УДК 351.862(477):004.9:32.019.5
DOI https://doi.org/10.32782/2312-1815/2025-21-6

Любомир Братах
ORCID: 0009-0005-8619-8576

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ДЕЗІНФОРМАЦІЙНОГО ВПЛИВУ: ЗАГРОЗИ, ВИКЛИКИ, МЕХАНІЗМИ РЕАГУВАННЯ

У статті розглянуто проблематику забезпечення інформаційної безпеки України в умовах посилення дезінформаційного впливу. Дезінформація використовується з метою дестабілізації внутрішньої ситуації, послаблення довіри до державної влади, маніпуляції громадською думкою та створення сприятливого середовища для зовнішнього впливу.

Увагу зосереджено на дослідженні національних і міжнародних підходів до формування системи реагування на дезінформаційні впливи, включно з правовими, інституційними та технологічними інструментами. Окремо розглянуто роль державної інформаційної політики та діяльності органів, відповідальних за захист інформаційного простору. Здійснено аналіз чинного нормативно-правового забезпечення інформаційної безпеки України та виявлено його сильні й слабкі сторони. Запропоновано низку рекомендацій щодо вдосконалення національної стратегії протидії дезінформації, зокрема через розвиток стратегічних комунікацій, підвищення рівня медіаграмотності населення, впровадження цифрової гігієни та налагодження ефективного міжвідомчого та міжнародного співробітництва.

Ключові слова: *інформаційна безпека, дезінформація, фейкові новини, стратегічні комунікації, медіаграмотність, цифрові загрози, інформаційна політика, національна безпека, нормативно-правове регулювання.*

Вступ. В умовах війни проти України інформаційний простір перетворився на своєрідне поле бою, де дезінформація прирівнюється до стратегічної зброї. Прокремлівська риторика спрямована на те, щоб впливати на свідомість громадян, деморалізуючи суспільство та знижуючи довіру до органів влади України. Масштабні дезінформаційні кампанії Росії увібрали в себе весь спектр новітніх засобів і технологій впливу. Серед них є як традиційна пропаганда, так і кібератаки, кампанії з використанням штучного інтелекту і deepfake, що дещо ускладнює їхнє виявлення та нейтралізацію, особливо серед старшого покоління, малознайомого з технологіями.

Інформаційна безпека становить вагому частку системи національної безпеки України та є важливим аспектом, що забезпечує стійкість держави під час війни. Вона охоплює не лише захист інформаційного простору від зовнішніх загроз, а й формування внутрішньої спроможності суспільства протистояти маніпуляціям. Саме тому дослідження загроз, викликів і механізмів реагування на дезінформаційний вплив набуває особливого значення в контексті сучасних трансформаційних процесів та європейської інтеграції України.

Аналіз останніх досліджень і публікацій. Серед наукових праць, спрямованих на дослідження інформаційної безпеки, можна виокремити праці таких науковців, як Леоненко Н., Поступна О., Ільницька У., Крап А., Петрик В., а також дослідження Мазуренко Л., де розглядаються інформаційні виклики в месенджерах і загроза маніпуляції суспільством.

Методи дослідження. Для оптимізації дослідження слід виділити такі методи дослідження: емпіричний, порівняльний, системний, кейс-стаді та структурно-функціональний

методи. Велика частина праць, написаних за цією тематикою, глибше розкривають поняття маніпуляції, протистояння маніпуляціям, технології використання пропаганди та запровадження нових правових форм контролю, тому актуальність і практичність цієї тематики є затребуваною в науковій літературі.

Мета дослідження – аналіз характеру дезінформаційного впливу на загрози інформаційній безпеці України, окреслення основних викликів, а також обґрунтування ефективних механізмів реагування на інформаційний впливи.

Результати й обговорення. Інформаційна безпека становить невід'ємну частину національної безпеки та розглядається як одна з ключових функцій держави. Вона поєднує в собі два взаємозалежні аспекти: забезпечення громадянам доступу до повної, достовірної та різноманітної інформації, а також захист інформаційного простору від загроз дезінформації. З одного боку, це означає підтримку свободи інформації та прозорості, з іншого – необхідність запобігання інформаційним маніпуляціям, психологічному тиску, пропаганді та спробам підриву суспільної єдності. Безпека насамперед передбачає конфіденційність інформації, цілісність та доступність компонентів і ресурсів системи. Ефективне впровадження контролю за інформаційним простором і боротьбою з дезінформацією допоможе отримувати якісну достовірну інформацію і викреслити проблемні виклики, які вона несе [6, с. 35–36].

