DOI 10.52363/2414-5866-2024-1-2
УДК 35.975(477)

***Лопатченко І.М.**, к.держ.упр., ННВЦ НУЦЗУ, м. Харків,*
ORCID: 0000-0002-4838-2154,
***Помаза-Пономаренко А.Л.**, д.держ.упр., с.д., ННВЦ НУЦЗУ, м. Харків,*
ORCID: 0000-0001-5666-9350,
***Батир Ю.Г.,** к.е.н., доц., ННВЦ НУЦЗУ, м. Харків,*
ORCID: 0000-0001-5282-3680

***Lopatchenko I.**, PhD of Public Administration, Lecturer of the Department of Public Administration in the sphere of Civil Defense of the Training Research and Production Centre of National University of Civil Protection of Ukraine, Kharkiv,*
***Pomaza-Ponomarenko A**., Doctor bin Public Administration, Senio rResearcher, Head of the Scientific Department for State Security Problems of the Training Research and Production Centre of National University of Civil Protection of Ukraine, Kharkiv, ORCID: ORCID: 0000-0001-5666-9350,*
***Batyr Yu.**, PhD of Economic Sciences, associate professor, National university of civil defence of Ukraine, Kharkiv*

ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

STATE REGULATION N THE SPHERE OF INFORMATION SECURITY OF UKRAINE UNDER THE CONDITIONS OF THE STATE OF MARTIAL

У сучасних військово-політичних реаліях важко і навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати війни та політичні кризи без жодного пострілу, формуючи та розпалюючи внутрішні протиріччя. Така тактика характерна для війн нового формату – гібридних, де безпосередній військовий фактор є лише однією зі складових цілого. Варто звернути увагу на те, що в умовах, коли цілий комплекс інформації розрахований на маніпулювання громадською думкою, свідомістю людини та подається за допомогою фізіологічних і психологічних методів і засобів її сприйняття, постає питання низького рівня інформаційної культури, що спричиняє зниження здатності людини до критичного сприйняття, стає важливим аналіз та оцінка отриманої інформації. У цьому випадку здатність до формування власної думки практично відсутня. Цілком правильно вважати, що інформаційна безпека

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

передбачає: належний рівень інформаційної культури, тобто теоретичну і практичну підготовку особистості, що забезпечує захист і реалізацію її життєво важливих інтересів і гармонійний розвиток в умовах інформаційного суспільства, незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку та задоволення інформаційних потреб особи незалежно від наявності інформаційних загроз; забезпечення, розвиток і використання інформаційного середовища в інтересах особи; захист від різноманітних інформаційних загроз. У статті розкриваються аспекти забезпечення інформаційних прав та свобод суспільства з врахуванням захисту інформаційної безпеки держави в умовах воєнного стану. Визначаються пріоритетні напрямки захисту інформаційної безпеки. Розглядаються типові загрози інформаційній безпеці та їх походження. Також, важливим є висновок про те, що забезпечення інформаційної безпеки полягає у створенні заходів щодо забезпечення інформаційної безпеки.

Ключові слова: *інформаційна безпека, інформаційна культура, загрози інформаційній безпеці.*

In modern military realities, it is difficult and even inappropriate to deny the role of information as a tool of confrontation, in fact - a weapon. Information allows you to win the war without firing a single shot, creating and fueling internal contradictions. Such tactics are characteristic of new format wars - hybrid wars, where the direct military factor is only one of the components of the whole. It is worth paying attention to the fact that in conditions where a whole set of information is designed to manipulate public opinion, human consciousness and is presented with the help of physiological and psychological methods and means of its perception, the issue of a low level of information culture arises, which causes a decrease in a person's ability to critical perception , the analysis and evaluation of the received information becomes important. In this case, the ability to form one's own opinion is practically absent.

Key words: *information security, information culture, threats to information security.*

Постановка проблеми. У сучасних умовах інформатизації суспільства, за допомогою фейкової або маніпулятивної інформації ворог не втрачає можливість скористатися цим на свою користь, посіяти в суспільстві страх та панічні настрої, дестабілізувати політичну та соціально-економічну ситуацію в Україні. Вторгаючись в український інформаційний простір, ворог робить замах на громадянську ідентичність українців. Актуальність статті полягає у необхідності аналізу наявних механізмів протидії інформаційним операціям країни-агресора в умовах воєнного стану.

Варто звернути увагу на те, що в умовах, коли цілий комплекс інформації розрахований на маніпулювання громадською думкою,

свідомістю людини та подається за допомогою фізіологічних і психологічних методів і засобів її сприйняття, постає питання низького рівня інформаційної культури, що спричиняє зниження здатності людини до критичного сприйняття, стає важливим аналіз та оцінка отриманої інформації. У цьому випадку здатність до формування власної думки практично відсутня.

Цілком правильно вважати, що інформаційна безпека передбачає: належний рівень інформаційної культури, тобто теоретичну і практичну підготовку особистості, що забезпечує захист і реалізацію її життєво важливих інтересів і гармонійний розвиток в умовах інформаційного суспільства, незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку та задоволення інформаційних потреб особи незалежно від наявності інформаційних загроз; забезпечення, розвиток і використання інформаційного середовища в інтересах особи; захист від різноманітних інформаційних загроз [6].

