідносин.

Дисциплінарна відповідальність розглядається як один із видів юридичної відповідальності, що полягає в обов'язку працівника відповідати за порушення трудової дисципліни та зазнавати передбачених законом заходів впливу. Її підставою є дисциплінарний проступок, тобто протиправне та винне невиконання або неналежне виконання службових обов'язків, зокрема у сфері поводження з інформацією. Важливою особливістю є те, що така відповідальність може застосовуватися одночасно з іншими видами відповідальності, що підкреслює її допоміжний, але необхідний характер [13, с. 268-270].

В умовах збройної агресії та запровадження воєнного стану в Україні особливого значення набуває питання юридичної відповідальності військовослужбовців і військовозобов'язаних. Правовою основою таких змін є Закон України «Про правовий режим воєнного стану». Відповідно до ст. 1–2, воєнний стан – це особливий правовий режим, що передбачає встановлення спеціальних умов функціонування держави, а також можливість обмеження окремих прав і свобод громадян з метою забезпечення оборони та безпеки.

Особливістю цього режиму є поєднання обмеження прав (ст. 12–15) із розширенням повноважень держави у сфері оборони. У таких умовах до військовослужбовців висуваються підвищені вимоги щодо дисципліни та безумовного виконання наказів (ст. 10–11, 19–20) [16].

Військовослужбовці залежно від характеру вчиненого правопорушення несуть дисциплінарну, адміністративну, матеріальну, цивільно-правову та кримінальну відповідальність. Водночас важливим є розмежування загальної та спеціальної відповідальності: у першому випадку йдеться про правопорушення, не пов'язані з проходженням служби, тоді як спеціальна відповідальність виникає за порушення, що безпосередньо пов'язані з виконанням військових обов'язків. Такий підхід дозволяє враховувати специфіку військової діяльності при визначенні виду та міри покарання.

Особливістю відповідальності військовослужбовців є також її трансформаційний характер. Зокрема, за окремі адміністративні правопорушення вони можуть нести як адміністративну, так і дисциплінарну відповідальність, що обумовлено посиленням ролі командирів у підтриманні правопорядку. Крім того, у законодавстві виокремлено спеціальну категорію військових адміністративних правопорушень, за які передбачено підвищені санкції [17, с. 5-8].

Окремої уваги потребує і відповідальність військовослужбовців у інформаційній сфері. В умовах війни інформація набуває стратегічного значення, а її неправомірне використання, розголошення або викривлення може створювати загрози національній безпеці. Саме тому порушення порядку обігу службової інформації, розголошення відомостей з обмеженим доступом чи поширення недостовірної інформації можуть розглядатися як дисциплінарні, адміністративні або навіть кримінальні правопорушення. У цьому контексті відповідальність виконує не лише каральну, а й превентивну функцію, спрямовану на недопущення інформаційних загроз у військовій сфері [18, с. 598-600].

В умовах сучасної російсько-української війни особливого значення набуває проблема поширення дезінформації та пропаганди, які виступають важливими інструментами інформаційного впливу. Інформаційна сфера фактично перетворюється на окремий фронт, де відбувається боротьба за громадську думку та стабільність держави. У таких умовах питання юридичної відповідальності за поширення неправдивої інформації набуває особливої актуальності.

Дезінформація та пропаганда мають цілеспрямований характер і спрямовані на маніпулювання суспільною свідомістю, підрив довіри до державних інституцій та створення атмосфери невизначеності. Вони реалізуються через спотворення фактів, поширення фейкових новин і викривлення подій, що негативно впливає на моральний

стан населення та інформаційну безпеку держави. Особливістю таких інформаційних впливів є їх системність і орієнтація як на внутрішню, так і на міжнародну аудиторію.

Важливу роль у цьому процесі відіграють медіа та соціальні мережі, які забезпечують швидке поширення інформації, але водночас створюють умови для масового розповсюдження недостовірних даних. Через алгоритми цифрових платформ та швидкість поширення контенту фейкова інформація часто випереджає її спростування, що підсилює негативний ефект дезінформації.

