**УДК 34:316.77-049.5**

**Д.М. Шебаніц,**
**Д.А. Тріфонов**

# ІНФОРМАЦІЇ ЯК СУЧАСНА ЗБРОЯ: НАЦІОНАЛЬНА ТА МІЖНАРОДНА ПРАКТИКА ПРОТИДІЇ

*Дана стаття присвячена визначенню ролі інформації як ключового інструменту сучасних воєн і гібридних конфліктів, а також правовому регулюванню інформаційної безпеки в умовах військових дій.*

*У дослідженні проаналізовано функціонування інформації як об'єкта правової охорони та як засобу впливу в умовах збройного конфлікту. Особлива увага приділена вивченню психологічних операцій, дезінформації, пропаганди, кібератак як елементів інформаційної агресії. З перших днів конфлікту в Україні Росія розгорнула потужну пропагандистську кампанію, метою якої було створити в інформаційному просторі викривлену картину подій. Так, на міжнародному рівні Російська Федерація намагалася виправдати свої дії, подаючи їх як «захист російськомовного населення», «спецоперацію проти нацизму», «реакцію на загрози з боку НАТО». Ще одним напрямом стала боротьба за міжнародну інформаційну ініціативу. Російська Федерація використовувала всі можливості для впливу на громадську думку за кордоном, зокрема через мережу державних і приватних пропагандистських медіа (RT, Sputnik тощо), інформаційні атаки на міжнародні інституції, просування альтернативних трактувань подій в Україні. Поширювалися наративи про нібито «втручання Заходу», «зовнішнє управління Україною», «біолабораторії США», «геноцид у Донбасі» тощо. Такі меседжі активно підтримувалися на рівні офіційних заяв, дипломатичних демаршів, фінансування дружніх політичних сил за кордоном.*

*У межах дослідження проаналізовано положення міжнародного гуманітарного права, національного законодавства України щодо інформаційної безпеки, а також міжнародну практику протидії інформаційній агресії. Сучасна правова демократична держава повинна забезпечити баланс між свободою слова, поширення інформації та інформацією як інструментом сучасних інформаційних війн. Одним з варіантів досягнення такого балансу є створення незалежних регуляторних органів, що діятимуть на основі закону і з дотриманням міжнародних стандартів.*

*Запропоновано підходи щодо вдосконалення правового регулювання використання інформації у воєнний час, обґрунтовано необхідність розробки окремих правових механізмів ефективної протидії інструментам інформаційної війни.*

***Ключові слова:*** *інформаційна війна, дезінформація, пропаганда, гібрідна війна, інформаційна агресія, інформаційна безпека.*

**DOI 10.34079/2518-1521-2025-15-43-157-166**

**Постановка проблеми.** Війна, яка триває між Російською Федерацією та Україною з 2014 року і яка з 24 лютого 2022 року набула повномасштабного характеру, є найбільш яскравим прикладом сучасного конфлікту, в якому інформація використовується як повноцінна зброя. Особливістю цієї війни є те, що поряд із застосуванням традиційних засобів ведення бойових дій противник системно та цілеспрямовано використовує інструменти інформаційної агресії, зокрема дезінформацію, психологічні операції, кібератаки, пропаганду, втручання у внутрішній

медіапростір України, вплив на міжнародну громадську думку тощо. У цьому контексті російсько-українська війна є класичним прикладом гібридного конфлікту, в якому інформаційна складова відіграє не допоміжну, а ключову роль.

**Метою дослідження** є обґрунтування правової кваліфікації використання інформації як засобу сучасної зброї, уточнення правових механізмів її регулювання в сучасних умовах, а також формулювання пропозицій щодо вдосконалення національного та міжнародного законодавства задля більш ефективної протидії.

**Стан опрацювання проблематики.** Серед вітчизняних дослідників, які досліджували питання інформаційних війн, питання дезінформації як інструменту інформаційної агресії у сучасних війнах, питання гібрідних війн, стратегії та тактики російської пропаганди це Магда Є. (Магда, 2014; 2015), Павлюх М.В. (Павлюх, 2022), Почепцов Г. (Почепцов, 2015), Галіпчак В. (Галіпчак, 2023). Науковці Курило В., Савченко С. (Курило та Савченко, 2017), більш детально досліджували питання інформаційних технологій які використовуються для маніпулювання масовою свідомістю, впливу та управління людьми. Зазначається, що інформаційна агресія стала активно застосовуватись в ході анексії Криму та частини Донбасу, а її ефективність обумовило її більш активне застосування до та під час активних бойових дій у лютому 2022 року. Важливими є дослідження фахівців з даної проблематики Вєдєнєєва Д. та Семенюка О. (Вєдєнєєв та Семенюк, 2022; 2023), які зосередили увагу на вивченні протидії інформаційно-психологічній зброї, дезінформації, нормативно-правової державної політики тощо, а також власні наукові доробки Шебаніц Д., Шебаніц В. (Шебаніц, Д. та Шебаніц, В., 2025; 2022).