На тлі технологічних і геополітичних перетворень інформація стала вагомим ресурсом, завдяки якому держава, суспільство чи окремий індивід може посилити свої позиції або нав'язати власні погляди як у країни, так і на міжнародній арені.

Ключовою особливістю інформації на сьогодні є швидкість її поширення. Якщо кілька десятиліть або століть тому передача відомостей здійснювалася переважно через друковані видання, поштовий зв'язок чи в усній формі, що займало значний проміжок часу, то сьогодні завдяки цифровим технологіям, інтернету та соціальним мережам інформація поширюється миттєво, охоплюючи мільйони людей у різних куточках світу.

Наразі інформація зачіпає всі сфери життєдіяльності людини, що дає змогу напряму впливати на процеси всередині раїни, а в окремих випадках інформаційний вплив на країну можна прирівняти до інформаційної війни. Незалежно від її змісту та контексту, інформація несе потенційну загрозу, тому питанням її регулювання та забезпечення інформаційної безпеки в Україні займалися В. Горбулін, Г. Почепцов, В. Ліпкан ще в 1990-х – на початку 2000-х. Саме їх праці заклали теоретико-правові та комунікативні основи інформаційної безпеки.

Інформаційна безпека є одним із ключових елементів під час військових дій. Випадково чи умисно неправильно подана чи помилкова інформація негативно впливає на настрої в суспільстві, перебіг подій, погіршує імідж політичного та військового керівництва. Таким чином, боротьба з поширенням шкідливої інформації під час війни має істотне значення для перебігу воєнного конфлікту [16, с. 52–53].

Проблема забезпечення інформаційної безпеки в сучасному світі, особливо для України, має особливе значення, враховуючи вторгнення РФ на територію України та постійні морально-підривні та інформаційно-психологічні атаки проти України. Подібний дискредитаційний характер дій агресора має на меті позбавлення України її стратегічних союзників у країнах НАТО та створення перешкод для просування національних інтересів нашої країни у світі. Агресивні дії Росії проти України спричинили руйнування не лише української чи європейської, а й глобальної безпеки. Сам російсько-український конфлікт розкрив недоліки системи інформаційної безпеки не лише в регіоні, а й в глобальному вимірі. Аспекти, які б мали бути використані для захисту національних інтересів, протидії дезінформаційним кампаніям і зміцнення кіберстійкості держав, на практиці виявилися недостатньо розвиненими або фрагментарними. Це стосується як відсутності комплексних стратегій реагування, так і браку координації між національними та міжнародними інституціями, що створює додаткові вразливості

у світовому інформаційному просторі. Оскільки російська машина використовує проти України не лише військову силу на фронті, а й терор мирного населення ракетами та дронами, міжнародну дипломатію, економічні засоби та інформаційний вплив, термін «гібридна війна» найбільш підходяще описує специфіку дій агресора [8, с. 53–55].

В умовах гібридної агресії проти України поруч із військовим і дипломатичним фронтом, інформаційна сфера стала однією з головних точок протистояння ворогу. В інформаційній сфері виділяють внутрішні та зовнішні загрози. Зовнішні загрози переважно пов'язані з цілеспрямованим інформаційним впливом Росії, що реалізується через масштабні пропагандистські операції, створення фейкових новинних ресурсів, використання бот-мереж і новітніх технологій (deepfake). Наприклад, компанія Doppelgänger створює копії медіа (Le Monde, Fox News), поширюючи фейкові антиукраїнські наративи [19]. Внутрішні загрози зумовлені низьким рівнем медіаграмотності частини населення, що супроводжується широким поширенням пропаганди не тільки з-за кордону, але й з боку політичних опонентів, блогерів, активістів, які не мають зловмисних намірів, але підсилюють суспільні суперечності. Варто виділити і поширення анонімних джерел у цифровому середовищі, а також політичну поляризацію, яка створює сприятливе підґрунтя для маніпуляцій. Так, платформа **Telegram** використовується громадянами для новин, проте водночас слугує каналом для анонімної дезінформації [23]. У цих умовах інформаційна безпека України стає визначальним фактором стійкості держави, а дослідження механізмів реагування на дезінформаційний вплив є одним із пріоритетних напрямів наукових і практичних пошуків [16, с. 54–55].