Водночас медіа виступають ключовим інструментом протидії таким явищам, здійснюючи фактчекінг, забезпечуючи об'єктивне висвітлення подій та сприяючи підвищенню рівня медіаграмотності населення. Формування критичного мислення дозволяє зменшити вплив маніпулятивної інформації та підвищує стійкість суспільства до інформаційних атак.

Таким чином, дезінформація та пропаганда становлять серйозну загрозу інформаційній безпеці, що зумовлює необхідність встановлення ефективних механізмів юридичної відповідальності за їх поширення та формування комплексної системи протидії таким явищам [19, с. 102].

Важливим елементом міжнародної практики протидії інформаційним правопорушенням є Конвенція про кіберзлочинність, яка встановлює єдині підходи до криміналізації кіберзлочинів та співпраці держав у цій сфері. Зокрема, відповідно до ст. 2 Конвенції передбачена відповідальність за незаконний доступ до комп'ютерних систем, ст. 4 – за втручання в дані, а ст. 5 – за втручання в роботу комп'ютерних систем.

Особливістю Конвенції є також закріплення механізмів міжнародної взаємодії (розділ III), які передбачають обмін інформацією, взаємну правову допомогу та координацію дій правоохоронних органів різних держав. Це має особливе значення в умовах війни, коли інформаційні правопорушення часто мають транснаціональний характер і здійснюються через кіберпростір.

Застосування положень Конвенції про кіберзлочинність сприяє підвищенню ефективності боротьби з інформаційними правопорушеннями, узгодженню національного законодавства з міжнародними стандартами та посиленню кібербезпеки держави [2].

Європейський підхід до протидії інформаційним маніпуляціям базується на комплексному поєднанні правових, організаційних і технологічних заходів. Зокрема, важливими інструментами є впровадження програм медіаграмотності, розвиток систем швидкого реагування на дезінформаційні кампанії, а також встановлення вимог до діяльності цифрових платформ щодо модерації контенту та забезпечення його прозорості. Значна увага приділяється також підтримці незалежних фактчекінгових організацій і запровадженню механізмів контролю за політичною рекламою.

Водночас європейська практика передбачає і застосування обмежувальних заходів до суб'єктів, які системно поширюють дезінформацію, включаючи санкції та обмеження діяльності окремих медіаресурсів. Окремого значення набуває правове регулювання новітніх технологій, зокрема штучного інтелекту, який може використовуватися для створення маніпулятивного контенту (наприклад, deepfake).

Європейські практики демонструють ефективність комплексного підходу до протидії інформаційним загрозам, що поєднує правове регулювання, технологічні інструменти та підвищення рівня обізнаності суспільства. Їх адаптація в Україні є важливим кроком для посилення відповідальності за інформаційні правопорушення та забезпечення інформаційної безпеки в умовах війни [20, с. 108].

Висновки

Отже, інформаційна сфера в сучасному суспільстві посідає центральне місце у забезпеченні функціонування держави, реалізації прав і свобод людини та підтриманні

суспільної стабільності. Інформація виступає не лише ресурсом, але й стратегічним фактором впливу, що зумовлює необхідність її належного правового регулювання та захисту. Саме тому формування ефективної системи юридичної відповідальності за правопорушення в інформаційній сфері є важливим елементом правової держави.

Право на інформацію, закріплене на конституційному рівні та деталізоване у спеціальному законодавстві, створює основу для реалізації інформаційних правовідносин. Водночас його не абсолютний характер передбачає встановлення певних обмежень, що спрямовані на забезпечення балансу між свободою інформації та захистом інших суспільно значущих інтересів. Саме порушення цих меж стає підставою для виникнення інформаційних правопорушень, які характеризуються специфічними ознаками, пов'язаними з використанням інформаційних технологій та впливом на інформаційні процеси.