Серед зарубіжних дослідників, які вивчають питання інформаційних та гібрідних війн слід зазначити Гуаданьйо Р., Гуттієрі К. (Guadagno & Guttieri, 2019), Гофман Ф. (Hoffman, 2009) та ін.

**Виклад основного матеріалу.** З перших днів конфлікту Росія розгорнула потужну пропагандистську кампанію, метою якої було створити в інформаційному просторі викривлену картину подій. Так, на міжнародному рівні Російська Федерація намагалася виправдати свої дії, подаючи їх як «захист російськомовного населення», «спецоперацію проти нацизму», «реакцію на загрози з боку НАТО». У внутрішньому російському медіапросторі інформація суворо контролюється державою, незалежні джерела заборонені, а споживачі отримують лише офіційно дозволену інформацію, що має на меті легітимізувати війну та мобілізувати підтримку серед населення. Це створює паралельну реальність, в якій викривлене уявлення про події в Україні формується як єдино правильне.

Водночас значна частина інформаційної агресії була спрямована безпосередньо на Україну. Це проявлялося у поширенні фейкових повідомлень про ситуацію на фронті, втрати серед українських військових, зради з боку керівництва, провокуванні паніки серед цивільного населення. Ворожі телеграм-канали, сторінки у соціальних мережах, ботоферми і навіть зламані облікові записи державних установ використовувалися для дестабілізації ситуації. Під час активних бойових дій у Київській, Чернігівській, Харківській, Сумській областях системно поширювалися повідомлення про здачу міст, накази про евакуацію, вибухи чи інші події, які не відповідали дійсності. Такі інформаційні атаки мали на меті посіяти страх, зневіру, змусити населення до хаотичних дій, а також знизити рівень опору окупації.

Окремим напрямом інформаційної агресії стали кібератаки. Починаючи з 2014 року, Україна регулярно ставала об’єктом нападів на критичну інфраструктуру, державні бази даних, урядові портали. Серед найбільш відомих прикладів - атака на енергосистему у грудні 2015 року, що призвела до відключення електроенергії в

кількох регіонах. У 2017 році Україна зазнала масштабної кібератаки вірусу Petya/NotPetya, який паралізував роботу державних і приватних систем, включаючи банки, транспорт, телекомунікації. У 2022-2023 роках ці атаки продовжились - зокрема, мали місце спроби зламу систем управління військовими операціями, сайтів уряду, медичних закладів, об'єктів логістики. Ці дії супроводжувалися кампаніями дезінформації, які мали створити ефект дестабілізації та безпорадності (Ткаченко, 2022, с. 88).

Ще одним напрямом стала боротьба за міжнародну інформаційну ініціативу. Російська Федерація використовувала всі можливості для впливу на громадську думку за кордоном, зокрема через мережу державних і приватних пропагандистських медіа (RT, Sputnik тощо), інформаційні атаки на міжнародні інституції, просування альтернативних трактувань подій в Україні. Поширювалися наративи про нібито «втручання Заходу», «зовнішнє управління Україною», «біолабораторії США», «геноцид у Донбасі» тощо. Такі меседжі активно підтримувалися на рівні офіційних заяв, дипломатичних демаршів, фінансування дружніх політичних сил за кордоном. Цей інформаційний тиск був спрямований на зменшення підтримки України, ослаблення санкцій проти РФ, вплив на внутрішньополітичні дискусії в країнах-членах НАТО та ЄС (Петренко, 2021, с. 112).

Національна інформаційна безпека України виявилася достатньо стійкою до масштабної інформаційної агресії, хоча ситуація вимагає постійної адаптації та удосконалення. Держава оперативно реагує на інформаційні виклики: блокуються проросійські канали, запроваджуються санкції до інформаційних ресурсів, активізувалася робота Центру стратегічних комунікацій, впроваджено практику офіційного спростування фейків.