Сучасні цифрові технології та соціальні мережі дають змогу миттєво поширити будь-яку новину (у тому числі фейкову або спотворену). У подібних умовах ключовими є механізм перевірки подібного контенту на достовірність та інформаційна грамотність населення. Однак банальна перевірка інформації займає певний час, а деяка інформація потребує технічної комплексної перевірки спеціалістами, до того ж, зважаючи на швидкість поширення інформації, навіть викривши дезінформацію чи фейк, все одно буде нанесено дипломатичну, економічну чи морально психологічну шкоду населенню і країні загалом. Подібні інформаційні атаки є однією з причин загострення політичного протистояння в країні, що сприяє ослабленню демократичних інституцій, впливають на громадян і державні структури, ускладнюючи ухвалення рішень [11]. До загроз інформаційній безпеці України можна віднести дезінформацію, пропаганду, фейкові новини, кібератаку, цифрове шпигунство та ін.

Дезінформація. Алгоритми штучного інтелекту здатні миттєво поширювати неправдиву інформацію, яка підриває довіру до інституцій, руйнує політичні процеси та провокує соціальні заворушення. Росія активно застосовує дезінформаційні кампанії для підриву морального духу населення, дестабілізації ситуації та послаблення довіри до влади [11]. Прикладом є кампанія 2022 року, коли масово поширювалися фейки про «швидку капітуляцію України», «евакуацію влади з Києва» чи «розпад Збройних Сил». У 2023 році розповсюджувалися фальшиві повідомлення про «зраду» українського керівництва під час боїв за Бахмут, а у 2024 році – кампанія дезінформації про «недопоставки західної зброї» та «корупційні схеми» у військовій допомозі, що було спрямовано на підрив довіри партнерів і зниження рівня міжнародної підтримки [15].

Пропаганда. Системна пропаганда спрямована на спотворення образу України у світовому інформаційному просторі. Використовуючи соціальні мережі та цифрові платформи, зловмисники поширюють фейки, експлуатують наративи про «фашистську Україну» чи «звільнення від націоналістів», формуючи панічні настрої, розколюючи суспільство й дискредитуючи владу. З 2022 року Кремль активно використовує свої медіаресурси та соціальні мережі для поширення меседжів про «неіснування української нації» та «легітимність російського вторгнення». Складні кампанії, зокрема відомий проєкт Doppelganger, використовували AI-генерований контент для створення фейкових новинних сайтів, коментарів і соцмережевих

публікацій різними мовами для просування російських наративів щодо війни. Частину цих операцій виявила компанія OpenAI у 2024 році [20].

Фейкові новини. Як навмисно сфабрикована інформація, фейки поширюються через месенджери, соціальні мережі й онлайн-платформи. Вони спрямовані на маніпулювання громадською думкою, дискредитацію політичних опонентів і створення паніки. У контексті війни такі повідомлення стали частиною гібридної агресії, яка дає змогу дистанційно управляти суспільними настроями [16, с. 53–56].

Deepfakes. Технології глибокої підробки дають змогу створювати реалістичні аудіо- та відеофайли, які важко відрізнити від справжніх. Вони використовуються для маніпуляцій, шантажу та дискредитації політичних лідерів, що підриває довіру до інформаційних джерел і ускладнює захист інформаційної безпеки. У березні 2022 року Центр стратегічних комунікацій попередив про можливе поширення deepfake-відео, на якому президент Зеленський нібито закликає скласти зброю. Справді, 16 березня з'явився підроблений ролик на Facebook, YouTube, Telegram, швидко видалений після реакції влади та платформ [17].

Кібератаки є одним із найнебезпечніших інструментів сучасної інформаційної війни. Вони здійснюються з метою порушення функціонування державних і приватних інформаційних систем, крадіжки конфіденційних даних або блокування доступу до важливої інфраструктури [7, с. 22–23]. Найбільш поширеними є атаки типу *DDoS*, які спрямовані на перевантаження серверів і тимчасове виведення їх з ладу, що паралізує роботу державних установ, банків, ЗМІ чи транспортних систем. У грудні 2024 року надважлива атака на реєстри держави (включно з порталом «Дія») вивела з ладу сервіси Мін'юсту; відповідальність за хакерську операцію взяла на себе група XakNet Team [18].

Фішингові атаки становлять особливу небезпеку через використання соціальної інженерії. Зловмисники створюють підроблені вебсайти або електронні листи, які зовні ідентичні офіційним, з метою отримання паролів, банківських реквізитів чи персональних даних громадян. В умовах війни такі атаки часто маскуються під «повідомлення від банку», «оновлення від державних сервісів» або «інструкції щодо безпеки», що збільшує ризик їхньої успішності. Восени 2023 року CERT-UA зафіксував використання PDF-файлів із посиланнями, що встановлювали шпигунське або знищувальне ПЗ, – PicassoLoader, njRAT, RoarBAT (UAC-0165 / Sandworm) [22].