Аналіз поняття та ознак інформаційних правопорушень дозволяє зробити висновок про їх комплексний характер. Вони охоплюють широкий спектр діянь - від незаконного доступу до інформації до її маніпулятивного поширення. Особливістю таких правопорушень є їх тісний зв'язок із цифровими технологіями, що постійно розвиваються, унаслідок чого з'являються нові форми протиправної поведінки. Це, у свою чергу, вимагає постійного вдосконалення законодавства та адаптації правових механізмів до сучасних викликів.

Важливу роль у формуванні національної системи протидії інформаційним правопорушенням відіграють міжнародні правові акти, зокрема Конвенція про кіберзлочинність. Її положення сприяли гармонізації українського законодавства з міжнародними стандартами та визначенню ключових напрямів боротьби з кіберзлочинністю. Це є особливо актуальним з огляду на транснаціональний характер інформаційних правопорушень, які часто виходять за межі однієї держави.

Система юридичної відповідальності за правопорушення в інформаційній сфері має міжгалузевий характер і включає кримінальну, адміністративну, цивільно-правову та дисциплінарну відповідальність. Кожен із цих видів виконує окрему функцію та застосовується залежно від ступеня суспільної небезпечності правопорушення. Кримінальна відповідальність є найбільш суворою формою реагування держави та застосовується за вчинення тяжких правопорушень, що посягають на інформаційну безпеку. Водночас адміністративна відповідальність забезпечує оперативне реагування на менш небезпечні порушення та виконує важливу превентивну функцію.

Не менш важливими є цивільно-правова та дисциплінарна відповідальність, які спрямовані відповідно на відшкодування завданої шкоди та забезпечення дотримання трудової дисципліни. Їх застосування дозволяє комплексно реагувати на правопорушення, забезпечуючи не лише покарання винних осіб, але й відновлення порушених прав. Особливістю є можливість поєднання різних видів відповідальності, що підкреслює системний характер правового регулювання у цій сфері.

Окремої уваги заслуговують питання відповідальності за порушення законодавства про захист персональних даних. У сучасних умовах цифровізації ці правовідносини набувають особливої значущості, оскільки обробка персональних даних є невід'ємною частиною діяльності як державних органів, так і приватного сектору. Недотримання встановлених вимог створює загрозу порушення права на приватність та може мати серйозні наслідки для особи.

Суттєвим викликом залишається недосконалість нормативно-правового регулювання, яка проявляється у фрагментарності законодавства, дублюванні норм та відставанні правового регулювання від темпів розвитку інформаційних технологій. Це ускладнює ефективне застосування юридичної відповідальності та потребує системного вдосконалення законодавчої бази.

Особливого значення питання юридичної відповідальності набувають в умовах воєнного стану та збройної агресії. У цей період інформаційна сфера перетворюється на один із ключових елементів національної безпеки, а інформація - на інструмент ведення війни. Це зумовлює посилення вимог до поведінки військовослужбовців і військовозобов'язаних, а також встановлення підвищеної відповідальності за порушення, пов'язані з обігом інформації.

Поширення дезінформації та пропаганди в умовах війни становить серйозну загрозу для держави та суспільства. Такі дії спрямовані на дестабілізацію ситуації, підрив довіри до державних інституцій та маніпулювання громадською думкою. У зв'язку з цим виникає необхідність формування ефективних механізмів юридичної відповідальності за подібні правопорушення, а також розвитку системи протидії інформаційним загрозам.

Важливу роль у цьому процесі відіграє міжнародний досвід, зокрема європейські підходи до боротьби з дезінформацією, які передбачають поєднання правових, організаційних та технологічних заходів. Їх впровадження в Україні сприятиме підвищенню ефективності захисту інформаційного простору та зміцненню національної безпеки.

