

УДК 34.004: 354.7 (477)

DOI <https://doi.org/10.24144/2788-6018.2025.01.78>

ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Кушнір І.П.,

доктор юридичних наук, доцент,
заступник начальника кафедри адміністративної діяльності
Національної академії Державної прикордонної служби України
імені Богдана Хмельницького
ORCID: 0000-0003-0286-7591

Адамчук С.В.,

кандидат наук з державного управління,
викладач кафедри адміністративної діяльності
Національної академії Державної прикордонної служби України
імені Богдана Хмельницького
ORCID: 0000-0003-4216-7397

Кушнір І.П., Адамчук С.В. Протидія дезінформації: організаційно-правовий аспект.

У статті проаналізовано поняття дезінформації крізь призму правового регулювання; як соціальне явище у сучасному інформаційному суспільстві.

Визначено, що дезінформація – це відомості, які не відповідають дійсності, котрі адресуються як широкому загалу, так і окремому адресату, спрямовані на зміну світогляду, виклик бажаної реакції та мають (відомості) негативний контекст. Констатовано, що невід’ємним супутником поширення дезінформації є мета, якої хоче досягти суб’єкт її поширення, як правило, може мати декілька завдань, найперше це введення в оману тих, кому вона транслюється (конкретній особі чи безособово), а далі зазвичай наступний результат, якого хотів досягти зловмисник – отримання персональних даних, зміна суспільної думки (очікувана реакція) в суспільстві під час проведення виборів, інформаційної війни, отримання доступу до фінансів тощо. Наголошено на тому, що дезінформація формується та поширюється умисно.

Важливим нормативно-правовим актом у сфері інформаційної безпеки і правового врегулювання окремих аспектів дезінформації є Стратегія інформаційної безпеки, прийнята Радою національної безпеки і оборони України, що визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних

Зроблено висновок, що дезінформація є неологізмом у сучасній правовій науці, і має негативну природу, мету та наслідки отриманого чи поширеного повідомлення. Запропоновано розглядати дезінформацію як інформацію (дані) чи повідомлення, яке повністю чи частково є неправдивим, перекрученим, взятим із контексту з негативною метою (може бути будь-що: психологічний вплив, зміна поведінки та думок суб’єкта впливу, отримання даних про банківські картки, коди доступу/паролі, отримання грошей, дестабілізації у суспільстві, дискредитація органів влади, тощо). Сформульовано, що протидія дезінформації залежить від багатьох чинників, у тому числі від: нормативно-правових, інституційних, організаційних, освітніх, принципової позиції населення України щодо бажання оволодіти навичками її розпізнання та недопущення впливу, психологічної стійкості, інформаційної гігієни тощо.

Ключові слова: дезінформація, інформаційна безпека держави, Стратегія інформаційної безпеки, інформаційні права людини та громадянина, протидія дезінформації, інформаційні загрози.

Kushnir I.P., Adamchuk S.V. Countering disinformation: organizational and legal aspect.

The article analyzes the concept of disinformation through the prism of legal regulation; as a social phenomenon in the modern information society.

It is determined that disinformation is information that is not true, which is addressed to both the general public and a specific addressee, aimed at changing the worldview, evoking the desired reaction and having a (known) negative context. It is stated that an integral companion to the dissemination of disinformation is the goal that the subject of its dissemination wants to achieve, which can usually have several objectives, first of all, misleading those to whom it is broadcast (a specific person or impersonally), and then usually the next result that the attacker wanted to achieve is obtaining

personal data, changing public opinion (expected reaction) in society during elections, information warfare, gaining access to finance, etc. It is emphasized that disinformation is formed and disseminated intentionally.

An important regulatory act in the field of information security and legal regulation of certain aspects of disinformation is the Information Security Strategy adopted by the National Security and Defense Council of Ukraine, which defines current challenges and threats to Ukraine's national security in the information sphere, strategic goals and objectives aimed at countering such threats, protecting the rights of individuals to information and personal data protection.

It is concluded that disinformation is a neologism in modern legal science and has a negative nature, purpose and consequences of the message received or disseminated. It is proposed to consider disinformation as information (data) or a message which is fully or partially false, distorted, taken out of context for a negative purpose (it can be anything: psychological influence, changing the behavior and opinions of the subject of influence, obtaining bank card data, access codes/passwords, obtaining money, destabilizing society, discrediting authorities, etc.) It is formulated that countering disinformation depends on many factors, including: regulatory, institutional, organizational, educational, principled position of the population of Ukraine regarding the desire to master the skills of recognizing and preventing its influence, psychological stability, information hygiene, etc.