Цифрове шпигунство є цілеспрямованою діяльністю, яка використовується проти державних органів, військових структур і стратегічно важливих корпорацій. Воно може передбачати встановлення шпигунського програмного забезпечення, приховане спостереження за електронною поштою, перехоплення переговорів або злам захищених каналів зв'язку. Здобута інформація використовується для політичного тиску, економічних диверсій чи підготовки військових операцій. У травні 2025 року російське ГРУ (група APT28 / Fancy Bear) здійснювало масштабне проникнення в системи спостереження вздовж кордону, зокрема залізничні станції та митні переходи. Було скомпрометовано понад 10 000 камер відеоспостереження, що використовувалися для відстеження логістики допомоги Україні, як кадри, так і пересилання вантажів [21].

Злом баз даних має не менш руйнівний характер, адже може призвести до масштабного витоку персональної, фінансової чи службової інформації. Такі дані часто використовуються на чорному ринку для шахрайства, підробки документів чи вербування агентури. Для держави подібні витоки можуть спричинити серйозні ризики – від підриву довіри громадян до інституцій до загроз національній безпеці. Особливу небезпеку становить злам баз критичної інфраструктури, оскільки він може паралізувати цілі галузі – енергетику, транспорт чи банківську систему. Влітку 2023 року групи Sandworm (UAC-0165) використали скриптовий віпер RoarBAT та макрос-навантажувачі PicassoLoader для знищення або витоку файлів у держорганах [22].

Штучний інтелект. Попри потенціал для створення систем кіберзахисту, він активно використовується зловмисниками. Алгоритми машинного навчання допомагають виявляти

вразливості, адаптувати атаки та створювати шкідливе програмне забезпечення. Особливу небезпеку становить автоматизація шпигунства й цілеспрямованих атак, що посилює загрози для національної безпеки [14, с. 163–164]. У 2023 році дослідники виявили мережі акаунтів, що використовували нейромережі для масового створення контенту на кшталт «новинних сайтів», які поширювали російські наративи англійською та німецькою мовами. Водночас Україна і партнери також застосовують ШІ для виявлення ботів, розпізнавання підробленого контенту й оперативного реагування на інформаційні атаки. Російсько спрямовані кампанії використовували інструменти штучного інтелекту для генерації коментарів, постів, статей і створення фейкових акаунтів на платформах X (Twitter), Facebook, Telegram тощо [20].

Міністерство внутрішніх справ України виконує важливу роль у боротьбі з кіберзлочинністю. Воно здійснює розслідування та вживає превентивні заходи для протидії кіберзагрозам, а також активно співпрацює з внутрішніми та зовнішніми партнерами для забезпечення безпеки в інформаційному середовищі.

Рада національної безпеки та оборони України є головним органом, що визначає стратегічні напрями у сфері безпеки й оборони країни, зокрема в питаннях інформаційної безпеки. Вона враховує національні інтереси й актуальні загрози, що виникають через геополітичні та технологічні зміни.

Комітет з питань національної безпеки та оборони Верховної Ради України виступає законодавчим органом, який формує та вдосконалює правову базу у сфері інформаційної безпеки. Усі ці структури взаємодіють для забезпечення суверенітету країни у цифровому просторі та впровадження ефективних заходів щодо захисту національних інтересів [12, с. 18–20].

Під час побудови механізмів захисту інформаційної безпеки та протидії дезінформаційному впливу потрібно також враховувати психологічний вплив на громадян. Механізмами захисту від психологічних наслідків інформаційних загроз мають виступати такі інструменти: гарантування свободи слова, забезпечення незалежності засобів масової інформації та свободи друку. Водночас діяльність медіа повинна бути спрямована на підтримку національних інтересів і безпеки держави. Важливо, щоб органи державної влади систематично акцентували увагу журналістів і населення на відповідальність за поширення свідомо неправдивої або маніпулятивної інформації.

Окремим елементом забезпечення інформаційно-психологічної безпеки є блокування прихованого шкідливого інформаційного впливу, зокрема через заборону ресурсів, що можуть використовуватися для пропаганди чи збору даних. Показовим прикладом стало обмеження у 2017 році доступу до російських сервісів «VK» та «Одноклассники», що стало особливо важливим кроком для захисту жителів фронтових і прифронтових територій від інформаційних маніпуляцій [16, с. 55–56].