9 вересня 2024 року відбулося засідання Національного координаційного центру кібербезпеки (НКЦК) - ключового органу координації та контролю у сфері кібербезпеки України, на якому було прийнято рішення обмежити використання месенджера Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури. З метою мінімізації кіберзагроз було прийнято рішення щодо заборони встановлення та використання Telegram на службових пристроях працівників органів державної влади, військовослужбовців, працівників сектору безпеки і оборони, а також підприємств - операторів критичної інфраструктури (Рада національної безпеки і обори України, 2024).

На національному рівні Україна вже здійснила низку кроків у напрямі посилення правових інструментів протидії інформаційній агресії. Зокрема, кримінальне законодавство доповнено статтями, що передбачають відповідальність за поширення стратегічної інформації під час війни, втручання в інформаційні системи, співпрацю з державою-агресором у медіа-сфері. Водночас існує потреба у розробці та прийняті комплексного Закону України «Про інформаційну безпеку», який би системно визначав поняття інформаційної агресії, встановлював межі допустимого інформаційного впливу, регламентував порядок реагування на загрози, врегульовував діяльність уразливих до впливу платформ і визначав відповідальність за порушення. Окремим блоком правових викликів є сфера цифрових платформ і соціальних мереж. В Україні, як і в більшості країн, відсутній прямий державний контроль над алгоритмами поширення контенту в глобальних медіасервісах. Це створює ситуацію, в якій ворожий контент може масово поширюватися через телеграм-канали, YouTube, Facebook або TikTok, не підпадаючи під національні заборони. Для подолання цієї проблеми потрібні як двосторонні домовленості з цифровими корпораціями, так і створення правового механізму примусу до співпраці у сфері видалення небезпечного контенту, блокування

фейкових акаунтів, маркування дезінформації. Україна вже має певний досвід у цьому напрямі, проте ці заходи залишаються фрагментарними і мають бути закріплені в нормативно-правових актах (Президент України, 2021).

Не менш важливим є питання прав людини в умовах боротьби з інформаційною агресією. У демократичних державах обмеження свободи слова повинні бути пропорційними, законними та необхідними в умовах конкретної ситуації (Литвиненко, 2021, с. 22). Саме тому розробка правових механізмів має враховувати баланс між забезпеченням інформаційної безпеки та збереженням фундаментальних свобод. Одним з варіантів досягнення такого балансу є створення незалежних регуляторних органів, що діятимуть на основі закону і з дотриманням міжнародних стандартів. В Україні роль такого органу частково виконує Національна рада з питань телебачення і радіомовлення, однак необхідне подальше вдосконалення її повноважень у цифровому середовищі (Рада національної безпеки і оборони України, 2017).

Ще одним перспективним напрямом є правова підтримка фактчекінгових ініціатив. Платформи, що займаються верифікацією інформації, виконують важливу суспільну функцію, але часто працюють без чіткої нормативної підтримки. Законодавче закріплення їхнього статусу, гарантії захисту від переслідування, доступ до офіційної інформації - все це сприяло б формуванню ефективного механізму самоочищення інформаційного простору. Також важливо створити правові підстави для освіти у сфері медіаграмотності, оскільки правова культура споживання інформації є не менш важливою, ніж кримінально-правові заборони. У довгостроковій перспективі необхідно працювати над гармонізацією національного законодавства з європейськими підходами. Європейський Союз вже запровадив низку регуляторних актів - таких як Закон про цифрові послуги (Digital Services Act), що встановлює обов’язки платформ з видалення шкідливого контенту, прозорості алгоритмів, відповідальності за поширення дезінформації. Україна, прагнучи до інтеграції в європейське правове поле, має враховувати ці стандарти при формуванні власної системи протидії інформаційній агресії. Це дозволить не лише посилити захист інформаційного суверенітету, а й створити умови для спільної європейської інформаційної політики, що протистоятиме зовнішнім загрозам.

Використання інформації як зброї стало не лише проблемою окремих держав, таких як Україна, а й глобальним викликом для всієї міжнародної спільноти (International Committee of the Red Cross, 2022, с. 17). Інформаційні атаки, кібервтручання, маніпулювання громадською думкою, втручання у вибори, дезінформація в періоди криз і конфліктів, інформаційний тиск на міжнародні організації - усе це перетворює інформаційний простір на повноцінне поле гібридного протистояння. Відповіддю на ці загрози стали спроби міжнародних організацій - таких як НАТО, Європейський Союз, Організація Об’єднаних Націй - виробити концептуальні, нормативні та інституційні механізми протидії використанню інформації як зброї.

