

## ІНФОРМАЦІЙНІ ВІЙНИ: ПОШУК СТРАТЕГІЙ ПРОТИДІЇ

## INFORMATION WARS: SEARCH FOR COUNTERACTION STRATEGIES

У статті проаналізовано сутність поняття «інформаційна війна», окреслено особливості інформаційної війни, методи ведення якої описуються за допомогою поняття інформаційної зброї. Виокремлено значення та роль соціальних мереж у сфері інформаційних воєн та їх можливості у дезорганізації та дезорієнтації суспільства. Описано можливості нарративів як механізму деструктивного спрямування. У сучасному суспільстві термін «інформаційна війна» поступово перейшов з позицій смислової одиниці публіцистичної лексики до самостійної категорії наукового дискурсу, а інформаційна війна є багатоплановим феноменом сьогодення.

Досліджено законодавчу базу України, здійснено аналіз актуальних питань та завдань протидії інформаційній війні в українському законодавстві, а саме у Стратегічному оборонному бюлетені України, Стратегії інформаційної безпеки України, Стратегії національної безпеки України. Стратегія інформаційної безпеки є ключовим документом в законодавстві України в означеній сфері, і згідно з ним поняття «інформаційна безпека» визнається як складова частина національної безпеки України. Виявлено, що основними принципами організації системи управління в сфері протидії інформаційним загрозам мають бути такі: єдиноначальність управління, чітка вертикаль управління, відокремлення функцій з формування державної політики у сфері оборони від функції її реалізації, демократичний цивільний контроль.

Робиться висновок про необхідність систематичного виконання дій органів публічного управління України у напрямку своєчасного виявлення й ліквідації загроз і ризиків негативного впливу «інформаційної зброї» національного інформаційного простору, реалізації державної політики протидії «інформаційній війні», задіяння недержавних громадських організацій у заходах протистояння інформаційним загрозам та здійснення на всіх рівнях ефективного захисту інформаційного суверенітету держави.

**Ключові слова:** інформаційна війна, інформаційна зброя, інформаційна безпека, медіаграмотність, Стратегія інформаційної безпеки.

The article analyzes the essence of the concept of "information warfare", outlines the features of information warfare, the methods of which are described using the concept of information weapons. The importance and role of social networks in the field of information warfare and their capabilities in disorganizing and disorienting society are highlighted. The possibilities of narratives as a mechanism of destructive direction are described. In modern society, the term "information warfare" has gradually moved from the position of a sign-symbolic unit of journalistic vocabulary to an independent category of scientific discourse, and information warfare is a multifaceted phenomenon of our time.

The author examines the legislative framework of Ukraine, analyzes the topical issues and tasks of countering information warfare in Ukrainian legislation, namely, the Strategic Defense Bulletin of Ukraine, the Information Security Strategy, and the National Security Strategy of Ukraine. The Information Security Strategy is a key document in the legislation of Ukraine in this area, and according to it, the concept of "information security" is defined as an integral part of the national security of Ukraine. It is found that the main principles of organization of the management system in the field of countering information threats should be as follows: sole authority of management, clear vertical management, separation of the function of formulating the State policy in the field of defense from the function of its implementation, democratic civilian control.

The author concludes that it is necessary to systematically implement the actions of public administration bodies of Ukraine in the direction of timely detection and elimination of threats and risks of negative impact of "information weapons" of the national information space, implementation of the State policy of countering the "information war", involvement of non-governmental organizations in measures to counter information threats and effective protection of the information sovereignty of the State at all levels.

**Key words:** information warfare, information weapons, information security, media literacy, information security strategy.

УДК 351:355:008  
DOI <https://doi.org/10.32782/pma2663-5240-2023.33.3>

**Грицай Р.О.**

аспірант кафедри державного управління

Навчально-науковий інститут публічного управління та державної служби Київського національного університету імені Тараса Шевченка

**Постановка проблеми у загальному вигляді.** Справжнім викликом для Української держави стала гаряча фаза російсько-української війни, щорозпочалася 24 лютого 2022 року і є кровавим продовженням агресії росії проти України як в воєнному просторі, так і в інформаційному. В умовах російсько-української війни актуалізується вивчення проблеми інформаційної безпеки України, формування стратегії інформаційного протистояння та особливостей інформаційної війни на сучасному етапі.