Отже, юридична відповідальність за правопорушення в інформаційній сфері є складною та багатогранною системою, яка постійно розвивається під впливом технологічних і суспільних змін. Її ефективність залежить від узгодженості законодавства, здатності держави оперативно реагувати на нові виклики та рівня правової культури суспільства. У сучасних умовах особливо важливим є формування комплексного підходу до регулювання інформаційних відносин, який забезпечуватиме баланс між свободою інформації та необхідністю захисту національних інтересів і прав людини.

Список використаних джерел

1. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 20 січ. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
3. Кирилюк А. В. Поняття та види інформаційних правопорушень. Часопис цивілістики. 2017. № 3. С. 51-55. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/3b27acf8-2657-4ccd-b40b-56dbfcd141d9/content
4. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : станом на 8 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text
5. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
6. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері: навч. посіб. Київ: Нац. акад. СБУ. 2015. 175 с.
7. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
8. Жевелєва І. С. Кримінально правова кваліфікація правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. №4(91). С. 74-81. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/11/10-3.pdf
9. Марін О. Кримінальна відповідальність за зловживання в інформаційній сфері: постановка проблеми. Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове

регулювання. Матеріали VII Міжнародної науково-практичної конференції. Харків, 11 травня 2023 р. Харків: Право. 2023. С. 250-256. URL:https://www.academia.edu/download/104105192/Marin_Zlovzhyvannia_informac_sferi.pdf

10. Кодекс України про адміністративні правопорушення: Кодекс України від 07.12.1984 № 8073-X : станом на 1 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80732-10#Text
11. Глущенко Н., Головач А. Адміністративна відповідальність в інформаційній сфері. Молодий вчений. 2020. №11 (87). С. 286-289. URL: https://molodyivchenyi.ua/index.php/journal/article/view/204/198
12. Заярний О. А. Адміністративна караність правопорушень в інформаційній сфері: деякі проблеми доктринального визначення та законодавчого забезпечення. Адміністративне право і процес. 2014. №2 (8). С. 118-127. URL: file:///C:/Users/nesto/Downloads/429%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-727-1-10-20190422.pdf
13. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ: КВІЦ. 2019. 344 с.
14. Кодинець А. О. Підстави цивільної відповідальності за правопорушення у сфері інформаційних відносин: доктринальні засади та практичні наслідки. Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2018. №1(1). С. 58-61. URL:https://www.lj.journal.kspu.edu/index.php/lj/article/view/34/28
15. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 1 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text
16. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII : станом на 4 берез. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text
17. Бакало В. П. Загальні положення юридичної відповідальності військовослужбовців в умовах воєнного стану. Академічні візії. 2025. №50. С. 1-11. URL: https://www.academy-vision.org/index.php/av/article/view/2657/2510
18. Коба О. В. Військові правопорушення у контексті змісту загальної системи запобігання правопорушенням і злочинності. Аналітично-порівняльне правознавство. (2025. № 1. С.595-602. URL: https://app-journal.in.ua/wp-content/uploads/2025/02/101.pdf
19. Іванцов В., Бахмат В. Протидія дезінформації та пропаганді в умовах війни: роль медіа та соціальних мереж. Безпекова ситуація в Україні в умовах війни: стан, загрози, напрями забезпечення безпеки: матеріали Всеукраїнської наук.-практ. конференції (м. Київ, 27 вересня 2024 р.) [Редкол.: Вербенський М. Г., Опришко І. В., Лісниченко Л. В. та ін.]. Вінниця. 2024. 408 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/700df5a6-477e-416b-bf8f-62c97efd52ef/content
20. Дем'янюк Р. Новітні Європейські практики протидії інформаційним політичним маніпуляціям: можливості та проблеми запровадження в Україні. Науковий часопис Українського державного університету імені Михайла Драгоманова.. Політичні науки та методика викладання соціально-політичних дисциплін. 2025. № 22 (38). С. 100-114. URL: https://sj.udu.edu.ua/index.php/pnspd/uk/article/view/218/200