Для ефективного захисту потрібне поєднання технічних рішень, правового регулювання та міжнародної співпраці. Важливими заходами є удосконалення технологій кіберзахисту, гармонізація законодавства з міжнародними нормами, впровадження багаторівневої автентифікації, модернізація інфраструктури та підвищення медіаграмотності населення. Формування культури інформаційної безпеки, розвиток критичного мислення та відповідального користування цифровими технологіями є ключем до стійкості суспільства перед сучасними викликами.

На сьогодні проведено багато досліджень щодо маніпуляцій у медіапросторі, впливу інформації на населення та використання інформації як аспекту «гібридної війни». Так, Карп А. у своїй роботі є досліджує дезінформацію як загрозу демократії та державному управлінню, зокрема в контексті війни в Україні. Автор акцентує увагу на впливі дезінформації на суспільно-політичні процеси, механізми її поширення й оцінці ефективності існуючих стратегій протидії інформаційним маніпуляціям [11]. Галіпчак В., зі свого боку, акцентує увагу на важливості освіти та підвищення інформаційної грамотності суспільства, щоб громадяни були здатні розпізнавати й реагувати на дезінформацію [7, с. 22–23].

Значну частку в системі інформаційної безпеки України займає система правового регулювання інформаційної безпеки. Вона являє собою масив правових норм, які регулюють відносини в цій галузі та відповідні акти правозастосовного характеру [13, с. 44–46].

Законодавча база складається з Конституції України як основного закону держави, що закріплює право громадян на свободу слова та доступ до інформації [1], Закону України «Про інформацію», що визначає основні принципи інформаційних відносин, права й обов'язки суб'єктів інформаційної діяльності [2], Закону України «Про основні засади забезпечення кібербезпеки України», що визначає інституційну систему захисту від кіберзагроз, тісно пов'язаних із дезінформаційними атаками [3], Стратегії інформаційної безпеки України, що визначає цілі, завдання та пріоритети державної політики у сфері протидії дезінформації, пропаганді та кіберзагрозам [4], Доктрини інформаційної безпеки України, що передбачає комплекс заходів щодо формування державної політики протидії інформаційним загрозам [5].

Таким чином, нормативно-правова база у сфері інформаційної безпеки України є комплексною та містить як національні закони, так і стратегії, що визначають принципи захисту інформаційного простору, протидії кібератакам і дезінформації, а також регулюють взаємодію державних органів, приватного сектора та громадянського суспільства в забезпеченні інформаційної безпеки [16, с. 51–53].

Для ефективної протидії дезінформації та інформаційному впливу в Україні потрібно розвивати комплексний підхід, який охоплює кілька важливих сфер. Насамперед важливо вдосконалити інформаційне забезпечення зовнішньополітичного курсу України та створити умови для протидії дезінформації за кордоном. Це передбачає розробку стратегій для посилення міжнародного інформаційного впливу, а також удосконалення методів боротьби з порушенням прав громадян та юридичних осіб на території РФ [8, с. 55–58].

Ключовим елементом є підвищення медіаграмотності серед населення, що дасть змогу громадянам краще орієнтуватися у величезному потоці інформації, критично ставитися до медіа та визначати маніпуляції. Важливою складовою цього є розробка методик, що сприятимуть формуванню критичного мислення серед громадян, здатності розпізнавати фейки та інші загрози [11]. Іншим важливим кроком є активна боротьба з фейковою інформацією через фактчекінг, медіамоніторинг і правове регулювання інформаційного простору [11]. Потрібно посилити контроль за поширенням маніпулятивного контенту, запровадивши кримінальну відповідальність за створення та поширення дезінформації, особливо в умовах війни. Також слід впровадити механізми контролю за фейковими акаунтами й анонімними джерелами, які поширюють неправдиву інформацію в інтернеті.

Інформаційна безпека держави також передбачає активне використання кіберзахисту. Потрібно створити належну технічну базу для боротьби з кібератаками та дезінформацією в кіберпросторі. Для цього важливо забезпечити взаємодію між різними державними та приватними структурами, зокрема в рамках Ситуаційного центру кібербезпеки при СБУ. Виявлення фейкових новин і діпфейків потребує мобілізації спеціальних підрозділів у сфері кіберполіції та співпраці з громадськими ініціативами, як-от «КіберАрмія», для протидії інформаційним атакам з боку ворога [16, с. 55–56].