Key words: disinformation, information security of the state, information security strategy, information rights of a person and a citizen, countering disinformation, information threats.

Постановка проблеми. Суспільство сьогодні стикається з такими негативними інформаційними явищами як маніпуляція, дезінформація, фейк, діпфейки, недостовірна інформація, інформаційний вплив, інформаційні операції, підміна (викривлення) фактів, негативна пропаганда тощо. Ключовим у цих явищах є інформація, використання або поширення якої може завдати шкоди інтересам особи, суспільства чи держави. Негативний прояв інформації зазвичай позначають терміном «дезінформація», яке в законодавстві не знайшло закріплення, разом з тим використовується в Стратегії інформаційної безпеки у контексті «дезінформаційні кампанії», «дезінформаційні (деструктивні) стереотипи», «протидія дезінформації», або уособлюється із «недостовірною інформацією». Формування інформаційної стійкості в українському соціумі, як ніколи, є актуальним в умовах сьогодення, зокрема для підвищення рівня інформаційної безпеки у протистоянні, як зовнішнім, так і внутрішнім загрозам. Саме тому назріла потреба у правовому аналізі поняття «дезінформація».

Стан опрацювання проблематики. Про специфічність, новизну та актуальність теми, піднятої у цій статті, свідчить наявність численних наукових публікацій котрі присвячені дезінформації. Зокрема, дезінформацію у розрізі сучасної її багатоаспектності проаналізували: О. Бучковська (протидія дезінформації як напрямок бібліотечної практики), Ю. Горбань і О. Олійник (медіаграмотність як чинник захисту інформаційного простору від ворожої дезінформації в час війни), О. Горун (протидія ворожій медіа-пропаганді в умовах правового режиму військового стану в Україні), Б. Гривнак, І. Лопушинський, І. Сапіжак (дезінформація як загроза національній безпеці України в умовах неоголошеної російсько-української війни), О. Звоздецька (дезінформація як загроза національній безпеці Європейського Союзу), А. Марущак (передумови для формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки: постановка проблеми), О. Панченко, В. Антонов (дезінформація в сучасних соціокультурних умовах інформаційної екосистеми), Л. І. Рудник (поширення недостовірної інформації як засіб ведення гібридних війн) Ю. Синиціною та С. Федоренко (можливості та виклики штучного інтелекту та виявлення дезінформації), Т. Павленко (дезінформація: поняття, ознаки, перспективи протидії), Т. Шлемкевич (дезінформація в інформаційному просторі України як виклик сьогодення) та інші. Водночас, варто засвідчити про відсутність комплексного дослідження, присвяченого організаційно-правовим аспектам протидії інформації.

Мета статті: дослідити правове регулювання та онтологічні засади дезінформації, сформулювати поняття цього явища, визначити особливості протидії дезінформації.

Виклад основного матеріалу. Дезінформація сьогодні стала реальністю через інформаційні загрози, інформаційні операції, гібридну війну, заходи інформаційного впливу, що ворог активно використовує проти населення України (особливо тих, які знаходяться на тимчасово окупованих територіях), своїх громадян та у світі; маніпулювання свідомістю. Для того, щоб будувати ефективну систему протистояння/протидії необхідно з'ясувати сутність й особливості цього явища.

Онтологічне сприйняття дозволяє з'ясувати сутність досліджуваного [1, с.73], зокрема «дезінформації». У такому контексті можливе пізнання досліджуваного терміну безвідносного сутнісного існування у суспільстві та з'ясувати проблеми з урахуванням сучасних динамічних процесів та зв'язків із різними інформаційними потоками.

Тлумачення терміну «дезінформація» (від фр. des – заперечення і information – повідомлення) [2] на даний час в законодавстві не відображено. У словниках його інтерпретують таким чином: свідоме поширення неправильної інформації, аби ввести в оману громадську думку, викликати певну реакцію в адресата; один з найпоширеніших засобів політичної пропаганди з певною антигуманною метою [3, 4].

неправдиві, навмисно перекручені відомості про які-небудь події, чийсь діяльність і т. ін. [5]. введення в оману недостовірною інформацією [6, 4].