Нині інформаційна війна є складовою сучасної політики держав. Тому для збереження національної безпеки, держава має впроваджувати елементи захисту в інформаційному

просторі, а також формувати комплекс заходів спрямованих на виявлення та усунення загроз для суспільства у цій сфері.

**Аналіз останніх досліджень і публікацій.** Останнім часом тема інформаційної війни, форми та технології її ведення дуже активно обговорюються в науковій літературі. Помітний внесок в розробку цієї проблематики зробили Г. Почепцов, Є. Магда, О. Данильян, О. Дзьобань, І. Сопілко, В. Хорошко, Ю. Хохлачова, І. Жаровська, Н. Ортинська, О. Марунченко, О. Саган, М. Бучин, О. Курбан, В. Новородовський, М. Гетьманчук, М. Зубарева тощо. Поняття «інформаційна війна» нерозривно пов'язане

з поняттями «інформаційна безпека», «сміслова війна», «інформаційна зброя», «кібертероризм», «медіа-інформаційний тероризм».

**Метою статті** є розкриття сутності та особливостей поняття «інформаційна війна» і аналіз публічних (правових) засад протидії провадам інформаційної війни в Україні.

**Виклад основного матеріалу.** Г.Почепцов говорить про інформаційну війну як комунікативну технологію впливу на масову свідомість із короткочасними і довгостроковими цілями. Окремим типом інформаційних воєн він виокремлює смислову війну, яка розрахована на більший сегмент населення, ніж інформаційна війна, та на довготривалий період. «Кожен тип війни спрямований на власний тип простору. Звичайна війна – на простір фізичний, інформаційна – на інформаційний, сміслова – на простір когнітивний... Тут можна зауважити, мовляв, інформаційна війна теж має за мету «поцілити в голову людині». ... Інформаційні війни більш помітні, ніж смислові, тому в цьому випадку швидше починають бити на сполох. Сміслові війни закриті ореолом естетичної привабливості, тому вони залишаються більш непоміченими» [1, с. 24–25]

Дослідник гібридних воєн Євген Магда на прикладі України чітко і методично показує методи гібридної війни, які застосовуються росією починаючи з 2013 року. По суті, всі ці методи є складовими інформаційної війни, мета якої передбачає розхитування ситуації всередині держави, а також створення її негативного іміджу на міжнародній арені. Серед зазначених методів хочеться виділити такі:

– «криве дзеркало» – перекручування та пересмикування фактів;

– «килимове бомбардування дезінформацією» призводить до панічних настроїв та появи численних ліній розколу в українському суспільстві, що має призвести до дестабілізації ситуації всередині країни»;

– «перетягування Заходу» – спроби створити проросійську коаліцію, лобювання інтересів росії діючими та колишніми європейськими політиками разом з поширенням інформаційної кампанії щодо формування позитивного образу росії в Європі;

– «заперечення очевидного» має на меті створювати видимість відсутності агресії [2, с. 140]. Більшість цих методів використав володимир путін у своїй промові-посланні Федеральним зборам рф 21 лютого 2023 року, акцентуючи, що «США та НАТО прискорено розгортали біля кордонів нашої країни свої армійські бази, секретні біолабораторії, під час маневрів освоювали театр майбутніх воєнних дій, готували підвладний ним київський режим,

поневолену ними Україну до великої війни». *«Це вони розв'язали війну. А ми використовуємо силу, щоб її зупинити»*, – запевняв російський диктатор [15].

Методи, які застосовує агресор, дають можливість викривляти оцінку того, що відбувається, деморалізувати громадян. Всі методи ведення інформаційної війни спрямовані на формування стійкої суспільної думки в потрібному маніпуляторам напрямі і закладаються необхідні установки поведінки у свідомості громадян для можливого подальшого управління ними. На його думку, інформаційна війна – це узгоджена діяльність з використання інформації як зброї для ведення бойових дій. Головним стратегічним національним ресурсом стає інформаційний простір, тобто інформація, мережева інфраструктура та інформаційні технології.