Загалом для успішної боротьби з дезінформацією важливо об'єднати зусилля держави, медіа, громадських організацій та міжнародних партнерів, активно впроваджуючи нові технології та методи для запобігання маніпуляціям і захисту національних інтересів.

Висновки. Інформаційна безпека є складовою системи національної безпеки України та важливим аспектом, що забезпечує стійкість держави під час війни.

Україна стикається з комплексним викликом: дезінформація сьогодні є не лише інформаційною загрозою, а й стратегічною зброєю. Вона впливає на мораль, внутрішню єдність, а також на міжнародну підтримку. Однією з основних загроз є недостатній рівень кібербезпеки,

що може призвести до масштабних кібератак, здатних зруйнувати інфраструктуру країни або вивести з ладу важливі системи доступу до конфіденційної інформації. Для вирішення цих проблем потрібно здійснити низку заходів, включно з удосконаленням законодавства щодо свободи та незалежності медіа, покращенням кібербезпеки, розвитком медіакультури серед населення та підтримкою незалежних ЗМІ.

Для ефективного забезпечення інформаційної безпеки країни необхідна активна співпраця уряду, громадян і міжнародних партнерів. Сучасні виклики та загрози потребують постійної готовності до інновацій та вдосконалення механізмів протидії інформаційним агресіям, що особливо актуально в умовах війни. Захист національного інформаційного простору та боротьба з ворожими маніпуляціями стають пріоритетними завданнями для збереження суверенітету й розвитку держави.

Аналізуючи важливість інформаційної безпеки під час бойових дій, можна стверджувати, що дезінформація може значно впливати на моральний стан населення, викликати паніку та дестабілізувати ситуацію. Вона здатна спричиняти соціальні потрясіння й посилювати негативні наслідки для Збройних Сил України. Для ефективної протидії інформаційній агресії важливо залучати міжнародні організації та активно співпрацювати з міжнародною спільнотою. В умовах сучасної інформаційної війни не існує кордонів, тому захист відкритого інформаційного простору країни є важливим кроком для відсічі ворожим впливам і маніпуляціям.

Література:

1. Конституція України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. С. 141.

2. Про інформацію : Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*. № 48. С. 650.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. С. 403.

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента від 28.12.2021 № 685/2021 URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України : Указ Президента від 25.02.2017 № 47/2017 URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text.

6. Босак І. Інформаційна безпека України: загрози та методи протидії. *Київський економічний науковий журнал*. 2025. № 9. С. 33–38. Режим доступу: https://doi.org/10.32782/2786-765X/2025-9-4.

7. Галіпчак В. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. *Науковий журнал «Політикус».* 2023. № 5. С. 19–24.

8. Запорожець С. Інформаційна безпека України в умовах гібридної війни. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. 2019. № 17. С. 52–63. URL: https://doi.org/10.46972/2076-1546.2019.17.05.

9. Кобець Т. Аналіз загроз когнітивній безпеці українського суспільства: класифікаційні підстави. 2024. С. 67–72. URL: https://journals.pnu.if.ua/index.php/politology/article/view/182/178.

10. Кочубей Л., Некряч А. Державна інформаційна політика України в умовах євроінтеграції. *Публічне управління і політика*. 2025. № 4 (8). С. 1–9. URL: https://www.researchgate.net/publication/391834174_DERZAVNA_INFORMACIJNA_POLITIKA_UKRAINI_V_UMOVAH_EVROINTEGRACIISTATE_INFORMATION_POLICY_OF_UKRAINE_IN_THE_CONTEXT_OF_EUROPEAN_INTEGRATION.

11. Крап А. Дезінформація як загроза демократії та державному управлінню. *Український політико-правовий дискурс*. 2025. № 9. URL: https://zenodo.org/records/15108404.

12. Лісовський О. Кібербезпека та інформаційна війна: виклики та загрози. Львів : Магнолія, 2021. С. 16–23.

13. Новицька Н. Правове забезпечення інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2009. № 1. С. 44–47.

14.Шевчук М. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Актуальні проблеми вітчизняної юриспруденції.* 2024. № 6. С. 160–166. URL: http://www.apnl.dnu.in.ua/6_2024/6_2024.pdf#page=160.