Деінформація, пишуть Ю. Синиціна та С. Федоренко – «це поширення неправдивої або маніпульованої інформації з метою впливу на громадську думку» [7, с. 391]. Деінформація, зазначає Л. Рудник, «це неправдива, оманлива, маніпулятивна інформація, яку створили навмисне, аби отримати економічну, політичну або іншу вигоду» [8, с. 50].

Отже, дезінформація – це відомості, які не відповідають дійсності, котрі адресуються як широкому загалу, так і окремому адресату, спрямовані на зміну світосприйняття, виклик бажаної реакції та мають (відомості) негативний контекст.

Невід’ємним супутником поширення дезінформації є мета, якої хоче досягти суб’єкт (далі – зловмисник) її поширення, як правило, може мати декілька завдань, найперше – це введення в оману тих кому вона транслюється (конкретній особі чи безособово), а далі, зазвичай, наступний результат якого хотів досягти зловмисник – отримання персональних даних, зміна суспільної думки (очікувана реакція) в суспільстві під час проведення виборів, інформаційної війни, отримання доступу до фінансів тощо. Отже, дезінформація формується та поширюється умисно. З цього приводу Л.І. Рудник підкреслює, що «ключовою ознакою дезінформації, яка відрізняє її від звичайної недостовірної інформації – умисел на її створення. А у випадку, якщо умислу не було, то йдеться про неперевірену інформацію, яка виявилася недостовірною» [8, с. 50].

На рівні законодавчих актів термін «дезінформація», що має негативний прояв, як правило, необхідно розглядати в контексті забезпечення інформативної безпеки, або як її загрози.

Стаття 17 Конституції України покладає на державу обов’язок щодо недопущення деструктивного впливу дезінформації в межах її юрисдикції, а саме «...забезпечення інформаційної безпеки..» яка є однією із найважливіших функцій держави. Ряд статей Основного закону, так чи інакше стосуються убезпечення чи недопущення негативного впливу від інформації, зокрема статті 31, 32, 34, 40 тощо [9]. Закон України «Про інформацію» серед основних принципів інформаційних відносин закріплює «достовірність і повнота інформації» [10].

Важливим нормативно-правовим актом у сфері інформаційної безпеки і правового врегулювання окремих аспектів дезінформації стала Стратегія інформаційної безпеки (далі – Стратегія), яка була прийнята Радою національної безпеки і оборони України 15 жовтня 2021 року та затверджена Указом Президента України від 28 грудня 2021 року. Стратегія визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [11].

Ключовим у Стратегії є визначення інформаційної безпеки, у якій чітко зазначено її складові. Зокрема, акцентуємо увагу на тих, які безпосередньо стосуються предмету дослідження – це стан захищеності за якого належним чином забезпечуються:

конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації;

право людини на доступ до достовірної та об’єктивної інформації;

існування ефективної системи захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [11].

З урахуванням цього чотири з семи стратегічних цілей та напрямів реалізації Стратегії інформаційної безпеки стосуються протидії дезінформації:

Протидія дезінформації та інформаційним операціям, насамперед, держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини (Стратегічна ціль 1) [11]. Ця стратегічна ціль підкреслює рівень загрози незалежності України від інформаційних операцій та дезінформації, що спрямована від ворожої країни. І це не безпідставно, адже масштабність, цілеспрямованість та фінансове забезпечення такої операції російською федерацією (далі – рф) є досить потужною. Причому бюджет рф на фінансування інформаційної політики кожного року значно збільшується.

Підвищення рівня медіакультури та медіаграмотності суспільства. Українське суспільство повинне бути захищене від деструктивного впливу дезінформації та маніпулятивної інформації, а медіасередовище – бути соціально відповідальним і функціонувати стабільно. За таких умов українське суспільство зможе більш ефективно протистояти державі-агресору та залишатися стійким перед широким спектром загроз, зокрема в інформаційній сфері (Стратегічна ціль 3) [11]. Превентивні заходи щодо підвищення рівня інформаційної гігієни, у тому числі у віртуальному просторі, є потребою сучасного інформаційного суспільства та запорукою ефективної протидії деструктивному інформаційному впливу. Такі кроки дозволять сформувати стійкість до інформаційних загроз, мінімізувати вплив дезінформації, розуміти характер небезпеки, загалом виробити національний «інформаційний імунітет».