Аналізуючи роль соціальних мереж у сфері інформаційних воєн та місце в ній росії, Новородовський Валерій припускає, що «використовуючи facebook як основну інформаційну платформу, створювалася основа для конфлікту» [3, с. 154]. І мова йде не лише про російсько-українську війну, але й конфлікт у Грузії, Нагорному Карабасі, Придністров'ї. Російські пропагандисти, використовуючи соціальні мережі «вконтакте» та «однокласники», які були популярні в Україні на початку 2000-х років, формували через певні спільноти меседжі, що були спрямовані на дезорганізацію та дезорієнтацію суспільства. В результаті маніпуляцій та впливу на суспільну свідомість «відбулося поширення ідей «русского мира», що зумовлювало маргіналізацію певних прошарків суспільства і створювало передумови для розгортання сепаратистських рухів на території іншої країни» [3, с. 156]. Застосування інформації та дезінформації як зброї є потужним елементом путінського режиму в системі просування власних цінностей та наративів. Завдяки їм досягається панування в публічному просторі. Ба, більше, «переважна більшість інформаційних кампаній, атак чи просто активного поширення повідомлень у вітчизняному інформпросторі, які здійснюються технологічними пропагандистськими центрами Кремля, мають на меті створення атмосфери тотального страху, непевності, приниження, безвиході, відчаю тощо» [4, с. 43].

Найбільш «проникливою» сферою застосування інформаційної зброї є людська свідомість. Впливаючи на неї відбувається нагромадження нестійкого сприйняття світу, розгубленості, тривожності. Ми можемо з впевненістю сказати, що інформаційна зброя постає в сьогоденні як новий і унікальний вид

зброї. Її унікальність у прихованому характері, масштабі застосування та збереженні матеріальних та людських цінностей. «Інформаційна зброя розглядається як засіб ведення інформаційної війни, що є лише ключовим елементом повномасштабної війни» [17, с. 52]. На думку групи дослідників, не можна недооцінювати можливості інформаційної зброї у сучасній війні, оскільки це може призвести до фатальної помилки під час подальшої воєнно-політичної боротьби [17].

Про важливість соціальних мереж та інтернет-майданчиків у розрізі питання інформаційних воєн говорить Саган О. [5]. В умовах інформаційної агресії, на її переконання, знаково-символічна сфера людини, у якій ключову роль відіграють мова, символічна культура, цінності, зазнає впливу вибіркової значень подій і речей. Вони формують так би мовити, «мозаїчну свідомість», характерною особливістю якої є втрата особистістю змоги критично мислити та адекватно оцінювати реальність. Людина легко піддається мові ворожнечі, а також радикальному та екстремістському впливам. «Специфіка організації блогосфери та особливості інтернет-культури перетворили соціальні мережі на небезпечний інструмент пропаганди екстремізму, тероризму та рекрутування молодих людей до лав терористичних організацій» [5, с. 9].

Марунченко О. в дисертаційному дослідженні акцентує, що незважаючи на різні тлумачення поняття «інформаційна війна», основною ознакою цього типу кампаній є гостра, агресивна взаємодія протиборчих сторін в інформаційній сфері, яка негативно відбивається на стані політичних комунікацій суспільства в цілому. На його думку, через високу інтенсивність суперечки інформаційні війни погано піддаються управлінню та свідомому регулюванню [6, с. 56]. Використовуючи термінологію Ж. Бодріяра, а саме його поняття «гіперреальність», дослідник інформаційних воєн переконує, що засоби масової інформації насправді перестають відображати дійсність, а самі створюють образи та симулякри, які й визначають цю створену реальність більш реальною, ніж є насправді. Розмірковуючи в дусі постмодернізму, нам здається, що війна завдяки ЗМІ може здатися тотальною симуляцією. За допомогою текстів, які ми чуємо з екранів телевізорів та моніторів ютуб-каналів, війну прагнуть виграти специфічними для класичного розуміння засобами.