Розглядаючи сучасну практику, можна виокремити кілька ключових прецедентів та ініціатив, які свідчать про поступове формування міжнародної практики до цієї проблеми.

НАТО, як провідний військово-політичний альянс, одним з перших визнав гібридні загрози як пріоритетні. Ще у 2014 році, після початку агресії Російської Федерації проти України, в офіційних документах НАТО з’явилося поняття hybrid warfare, в якому інформаційна війна була визначена як один з основних елементів. У підсумковому документі Варшавського саміту 2016 року було зазначено, що Альянс розробляє механізми протидії дезінформації, веде роботу з аналізу інформаційних атак

та співпрацює з партнерами у сфері стратегічних комунікацій. З цією метою у НАТО створено спеціальний підрозділ StratCom COE (Центр передового досвіду зі стратегічних комунікацій), що базується в Ризі (Латвія). Він аналізує інформаційні кампанії держав-агресорів, розробляє рекомендації щодо протидії фейковим наративам, проводить навчання для країн-членів та партнерів Альянсу. Україна активно співпрацює з цим центром, отримуючи експертизу у сфері медіабезпеки та протидії російській пропаганді (Ahmadli, J., 2022, c. 7-8).

Одним із найбільш відомих прецедентів інформаційного втручання стала спроба Росії вплинути на президентські вибори у США у 2016 році. За даними розслідування спецпрокурора Роберта Мюллера, російські спецслужби організували масштабну кампанію у соціальних мережах, яка мала на меті посіяти розбрат у американському суспільстві, вплинути на результати голосування, послабити довіру до інститутів демократії. Цей випадок став каталізатором широкої дискусії в ООН і ЄС щодо меж свободи слова, відповідальності за поширення дезінформації та необхідності міжнародного регулювання цифрової сфери. У звітах НАТО та ЄС зазначалося, що подібні кампанії можуть розглядатися як акти гібридної агресії, а в разі значного впливу на суверенітет держави - навіть як форма втручання, що суперечить міжнародному праву.

Європейський Союз, реагуючи на ці виклики, створив у 2015 році структуру East StratCom Task Force - аналітичний підрозділ, який займається виявленням, документуванням і спростуванням російських дезінформаційних кампаній. Ця група публікує щотижневі звіти про фейки, які поширюються в країнах Європи, вивчає методи та канали їх поширення, а також пропонує інституційні заходи для протидії інформаційній агресії. У 2018 році Європейська комісія представила План дій щодо боротьби з дезінформацією, який передбачає тісну взаємодію між державами-членами, платформами соціальних медіа, громадянським суспільством та експертами. У документі визначено, що системне поширення неправдивої інформації може становити загрозу демократії, громадському порядку та безпеці держав, тому необхідне спільне реагування (Scholarly Community Encyclopedia, 2023).

Ще одним важливим кроком ЄС стало ухвалення Кодексу поведінки щодо боротьби з дезінформацією, який підписали найбільші технологічні компанії - Google, Facebook (Meta), Twitter, TikTok, Microsoft. Ці платформи зобов'язалися маркувати або видаляти недостовірний контент, обмежувати охоплення фейкових повідомлень, прозоро звітувати про дії щодо інформаційної безпеки, співпрацювати з фактчекінговими організаціями. Хоча документ має рекомендаційний характер, він став важливим інструментом тиску на цифрових гігантів з боку держав у сфері боротьби з інформаційною загрозою. Після початку повномасштабної війни Росії проти України у 2022 році ЄС також запровадив санкції проти російських пропагандистських каналів, таких як RT і Sputnik, заборонив їх мовлення в країнах-членах та блокував їх онлайн-присутність.

Організація Об'єднаних Націй поки що не має окремого правового механізму регулювання інформаційної безпеки, однак неодноразово порушувала це питання у своїх резолюціях і заявах. Зокрема, у Резолюції Генеральної Асамблеї ООН № 73/27 від 2018 року було визнано необхідність формування правил поведінки держав у сфері інформаційної безпеки, в тому числі в контексті кіберпростору (United Nations, 2018). У 2020 році створено Відкриту робочу групу ООН з питань кібербезпеки, яка займається розробкою глобального нормативного підходу до цифрових загроз, включаючи дезінформацію, інформаційне втручання у вибори, інформаційний шантаж. У своїх документах ООН визнає, що поширення фейкової інформації в умовах збройного

конфлікту може посилювати насильство, провокувати порушення прав людини та підривати суверенітет держав.