К.І. Беляков та І.М. Шопіна, впроваджуючи новий напрямку наукового дослідження, – «інформаційна гігієна» [12, с. 99], пропонують розглядати її як «проблемний напрямок інформаційної безпеки та культури людини в межах доктрини інформаційно-правових досліджень» [12, с. 118].

Забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів, гарантування їх безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту (Стратегічна ціль 4) [11]. Установлення меж приватності, зменшення обсягу поширення будь-якої інформації кожною особою мінімізує використання таких відомостей зловмисниками в деструктивних цілях.

Збереження приватного життя потребує розширення та деталізації механізму обробки та захисту інформації про особу, підвищення рівня інформаційної культури, як громадян, так і представників влади, посилення відповідальності за порушення інформаційної приватності, забезпечення громадян дієвими способами контролю за обробкою та доступом до їх персональних даних третіх осіб [13, с. 8; 14, с. 31].

Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору, а також відновлення їх права на інформацію, що дає їм змогу підтримувати зв'язок з Україною (в частині надання інформації, інформування громадян України, зокрема тих, які мешкають на тимчасово окупованих територіях, іноземної аудиторії про ситуацію на тимчасово окупованих територіях та дії України стосовно їх реінтеграції; спростування дезінформації, у тому числі ідеологем радянської та сучасної російської історіографії, щодо минулого і сучасного України та її територій, що нині є тимчасово окупованими державою-агресором, які поширюються в українських та іноземних засобах масової інформації (Стратегічна ціль 5) [11]. Грубе порушення рф норм міжнародного гуманітарного права, що стосується прав та свобод людини і громадянина на окупованій території потребують системного поступового підходу до їх відновлення.

Отже, основними напрямками інформаційної безпеки щодо протидії дезінформації є:
дотримання інформаційних прав громадян;
інформаційне протистояння державі-агресору;
підвищення рівня інформаційної культури (інформаційної гігієни [15, с. 84]).

Для ефективної протидії дезінформації в умовах інтенсивного розвитку цифрового суспільства, коли будь-яка інформація поширюється протягом декількох хвилин/годин, використання технологій штучного інтелекту для створення діпфейків, користувач Інтернету та/або соціальних мереж може опинитись в інформаційній ізоляції «інформаційній бульбашці». Для цього необхідне створення як правового, так і організаційного підґрунтя для розпізнання й недопущення деструктивного впливу неправдивої інформації на людину. Необхідність формування ефективних норм, методик та інструментів протидії дезінформації посилюється в умовах воєнного стану (гібридної війни) та здобуття перемоги над країною-агресором.

Ефективна протидія дезінформації повинна мати системний та комплексний характер, зокрема, нормативно-правове визначення дезінформації, формування векторів протидії загрозам, аналіз її проявів (загроз) як за певний період часу, так і в режимі реального часу й прогнозуванні подальшого поширення, прийняття рішень та вжиття заходів щодо недопущення її деструктивного масштабного поширення та впливу, створення освітніх програм (проектів), діяльність інституцій своєчасного реагування на такі інформаційні загрози тощо.

Протидія дезінформації, з урахуванням радянського минулого нашої країни, інколи викликає бажання у посадовців обмежити доступ до інформації, встановити контроль над засобами масової інформації. Такі спроби є не тільки незаконними, але й неефективними, адже новини поширюються різними інформаційними каналами – засобами масової інформації, телеграмканалами, а також соціальними мережами [16, с. 26]. Сьогодні кожен громадянин може бути джерелом масового

поширення інформації, а спроби контролювати або безпідставно обмежити розповсюдження інформації суперечить існуванню та розвитку демократичної європейської людиноцентрованої держави, й врешті частинам 1 і 2 статті 34 Конституції України, яка гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [9, ч. 1, 2 ст. 34]. Разом з тим, частина 3 згаданої вище статті дозволяє застосовувати обмеження цих прав у конкретно визначених випадках, інтересах чи для досягнення певної мети, а саме: в інтересах національної безпеки, територіальної цілісності, громадського порядку; з метою запобігання заворушенням чи злочинам; для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [9, ч. 3 ст. 34]. У такому випадку, обмеження повинні бути конституційними й достатньо обґрунтованими відповідно до зазначених умов.