В основі будь-якої війни лежить боротьба смислів, що відображаються у способі життя та цінностях протиборчих сторін. У цьому руслі і Курбан Олександр розглядає сучасні інфор-

маційні війни, а саме як протистояння ідей, образів, ідеологій і міфів. Ввівши в науковий обіг поняття «бойові наративи», головною ознакою яких є їх деструктивне спрямування, намагається виокремити близько десятка базових наративів (або супернاراتивів), які поділяються на субнاراتиви за тематикою та напрямками. Кожний базовий бойовий наратив має свою концепцію представлення, на основі якої створюється відповідний контент (меми, інфографіка, тексти, відео, фото). Як працює в інформаційній війні той, чи інший «бойовий наратив» можна зрозуміти на основі моніторингу та контент-аналізу матеріалів інтернет-видань. Так автор спирається на результати моніторингу інформаційного поля України, який на регулярній основі здійснює Центр протидії інформаційним агресіям «AM&PM» при Військовому інституті Київського національного університету імені Тараса Шевченка. Згідно з результатами зведеного аналітичного звіту за 2020 р. із виявлення деструктивних наративів в українському інформаційному полі, експерти Центру «AM&PM» визначили такі основні супернاراتиви, за допомогою яких РФ атакувала Україну: 1) збиття українського пасажирського літака в Ірані; 2) плівки Гончарука та «рука» Сороса; 3) коронавірус в Україні: американські біолабораторії; 4) війна на Сході України; 5) Україна і НАТО; 6) полювання на російськомовних [7, с. 151]. Якщо копнути глибше, то на поверхню піднімемо супернاراتив, який РФ тривалий час множила і множила – це ностальгія за СРСР. До числа гуманітарних технологій, які використовуються для промоції наративу «ностальгія за СРСР», Курбан О. виокремив такі: медіавіруси (вірусний контент), меметичні засоби, фейки, дезінформація, пропаганда.

Розібравшись з основними поняттями та категоріями, перейдемо до аналізу публічних (правових) засад протидії проявам інформаційної війни. Визначення «інформаційна війна» з'явилося в офіційних документах України у 2012 році. Згідно з Указом Президента України «Про Стратегічний оборонний бюлетень України» (що на сьогодні втратив чинність) «інформаційна війна – форма протиборства між суб'єктами (державами, блоками, партіями тощо), що передбачає інформаційний вплив на населення з використанням засобів масової інформації, комп'ютерних мереж тощо з метою формування відповідної суспільної думки, підризу морального духу як усього суспільства, так і окремих його інституцій».[8] Цей Указ втратив чинність на підставі Указу Президента № 240/2016 від 06.06.2016, а чинним є Стратегічний оборон-

ний бюлетень України, затверджений Указом Президента України від 17 вересня 2021 року № 473/2021. Цей документ вже не містить термін «інформаційна війна», хоча апелює до понять «ведення протиборства в інформаційному просторі та кіберпросторі», «кіберборотьба», «кіберзброя». Важливим складовим цього документу є Додаток 2, що містить основні принципи щодо організації системи управління, а саме:

- демократичний цивільний контроль;
- відокремлення функції з формування державної політики у сфері оборони від функції її реалізації;
- відокремлення функції генерування військ (сил) від функції їх застосування;
- об'єднаний характер операцій;
- командні (управлінські) повноваження;
- єдиноначальність управління;
- безперервність управління;
- чітка вертикаль управління;
- децентралізація повноважень для виконання завдання;
- комплексний підхід до організації управління;
- прозорість процесу прийняття рішень [9].

В Україні є низка документів, які визначають головні пріоритети інформаційної безпеки. Насамперед, до таких документів належить: Закон України «Про основні засади забезпечення кібербезпеки України» (2018 рік), Стратегія національної безпеки України (введена в дію Указом Президента України 14 вересня 2020 року), Стратегія кібербезпеки України (затверджена Указом Президента України від 26 серпня 2021 року), Стратегія інформаційної безпеки України (затверджена Указом Президента України від 28 грудня 2021 року).