Україна неодноразово зверталася до ООН, НАТО та ЄС із вимогою визнати інформаційну агресію як окремий тип агресії у розумінні Статуту ООН. У виступах представників України на Генеральній Асамблеї та Раді Безпеки неодноразово наголошувалося про необхідність створення міжнародного механізму фіксації та санкціонування випадків системної інформаційної агресії. Такі ініціативи ще не отримали статусу міжнародного договору, однак сприяли включенню питання інформаційної безпеки до порядку денного низки міжнародних форумів, конференцій з кібербезпеки, а також внутрішніх стратегій держав-членів ООН.

**Висновки.** Інформаційна війна між Україною та Російською Федерацією стала прикладом того, як слово, зображення, дані можуть мати такий самий вплив, як і ракети чи танки. Вона довела, що контроль над інформаційним простором, швидка реакція на фейки, інформаційна мобілізація населення, стратегічні комунікації з партнерами та послідовна інформаційна політика є не менш важливими, ніж фізична оборона. Успішне протистояння інформаційній агресії є фактором виживання держави, збереження її внутрішньої цілісності та міжнародного авторитету. Тому досвід України є важливим прикладом для міжнародного співтовариства, яке тільки починає формувати механізми правової та політичної реакції на нові виклики інформаційної війни. Україна стала реальним «полем бою» на якому проходять випробування не лише нові види військового озброєння, а й інструменти сучасної інформаційної війни. Анонсовані президентські вибори в Україні під час війни стануть реальним викликом інформаційного інструментарію та нададуть реальний досвід протидії впливу інформаційним війнам під час виборів в «особливих умовах» не тільки для України, а й для всього світу.

**Бібліографічний список**

Вєдєнєєв, Д. В.та Семенюк, О. Г. 2022. *Розвиток в Україні науково-концептуальних та організаційно-функціональних засад протидії інформаційно-психологічній зброї як знаряддю гібридної конфліктності (1991–2022 рр.).* Київ: ДП «Інфотех», 256 с.

Вєдєнєєв, Д. В. та Семенюк О. Г. 2023. Проблематика інформаційного протиборства в нормативно-правових й доктринальних документах сфери національної безпеки України. *Юридичний науковий електронний журнал*. [онлайн], 2, с. 21-25. Доступно: <http://lsej.org.ua/2_2023/2.pdf>

Галіпчак, В., 2023. Інформаційна війна як складова гібрідної війни у умовах російської агресії. *Вісник Прикарпатського університету. Серія: Політологія* [онлайн], 15, с. 26-32. Доступно: <https://journals.pnu.if.ua/index.php/politology/article/view/50/49>

Рада національної безпеки і оборони України, 2017. Доктрина інформаційної безпеки України: Рішення РНБО від 25.02.2017. *Верховна Рада України* [онлайн]. Доступно: <https://zakon.rada.gov.ua/laws/show/n0016525-16/ed20170228>

Курило, В. С. та Савченко, С. В., 2017. Інформаційна агресія в контексті гібридної війни на сході України. *Освіта та педагогічна наука.* [онлайн], 2(167), с. 5-13. Доступно: <https://dspace.luguniv.edu.ua/xmlui/bitstream/handle/123456789/4239/3.pdf?sequence=1&isAllowed=y>

Литвиненко, А. Г., 2021. *Інформаційна війна та безпека держави : монографія*. Київ : НАДУ. 276 с.

Магда, Є. В., 2014. Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України.* [онлайн], 5, с. 138-142. Доступно: <http://nbuv.gov.ua/UJRN/Nzizvru_ 2014_5_29>

Магда, Є.В., 2015. Міжнародний імідж України в контексті гібридної війни. *Вісник Дніпропетровського університету.* [онлайн], 4, с. 232-240. Доступно: <https://visnukpfs.dp.ua/index.php/PFS/article/view/764/804>

Рада національної безпеки і обори України, 2024. *НКЦК прийняв рішення обмежити використання Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури.* [онлайн] Доступно: <https://www.rnbo.gov.ua/ua/Diialnist/6994.html>

Павлюх, М. В., 2022. Методи та засоби російсько-української інформаційної війни (2014–2022): міфи і риторика пропаганди, с. 1017-1025. [онлайн] Доступно: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6346/13382-1?inline=1>

Петренко, І. М., 2021. *Кібербезпека та інформаційні війни : навч. посіб*. Львів: ЛНУ ім. І. Франка. 268 с.