15.Понад 40 % повідомлень про корупцію та боротьбу з нею є дезінформацією – результати моніторингу соцмереж у серпні. URL: https://nazk.gov.ua/uk/ponad-40-povidomlen-pro-koruptsiyu-ta-borotbu-z-neyu-e-dezinformatsieyu-rezultaty-monitoryngu-sotsmerezh-u-serpni.

16.Mazurenko L. Information security in the terms the Russian-Ukrainian war: challenges and threats. 2022. № 42. С. 50–57. URL: https://doi.org/10.26565/2220-8089-2022-42-08.

17.A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be. URL: https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.

18.Cyber Security Week in Review: December 20, 2024. URL: https://www.cybersecurity-help.cz/blog/4482.html?utm_source=chatgpt.com.

19.Doppelganger (disinformation campaign) URL: https://en.wikipedia.org/wiki/Doppelganger_%28disinformation_campaign%29.

20.OpenAI identified five influence operations in Russia, China, Iran, and Israel using its tools to manipulate public opinion. URL:https://time.com/6983903/openai-foreign-influence-campaigns-artificial-intelligence/.

21.Russia accused of trying to hack border security cameras to disrupt Ukraine aid. URL: https://www.theguardian.com/world/2025/may/21/russia-accused-trying-disrupt-aid-ukraine-hacking-border-crossings?utm_source=chatgpt.com.

22.The Russia/Ukraine war is approaching its second year, and both physical and cyber warfare continue. URL: https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023.

23.Ukrainian authorities are worried about online disinformation. URL: https://www.lemonde.fr/en/international/article/2024/04/18/ukrainian-authorities-are-worried-about-online-disinformation_6668838_4.html.

References:

1. Konstytutsiia Ukrainy: Zakon Ukrainy [Constitution of Ukraine: Law of Ukraine] (1996, June 28). *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine.* No. 254k/96-VR. P. 141 [in Ukrainian].

2. Pro informatsiiu: Zakon Ukrainy. [About information: Law of Ukraine] (1992, October 02). *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine*. No. 2657-XII. P. 650 [in Ukrainian].

3. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy [On the basic principles of ensuring cybersecurity in Ukraine: Law of Ukraine] (2017, October 05). *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of Verkhovna Rada of Ukraine*. No. 2163-VIII. P. 403 [in Ukrainian].

4. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku "Pro Stratehiiu informatsiinoi bezpeky": Ukaz Prezydenta [On the decision of the National Security and Defense Council of Ukraine of October 15, 2021 "On the Information Security Strategy": Decree of the President] (2021, December 28). No. 685/2021. Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].

5. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku "Pro Doktrynu informatsiinoi bezpeky Ukrainy": Ukaz Prezydenta [On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "About the Information Security Doctrine of Ukraine": Decree of the President] (2017, January 25). No. 47/2017. Retrieved from: https://zakon.rada.gov.ua/laws/show/47/2017#Text [in Ukrainian].

6. Bosak, I. (2025). Informatsiina bezpeka Ukrainy: zahrozy ta metody protydii [Information security of Ukraine: threats and methods of counteraction]. *Kyivskyi ekonomichnyi naukovyi zhurnal*, 9, 33–38. Retrieved from: https://doi.org/10.32782/2786-765X/2025-9-4 [in Ukrainian].

7. Halipchak, V. (2023). Derzhavno-pravovyi mekhanizm informatsiinoi bezpeky Ukrainy v umovakh rosiiskoi ahresii [State and legal mechanism of information security of Ukraine in conditions of Russian aggression] [in Ukrainian].

8. Zaporozhets, S. (2019). Informatsiina bezpeka Ukrainy v umovakh hibrydnoi viiny [Information security of Ukraine in the context of hybrid warfare]. *Problemy stvorennia, vyprobuvannia, zastosuvannia ta ekspluatatsii skladnykh informatsiinykh system*, 17, 52–63. Retrieved from: https://doi.org/10.46972/2076-1546.2019.17.05 [in Ukrainian].

9. Kobets, T. (2024). Analiz zahroz kohnityvnii bezpetsi ukrainskoho suspilstva: klasyfikatsiini pidstavy [Analysis of threats to the cognitive security of Ukrainian society: classification grounds]. P. 67–72. Retrieved from: https://journals.pnu.if.ua/index.php/politology/article/view/182/178 [in Ukrainian].