Стратегія інформаційної безпеки є ключовим документом в законодавстві України, і згідно з ним поняття «інформаційна безпека» визначається як «складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система 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 пору-

шення цілісності інформації з обмеженим доступом» [10]. Указом Президента України від 28 грудня 2021 року № 685/2021 затвердилась Стратегія інформаційної безпеки, а також проголошено Доктрину інформаційної безпеки України (2016 р.) як таку, що втратила чинність. До останнього документу було багато нарікань, як і з боку юристів, так і експертів у галузі інформаційної безпеки. Доктрина носила декларативний характер, не маючи конкретики. «Майбутні зміни до законодавства щодо механізмів інформаційної взаємодії між владою, ЗМІ та суспільством у документі лише «розпливчато» згадуються, але не зазначено, у чому вони мають полягати» [13]. Згідно з Доктриною інформаційної безпеки на Міністерство інформаційної політики покладається моніторинг загроз національним інтересам і національній безпеці в інформаційній сфері, проте «питання контентно-комунікаційної й комунікаційно-контентної взаємодії (на всіх рівнях) влади та суспільства залишається нерозв'язаним» [4, с.165]

Серед глобальних викликів і загроз Стратегія інформаційної безпеки виокремлює такі:

- інформаційна політика рф – є загрозою не лише для України, але й для інших демократичних держав; соціальні мережі є суб'єктами впливу в інформаційному просторі;

- недостатній рівень медіа грамотності в умовах стрімкого розвитку цифрових технологій [10]. На основі глобальних та національних загроз в документі визначається сім стратегічних цілей реалізації Стратегії, а саме:

- протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави;

- забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності;

- підвищення рівня медіакультури та медіаграмотності суспільства;

- 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;

- інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них

територіях України, до загальноукраїнського інформаційного простору;

- створення ефективної системи стратегічних комунікацій;

- розвиток інформаційного суспільства та підвищення рівня культури діалогу [10].

Реалізація Стратегії розрахована на період до 2025 року. В світлі виконання поставлених цілей Кабінет Міністрів України так і не затвердив на сьогодні План заходів з реалізації Стратегії та існує лише у формі проекту Розпорядження Кабінету Міністрів України про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. З цим проектом можна ознайомитися на сайті Міністерства культури та інформаційної політики України [13].

Серед заходів, запланованих в межах окресленого Плану, на нашу думку особливої уваги заслуговує проект «Spravdi», що спрямований на протидію дезінформаційним кампаніям та деструктивній пропаганді, фахова підготовка спеціалістів з раннього виявлення, прогнозування та запобігання гібридним загрозам, забезпечення реалізації Національного проєкту з медіаграмотності «Фільтр» [13].

В межах посилення соціогуманітарної складової внутрішньої політики України, розробки та впровадження цілісної системи соціогуманітарних технологій важливу роль у формуванні заходів протидії інформаційній війні відіграє політика пам'яті. В сучасній Україні у період 2014–2023 рр. вона була докорінно переорієнтована і, по суті, стала важливим напрямом протидії інформаційним атакам у ході війни, яку веде РФ проти України. На думку дослідників Іваненка В., Кривошеїна В. політика пам'яті за каденції третього президента України Віктора Ющенка (2005-2010 рр.) набула чітко вираженого україноцентричного змісту на протипагу державній політиці пам'яті за президентства Леоніда Кучми. Державна політика пам'яті в умовах нинішньої російсько-української війни є тією сферою державного управління, яка найбільш уразлива і чутлива до інформаційних впливів. Її значення дещо недооцінене. Хоч «формування монолітної історичної пам'яті як результат реалізації державної політики пам'яті має забезпечити націю від культурного, світоглядного, політичного розшарування, підсилить доцентрові настрої в суспільстві» [14, с. 20]. Підтвердженням цього можуть слугувати завдання, які покладаються на Український інститут національної пам'яті як орган виконавчої влади в питанні реалізації політики у сфері відновлення та збереження національної пам'яті українського народу. Серед них:

- забезпечення наукового супроводження реалізації Стратегії інформаційної безпеки,

- у тому числі щодо реагування на інформаційні впливи країни-агресора;

- забезпечення функціонування та наповнення інформацією Віртуального музею російської агресії;

- сприяння залученню вітчизняних істориків, політологів та філософів до підготовки спеціальних інформаційних продуктів, у тому числі з метою розвінчування російських історичних фейків та ознайомлення населення із сторінками нашого героїчного минулого [13].

Відповідальним виконавцем у забезпеченні виявлення, прогнозування та запобігання інформаційним загрозам як стратегічного завдання також є Центр протидії дезінформації при Раді національної безпеки та оборони, утворений відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою. До основних завдань Центру належить:

- 1) проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі;
- 2) виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, прогнозування та оцінка наслідків для безпеки національних інтересів України;
- 3) участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку;
- 4) участь у створенні інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;
- 5) розроблення методології виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру;
- 6) сприяння взаємодії держави та інституцій громадянського суспільства щодо протидії дезінформації та деструктивним інформаційним впливам і кампаніям [16].

Водночас, створення та реалізація всіх можливих заходів у сфері протистояння інформаційній агресії, в першу чергу РФ, нівелюється, якщо в суспільстві відсутнє критичне сприйняття інформації та критичне мислення особистості нерозвинене. Як механізм протидії ворожій російській пропаганді можуть виступати також недержавні проєкти, виконуючи завдання протидії інформаційним загрозам

у формі перевірки і спростування перекрученої інформації, посилення медіаграмотності. Так, наприклад, проект StopFake, заснований в 2014 р. Могілянською школою журналістики, не лише виявляє випадки поширення неправдивої інформації про події в Україні, а й ініціював міжнародну дискусію про те, як цьому протистояти.

**Висновки.** В сучасних умовах російсько-української війни, характер боротьби змінився, набувши якостей не лише інформаційної війни. Але при цьому вплив на суспільство інформаційної зброї не зменшується. Інформаційна війна – це одна з граней широкомасштабного вторгнення російської федерації в Україну. Вона розкривається через сукупність певних ідей, які руйнують національну самосвідомість. Але нам, українському суспільству, необхідно втримати зазіхання на знищення державності та національної ідентичності. Стратегічним завданням є необхідність систематичного виконання дій органів державного управління України у напрямку своєчасного виявлення й ліквідації загроз і ризиків негативного впливу «інформаційної зброї» національного інформаційного простору, реалізації державної політики протидії «інформаційній війні», задіяння недержавних громадських організацій у заходах протистояння інформаційним загрозам та здійснення на всіх рівнях ефективного захисту інформаційного суверенітету держави.