Почепцов, Г., 2015. *Інструментарій хаосу в гібрідній війні*. 20 с. [онлайн] Доступно: <https://d1wqtxts1xzle7.cloudfront.net/39410990/>

Президент України, 2021. *Про стратегію кібербезпеки України: Указ Президента № 447/2021 від 14.05.2021*. [онлайн] Доступно: <https://www.president.gov.ua/documents/4472021-40013>

Ткаченко, Л. І., 2022. *Протидія фейкам в умовах воєнного стану : монографія*. Львів : Новий Світ. 198 с.

Шебаніц, Д. та Шебаніц, В. 2025. Особливості правового регулювання забезпечення інформаційної безпеки на локальному рівні підприємства. *Європейські перспективи.* [онлайн], 1, с. 173-179. Доступно: <https://repository.mu.edu.ua/jspui/bitstream/123456789/8821/1/shebanic_osobl_2025_1_173.pdf>.

Шебаніц, Д. М. та Шебаніц, В. Ф. 2022. Інформаційні війни в період воєнного стану: правові засади протидії. *Особливості інтеграції країн у світовий економічний та політико-правовий простір*: IX міжнародна науково-практична конференція МДУ / За заг. ред. М.В. Трофименка. Київ: МДУ. с. 40-42. [онлайн] Доступно: <https://mu.edu.ua/storage/MSU/pages/conferences/2022/Особливості%20інтеграції%20країн%20у%20світовий%20економічний%20та%20політико-правовий%20простір.pdf>

Ahmadli, J. 2022. Review of NATO and EU's fight against hybrid threats. *NTUU "KPI" NEWSLETTER. Political Science. Sociology. Law*. 2(54), p. 6-11. [online] Available at: <https://visnyk-psp.kpi.ua/article/view/264384/260507>

Scholarly Community Encyclopedia, 2023. East StratCom Task Force. Disinformation Review. Brussels: EU External Action, [online] Available at: <https://encyclopedia.pub/entry/29106?utm_source=chatgpt.com>

Guadagno, R. E. & Guttieri, K. 2019. Fake news and information warfare: An examination of the political and psychological processes from the digital sphere to the real world. *In Research anthology on fake news, political warfare, and combatting the spread of misinformation*, p. 167-191. [online] Available at: <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/guadagnoguttieri_fakenews.pdf>

International Committee of the Red Cross, 2022. *International Humanitarian Law and Cyber Operations.* Geneva. 84 p.

Hoffman, F.G., 2009. Hybrid Warfare and Challenges. *Joint Force Quarterly*, p. 34-48. [online] Available at: <https://apps.dtic.mil/sti/pdfs/ADA516871.pdf >

United Nations, 2018. Resolution 73/27 on Developments in the Field of Information and Telecommunications in the Context of International Security. New York. [online] Available at: <https://docs.un.org/en/A/RES/73/27>

**References**

Ahmadli, J. 2022. Review of NATO and EU's fight against hybrid threats. *NTUU "KPI" NEWSLETTER. Political Science. Sociology. Law*. 2(54), p. 6-11. [online] Available at: <https://visnyk-psp.kpi.ua/article/view/264384/260507>

Guadagno, R. E. & Guttieri, K. 2019. Fake news and information warfare: An examination of the political and psychological processes from the digital sphere to the real world. *In Research anthology on fake news, political warfare, and combatting the spread of misinformation*, p. 167-191. [online] Available at: <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/guadagnoguttieri_fakenews.pdf>

Halipchak, V., 2023. Informatsiina viina yak skladova hibridnoi viiny u umovakh rosiiskoi ahresii [Information warfare as a component of hybrid warfare in the context of Russian aggression]. *Visnyk Prykarpatskoho universytetu. Seriia: Politolohiia* [online], 15, s. 26-32. Available at: <https://journals.pnu.if.ua/index.php/politology/article/view/50/49> (in Ukrainian).

Hoffman, F.G., 2009. Hybrid Warfare and Challenges. *Joint Force Quarterly*, p. 34-48. [online] Available at: <https://apps.dtic.mil/sti/pdfs/ADA516871.pdf >

International Committee of the Red Cross, 2022. *International Humanitarian Law and Cyber Operations.* Geneva. 84 p.