З цього приводу О.Ю. Горун справедливо підкреслює, що «протидія інформаційним загрозам – завдання складне й досить делікатне. Втручання у сферу масових комунікацій потребує збереження балансу між захистом основ національної безпеки, з одного боку, та дотриманням стандартів свободи слова, з іншого. Будь-які рішення держави з питань інформаційної політики мають не лише спиратися на правову основу, а й бути суспільно легітимними» [17, с. 118].

Ініціатива щодо недопущення негативного інформаційного впливу не повинна виходити виключно від держави, сьогодні кожна свідомо людина має цікавитись актуальними інформаційними загрозами, як не допустити шкідливий інформаційний вплив, яким медіа довіряти, критичного сприйняття інформації. Зрештою це стосується особистої інформаційної безпеки. Для цього існують різні освітні платформи, компетентні органи (у тому числі державні), котрі попереджають про інформаційні операції та спростовують неправдиві повідомлення тощо.

Висновки. Отже, дезінформація є неологізмом у сучасній правовій науці, запозиченим з французької мови і має негативну природу, мету та наслідки отриманого чи поширеного повідомлення.

Пропонуємо розглядати дезінформацію, як інформацію (дані) чи повідомлення, яке повністю чи частково є неправдивим, перекрученим, взятим із контексту з негативною метою (може бути будь-що: психологічний вплив, зміна поведінки та думок суб'єкта впливу, отримання даних про банківські картки, коди доступу/паролі, отримання грошей, дестабілізації у суспільстві, дискредитація органів влади, тощо). Протидія дезінформації залежить від багатьох чинників, у тому числі від: нормативно-правових, інституційних, організаційних, освітніх, принципової позиції населення України щодо бажання оволодіти навичками її розпізнання та недопущення впливу, психологічної стійкості, інформаційної гігієни тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кушнір І.П. Теоретичні та організаційні засади нормативно-правового регулювання інформаційних відносин у діяльності Державної прикордонної служби України: дис... д-ра юрид. наук: 12.00.07. Київ, 2020. 566 с., с. 73.
2. Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism». Ronald Rychlak, Lt. Gen. Ion Mihai Pacepa. WND Books, 2013, pp. 428.
3. Толковий словник української мови. URL: <http://surl.li/eebxjb>.
4. Slovnyk.Me. URL: <http://surl.li/aelowd>.
5. Словник української мови online. Томи 1-14. URL: <http://surl.li/xthyix>.
6. Великий тлумачний словник сучасної української мови / уклад. та голов. ред. В.Т. Бусел. Київ; Ірпінь: Перун, 2005. VIII, 1728 с., с. 280.
7. Синиціна Ю., Федоренко С. Можливості та виклики штучного інтелекту та виявлення дезінформації. *Матеріали VIII Міжнародної науково-практичної конференції (ДДУВС, 15.03.2024)*. Частина II. С. 391-392.
8. Рудник Л.І. Поширення недостовірної інформації як засіб ведення гібридних війн. *Інформація і право*. 2024. № 4(51), с. 46–54.
9. Конституція України: Закон України від 28.06.1996. *Голос України*. 13.07.1996. № 128.
10. Про інформацію: Закон України від 2 жовтня 1992 року. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650, ст. 2.
11. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.
12. Права приватної особи в умовах пандемії COVID-19. / Є.О. Харітонов, О.І. Харітонова, К.І. Беляков та ін. Київ: Гельветика. 2020. С. 404.

13. Кушнір І.П. Актуальні питання забезпечення інформаційної приватності у діяльності Державної прикордонної служби України. *Конституційно-правові академічні студії*. 2020. № 1. С. 7–13.
14. Кушнір І.П., Адамчук С.В. Інформаційна приватність як право, закріплене Конституцією України: правові та соціальні аспекти. *Правова позиція*. 2023. № 1 (38). С. 27–31.
15. Беляков К.І. Інформаційна гігієна. Енциклопедія соціогуманітарної інформалогії / коорд. Проекту та заг. ред. проф.. К.І. Беляков. Одеса: Видавничий дім «Гельветика», 2021. Т. 2, с. 84–87.
16. Кушнір І.П., Адамчук С.В. Про VIBER та TELEGRAM канали як засоби поширення інформації крізь призму інформаційного законодавства України. *Правова позиція*. 2022. № 3 (36). С. 24–29.
17. Горун О.Ю. Протидія ворожій медіа-пропаганді в умовах правового режиму військового стану в Україні. *Інформація і право*. 2023. № 1 (44). С. 116–128.