#### ЛІТЕРАТУРА:

1. Почепцов Г. Г. Смыслові та інформаційні війни. Інформаційне суспільство. 2013. Вип. 18. С. 21–27. URL: [http://nbuv.gov.ua/UJRN/is\\_2013\\_18\\_6](http://nbuv.gov.ua/UJRN/is_2013_18_6) (дата звернення: 09.02.2023).
2. Магда Є.В. Виклики гібридної війни: інформаційний вибір. Наукові записки Інституту законодавства Верховної Ради України. 2014. № 5. С. 138-142. URL: [http://nbuv.gov.ua/UJRN/Nzizvru\\_2014\\_5\\_29](http://nbuv.gov.ua/UJRN/Nzizvru_2014_5_29) (дата звернення: 02.02.2023).
3. Новородовський В. Інформаційна безпека України в умовах Російської агресії. *Соціум. Документ. Комунікація. Сер. Іст. науки*. 2020. Вип. 9. С. 150-179.
4. Любовець Г. Контент негативу. Як захистити себе та країну в умовах тотального інформаційного протистояння : монографія / Григорій Любовець, Валерій Король. Київ : Видавничий дім «Києво-Могілянська академія», 2021. 266 с.
5. Саган О.В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : автореф. дис. ... канд. політ. наук: 21.01.01. Київ, 2021. 22 с. URL: [https://niss.gov.ua/sites/default/files/2021-04/06.04.2021\\_1-avtorefer\\_pidpis.-sagan\\_sig.pdf](https://niss.gov.ua/sites/default/files/2021-04/06.04.2021_1-avtorefer_pidpis.-sagan_sig.pdf) (дата звернення: 09.02.2023).
6. Марунченко О.П. Інформаційна війна в сучасному політичному просторі : дис. ... канд. політ. наук : 23.00.02. Одеса, 2012, 208 с. URL: <http://dspace.pdpu.edu.ua/bitstream/123456789/1021/1/%d0%9c%d0%b0%d1%80%d1%83%d0%bd%d1%87%d0%b5%d0%ba%d0%be%20%d0%9e%d0%bb%d0%b5%d0%ba%d1%81%d0%b0%d0%bd%d0%b4%d1%80%20%d0%9f%d0%b5%d1%82%d1%80%d0%be%d0%b2%d0%b8%d1%87.pdf> (дата звернення: 09.02.2023).

7. Курбан О. Бойові нарративи в системі сучасних геополітичних інформаційних війн (досвід російсько-української гібридної інформаційної війни 2014–2021 рр.). *Синопис: текст, контекст, медіа*. 2021. № 27(3). С. 149–158. URL: [http://nbuv.gov.ua/UJRN/stkm\\_2021\\_27\(3\)\\_6](http://nbuv.gov.ua/UJRN/stkm_2021_27(3)_6). (дата звернення: 08.02.2023).

8. Стратегічний оборонний бюлетень України: схвалено Указом Президента України 29 грудня 2012 р. № 771/2012. URL: <https://zakon.rada.gov.ua/laws/show/771/2012#n16> (дата звернення: 03.02.2023).

9. Стратегічний оборонний бюлетень України, затверджений Указом Президента України від 17 вересня 2021 року № 473/2021. URL: <https://www.president.gov.ua/documents/4732021-40121> (дата звернення: 03.02.2023).

10. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 року № 685/2021 URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 09.02.2023).

11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 року № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 09.02.2023).

12. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/2017

13. Жуган Вікторія Доктрина інформаційної безпеки України – це лише декларація – експерти. URL: <https://www.radiosvoboda.org/a/28336852.html> (дата звернення: 24.02.2023).

14. Громадське обговорення проєкту розпорядження Кабінету Міністрів України «Про затвердження Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року» URL: <https://mkp.gov.ua/news/7512.html> (дата звернення: 24.02.2023).

15. Іваненко В., Кривошеїн В. Державна політика пам'яті в сучасній Україні в умовах інформаційної війни (2014–2021 рр.). *Науково-теоретичний альманах Грані*, 25(2), с.16-21. URL: <https://grani.org.ua/index.php/journal/article/view/1756> (дата звернення: 14.02.2023).

16. «Неонацисти, антиросія, карателі»: путін близько півгодини свого виступу в парламенті присвятив Україні та Заходу. URL: <https://www.slovoidilo.ua/2023/02/21/novyna/polityka/neonacysty-antyrosiya-karateli-putin-pivhodyny-svoho-vystupu-parlamentiprysvyatyv-ukrayini-ta-zaxodu> (дата звернення: 25.02.2023).

17. Про Центр. Центр протидії дезінформації при РНБО. URL: <https://cpd.gov.ua/documents/про-центр/> (дата звернення: 25.02.2023).

18. Хорошко В., Хохлачова Ю., Пірцхалава Т., Іванченко І. Інформаційна зброя як інструмент інформаційної війни. *Захист інформації*. Том 24, № 2, квітень-червень 2022. С. 50–58. URL: <https://jrn1.nau.edu.ua/index.php/ZI/article/view/16930> (дата звернення: 25.02.2023).