Kurylo, V. S. ta Savchenko, S. V., 2017. Informatsiina ahresiia v konteksti hibrydnoi viiny na skhodi Ukrainy [Information aggression in the context of hybrid war in eastern Ukraine]. *Osvita ta pedahohichna nauka*. [online], 2(167), s. 5-13. Available at: <https://dspace.luguniv.edu.ua/xmlui/bitstream/handle/123456789/4239/3.pdf?sequence=1&isAllowed=y> (in Ukrainian).

Lytvynenko, A. H., 2021. *Informatsiina viina ta bezpeka derzhavy : monohrafiia [Information War and State Security: Monograph].* Kyiv : NADU. 276 s. (in Ukrainian).

Mahda, Ye. V., 2014. Vyklyky hibrydnoi viiny: informatsiinyi vymir [Challenges of Hybrid War: Information Dimension] *Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy*. [online], 5, s. 138-142. Available at: <http://nbuv.gov.ua/UJRN/Nzizvru_ 2014_5_29> (in Ukrainian).

Mahda, Ye.V., 2015. Mizhnarodnyi imidzh Ukrainy v konteksti hibrydnoi viiny [International image of Ukraine in the context of hybrid war]. *Visnyk Dnipropetrovskoho universytetu*. [online], 4, s. 232-240. Available at: <https://visnukpfs.dp.ua/index.php/PFS/article/view/764/804> (in Ukrainian).

Pavliukh, M. V., 2022. Metody ta zasoby rosiisko-ukrainskoi informatsiinoi viiny (2014–2022): mify i rytoryka propahandy [Methods and means of Russian-Ukrainian information war (2014–2022): myths and rhetoric of propaganda], s. 1017-1025. [online] Available at: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6346/13382-1?inline=1> (in Ukrainian).

Petrenko, I. M., 2021. *Kiberbezpeka ta informatsiini viiny : navch. posib [Cybersecurity and information warfare: a textbook].* Lviv: LNU im. I. Franka. 268 s. (in Ukrainian).

Pocheptsov, H., 2015. *Instrumentarii khaosu v hibridnii viini [Toolkit of chaos in hybrid warfare]*. 20 s. [online] Available at: <https://d1wqtxts1xzle7.cloudfront.net/39410990/> (in Ukrainian).

Prezydent Ukrainy, 2021. Pro stratehiiu kiberbezpeky Ukrainy: Ukaz Prezydenta № 447/2021 vid 14.05.2021. [On the Cybersecurity Strategy of Ukraine: Presidential Decree No. 447/2021 of 05/14/2021. (data zvernennia 15.12.2025)] [online] Available at: <https://www.president.gov.ua/documents/4472021-40013> (in Ukrainian).

Rada natsionalnoi bezpeky i oborony Ukrainy, 2017. Doktryna informatsiinoi bezpeky Ukrainy: Rishennia RNBO vid 25.02.2017 [Doctrine of Ukraine: NSDC Decision of 25.02.2017]. *Verkhovna Rada Ukrainy* [online]. Available at: <https://zakon.rada.gov.ua/laws/show/n0016525-16/ed20170228> (in Ukrainian).

Rada natsionalnoi bezpeky i obory Ukrainy, 2024. NKTsK pryiniav rishennia obmezhyty vykorystannia Telegram v orhanakh derzhavnoi vlady, viiskovykh formuvanniakh, na obiektakh krytychnoi infrastruktury [The NCCC decided to restrict the use of Telegram in government bodies, military formations, and critical infrastructure facilities]. [online] Available at: <https://www.rnbo.gov.ua/ua/Diialnist/6994.html> (in Ukrainian).

Scholarly Community Encyclopedia, 2023. East StratCom Task Force. Disinformation Review. Brussels: EU External Action, [online] Available at: <https://encyclopedia.pub/entry/29106?utm_source=chatgpt.com>

Shebanits, D. M. ta Shebanits, V. F. 2022. Informatsiini viiny v period voiennoho stanu: pravovi zasady protydii [Information wars during martial law: legal principles of counteraction]. *Osoblyvosti intehratsii krain u svitovyi ekonomichnyi ta polityko-pravovyi prostir:* IX mizhnarodna naukovo-praktychna konferentsiia MDU / Za zah. red. M.V. Trofymenka. Kyiv: MDU. s. 40-42. [online] Available at: <https://mu.edu.ua/storage/MSU/pages/conferences/2022/Osoblyvosti%20intehratsiï%20kraïn%20u%20svitovyў%20ekonomichnyў%20ta%20polityko-pravovyў%20prostir.pdf> (in Ukrainian).