10. Kochubei, L., Nekriach, A. (2025). Derzhavna informatsiina polityka Ukrainy v umovakh yevrointehratsii [State information policy of Ukraine in the context of European integration]. *Public administration and politics*, 4 (8), 1–9. Retrieved from: https://www.researchgate.net/publication/391834174_DERZAVNA_INFORMACIJNA_POLITIKA_UKRAINI_V_UMOVAH_EVROINTEGRACIISTATE_INFORMATION_POLICY_OF_UKRAINE_IN_THE_CONTEXT_OF_EUROPEAN_INTEGRATION [in Ukrainian].

11. Krap, A. (2025). Dezinformatsiia yak zahroza demokratii ta derzhavnomu upravlinniu [Disinformation as a threat to democracy and public administration]. *Ukrainian political and legal discourse*. P. 9. Retrieved from: https://zenodo.org/records/15108404 [in Ukrainian].

12. Lisovskyi, O. (2021). Kiberbezpeka ta informatsiina viina: vyklyky ta zahrozy [Cybersecurity and information warfare: challenges and threats]. Lviv. P. 16–23 [in Ukrainian].

13. Novytska, N. (2009). Pravove zabezpechennia informatsiinoi bezpeky [Legal support for information security. Information security of man, society, state]. Vol. 1. P. 44–47 [in Ukrainian].

14. Shevchuk, M. (2024). Suchasni vyklyky i zahrozy v sferi informatsiinoi bezpeky derzhavy [Modern challenges and threats in the field of state information security]. *Aktualni problemy vitchyznianoi yurysprudentsii*, 6, 160–166. Retrieved from: http://www.apnl.dnu.in.ua/6_2024/6_2024.pdf#page=160 [in Ukrainian].

15. Ponad 40% povidomlen pro koruptsiiu ta borotbu z neiu ye dezinformatsiieiu – rezultaty monitorynhu sotsmerezh u serpni [Over 40% of messages about corruption and the fight against it are disinformation – results of social media monitoring in August]. Retrieved from: https://nazk.gov.ua/uk/ponad-40-povidomlen-pro-koruptsiyu-ta-borotbu-z-neyu-e-dezinformatsieyu-rezultaty-monitoryngu-sotsmerezh-u-serpni [in Ukrainian].

16. Mazurenko, L. (2022). Information security in the terms the Russian-Ukrainian war: challenges and threats. No. 42. P. 50–57. URL: https://doi.org/10.26565/2220-8089-2022-42-08.

17. A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be. Retrieved from: https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.

18. Cyber Security Week in Review: December 20, 2024. Retrieved from: https://www.cybersecurity-help.cz/blog/4482.html.

19. Doppelganger (disinformation campaign) Retrieved from: https://en.wikipedia.org/wiki/Doppelganger_%28disinformation_campaign%29.

20. OpenAI identified five influence operations in Russia, China, Iran, and Israel using its tools to manipulate public opinion. URL:https://time.com/6983903/openai-foreign-influence-campaigns-artificial-intelligence/.

21. Russia accused of trying to hack border security cameras to disrupt Ukraine aid. Retrieved from: https://www.theguardian.com/world/2025/may/21/russia-accused-trying-disrupt-aid-ukraine-hacking-border-crossings.

22. The Russia/Ukraine war is approaching its second year, and both physical and cyber warfare continue. Retrieved from: https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023.

23. Ukrainian authorities are worried about online disinformation. Retrieved from: https://www.lemonde.fr/en/international/article/2024/04/18/ukrainian-authorities-are-worried-about-online-disinformation_6668838_4.html.

Liubomyr Bratakh. Formation of the state information policy of Ukraine in the context of rapprochement with the European Union

The article examines the issues of ensuring information security in Ukraine in the context of increasing disinformation influence. Disinformation is used to destabilize the internal situation, weaken trust in state authorities, manipulate public opinion, and create a favorable environment for external influence. The focus is on the study of national and international approaches to the formation of a system of response to disinformation influences, including legal, institutional and technological tools. The role of state information

policy and the activities of bodies responsible for the protection of the information space are separately considered. An analysis of the current regulatory and legal framework for information security in Ukraine was carried out and its strengths and weaknesses were identified. A number of recommendations are proposed to improve the national strategy for countering disinformation, in particular through the development of strategic communications, increasing the level of media literacy of the population, implementing digital hygiene, and establishing effective interagency and international cooperation.

Key words: *information security, disinformation, fake news, strategic communications, media literacy, digital threats, information policy, national security, regulatory framework.*

Відомості про автора:
Братах Любомир – аспірант кафедри політичних наук,
Карпатський національний університет імені Василя Стефаника.

Надійшла 11.08.2025
Прийнята 02.08.2025
Опублікована 30.10.2025