Shebanits, D. ta Shebanits, V. 2025. Osoblyvosti pravovoho rehuliuvannia zabezpechennia informatsiinoi bezpeky na lokalnomu rivni pidpryiemstva [Peculiarities of legal regulation of information security at the local level of the enterprise]. *Yevropeiski perspektyvy.* [online], 1, s. 173-179. Available at: <https://repository.mu.edu.ua/jspui/bitstream/123456789/8821/1/shebanic_osobl_2025_1_173.pdf> (in Ukrainian).

Tkachenko, L. I., 2022. *Protydiia feikam v umovakh voiennoho stanu : monohrafiia [Counteraction to fakes in martial law: monograph]*. Lviv : Novyi Svit. 198 s. (in Ukrainian).

United Nations, 2018. Resolution 73/27 on Developments in the Field of Information and Telecommunications in the Context of International Security. New York. [online] Available at: <https://docs.un.org/en/A/RES/73/27>

Viedienieiev, D. V. ta Semeniuk O. H. 2023. Problematyka informatsiinoho protyborstva v normatyvno-pravovykh y doktrynalnykh dokumentakh sfery natsionalnoi bezpeky Ukrainy [The problem of information confrontation in regulatory and doctrinal documents of the national security sphere of Ukraine]. *Yurydychnyi naukovyi elektronnyi zhurnal*. [online], 2, s. 21-25. Available at: <http://lsej.org.ua/2_2023/2.pdf> (in Ukrainian).

Viedienieiev, D. V.ta Semeniuk, O. H. 2022. *Rozvytok v Ukraini naukovo-kontseptualnykh ta orhanizatsiino-funktsionalnykh zasad protydii informatsiino-psykholohichnii zbroi yak znariaddiu hibrydnoi konfliktnosti (1991–2022 rr.) [Development in Ukraine of*

*scientific-conceptual and organizational-functional principles of countering informational-psychological weapons as a tool of hybrid conflict (1991–2022)]*. Kyiv: DP «Infotekh», 256 s. (in Ukrainian).

Стаття надійшла до редакції 15.11.2025 р.

**D. Shebanits,**
**D. Trifonov.**

## INFORMATION AS A MODERN WEAPON: NATIONAL AND INTERNATIONAL PRACTICE OF COUNTERACTION

*This article is devoted to defining the role of information as a key tool in modern wars and hybrid conflicts, as well as the legal regulation of information security in military operations.*

*The study analyzes the functioning of information as an object of legal protection and as a means of influence in armed conflict. Particular attention is paid to the study of psychological operations, disinformation, propaganda, and cyberattacks as elements of information aggression. From the first days of the conflict in Ukraine, Russia launched a powerful propaganda campaign, the aim of which was to create a distorted picture of events in the information space. Thus, at the international level, the Russian Federation tried to justify its actions by presenting them as «protection of the Russian-speaking population», «a special operation against Nazism», and «a response to threats from NATO». Another direction was the struggle for an international information initiative. The Russian Federation used all opportunities to influence public opinion abroad, in particular through a network of state and private propaganda media (RT, Sputnik, etc.), information attacks on international institutions, and promotion of alternative interpretations of events in Ukraine. Narratives were spread about alleged «Western interference», «external control of Ukraine», «US biolaboratories», «genocide in Donbas», etc. Such messages were actively supported at the level of official statements, diplomatic demarches, and financing of friendly political forces abroad.*

*The study analyzed the provisions of international humanitarian law, national legislation of Ukraine on information security, as well as international practice of countering information aggression. A modern democratic state governed by the rule of law must ensure a balance between freedom of speech, dissemination of information, and information as a tool of modern information warfare. One option for achieving such a balance is to create independent regulatory bodies that will operate on the basis of the law and in compliance with international standards.*

*Approaches to improving the legal regulation of the use of information in wartime are proposed, and the need to develop separate legal mechanisms for effective counteraction to the tools of information warfare is substantiated.*

***Key words:*** *information warfare, disinformation, propaganda, hybrid warfare, information aggression, information security.*