Ми є свідками того, як ведеться інформаційний вплив спрямований на свідомість людини. Об'єктом даного впливу є як окремі особи, групи осіб, так і цілі держави. Психологічний вплив здійснюється за допомогою засобів масової інформації, а підставою для використання такого впливу є легкість сприйняття та поверхневість. Створення масових інформаційних атак, ботів, фейків, як свідчать сучасні реалії, є дієвими інструментами для дезорієнтації суспільства, залякування, маніпулювання та паніки. Спеціально створені інформаційні ресурси привчають людину бездумно сприймати інформацію та вірити в неї. Питання інформаційної безпеки та культури в умовах війни є питанням виживання людини, суспільства і держави. Адже забезпечення інформаційної безпеки обумовлено не тільки інтересами держави, але і інтересами людини в контексті забезпечення її прав та свобод [6]. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність та достовірність.

Аналіз останніх досліджень і публікацій. Проблемам державного регулювання інформаційної безпеки в умовах війни присвятили такі вчені, як В. Бондаренко Ю. Горбань, М. Дмитренко, Ф. Медвідь, А. Пишна, Я. Михальский, О. Черевко Д. Смотрич, Л. Браілко, Т. Француз-Яковець, І. Шинкаренко, І. Залєвська, Г. Удренас, Л. Мазуренко та ін.

Постановка завдання. Метою статті є дослідити окремі особливості державного регулювання інформаційної безпеки в умовах воєнного стану.

Виклад основного матеріалу дослідження. Національні інтереси України вимагають забезпечення сприятливих умов політичного розвитку країни. Так, інтереси особи полягають у реальному забезпеченні політичних прав і свобод громадян, суспільство потребує зміцнення демократії, а інтереси держави виражаються у необхідності ефективного захисту конституційного ладу суверенітету та територіальної цілісності країни, вста-

новлення та підтримання політичної стабільності, включаючи стабільність державної влади та її інститутів. В інформаційній сфері на основі національних інтересів України формуються стратегічні та поточні завдання політики держави щодо забезпечення інформаційної безпеки [6].

З метою забезпечення інформаційної безпеки в Україні Указом Президента України від 25.02.2017 р. була затверджена «Доктрина інформаційної безпеки України» [9]. У жовтні 2021 року була прийнята Стратегія інформаційної безпеки, що передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегією кібербезпеки України, затвердженою, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. У Стратегії було зазначено, що: «інформаційна політика РФ – загроза не лише для України, але й для інших демократичних держав» [10]. Згідно зі Стратегією, інформаційна безпека України – 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 порушення цілісності інформації з обмеженим доступом [9]. В умовах воєнного стану в Україні загострилось питання необхідності єдиної інформаційної політики. У зв'язку із цим Президент України підписав Указ № 152/2022, Сучасні проблеми правового, економічного та соціального розвитку держави 140 яким увів в дію Рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану».

В сучасних умовах війни 18.03.2022 р. прийнято рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки» [10]. Наразі в Україні функціонує також Центр протидії дезінформації при РНБО України, на сайті якого можна ознайомитись з актуальною інформацією та подіями в цій сфері.

Центр протидії дезінформації (далі – Центр) є робочим органом Ради національної безпеки і оборони України, утвореним 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. У своїй діяльності висвітлює тенденції з інформування стану військової справи, ОПК, боротьби зі злочинністю та корупцією, зовнішньої та внутрішньої політики, економіки, об'єктів критичної інфраструктури, екології, охорони здоров'я, соціальної сфери, формування суспільної свідомості, науково-технологічного напряму тощо. Основна увага зосереджена на протидії поширенню неправдивої інформації та боротьбі з інформаційним тероризмом. Центр функціонує відповідно до Конституції і законів України, актів Президента України та Кабінету Міністрів України, міжнародних договорів України, цього Положення, а також розпоряджень Секретаря Ради національної безпеки і оборони України.

Основними завданнями Центру є:

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, чинників, які впливають на їх формування, прогнозування та оцінка наслідків для безпеки національних інтересів України;

3) забезпечення Ради національної безпеки і оборони України, Голови Ради національної безпеки і оборони України інформаційно-аналітичними матеріалами з питань забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

4) підготовка та внесення Раді національної безпеки і оборони України, Голові Ради національної безпеки і оборони України пропозицій щодо: визначення концептуальних підходів у сфері протидії дезінформації та деструктивним інформаційним впливам і кампаніям; координації діяльності та взаємодії органів виконавчої влади з питань національної безпеки в інформаційній сфері, забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою; здійснення системних заходів, спрямованих на посилення спроможностей суб'єктів сектору безпеки та оборони, інших державних органів задля забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним

інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою, розвитку національної інфраструктури у відповідній сфері; удосконалення системи правового та наукового забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

5) участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку;

6) участь у розробленні та реалізації Стратегії інформаційної безпеки України, здійсненні аналізу стану її реалізації, зокрема з питань ефективності заходів щодо протидії дезінформації;

7) участь у створенні інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

8) розроблення методології виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру;

9) сприяння взаємодії держави та інституцій громадянського суспільства щодо протидії дезінформації та деструктивним інформаційним впливам і кампаніям, організація та участь в інформаційно-просвітницьких заходах з питань підвищення медіа-грамотності суспільства;

10) вивчення, узагальнення й аналіз досвіду інших держав і міжнародних організацій з протидії дезінформації та підготовка пропозицій щодо його використання в Україні;

11) бере участь у визначенні пріоритетів залучення міжнародної технічної допомоги з питань забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

Сьогодні Центр активно залучений у протидії російській агресії. Його пріоритетами є: оперативне інформування населення; розкриття дезінформації та маніпуляцій; забезпечення інформаційної безпеки; боротьба з інформаційним тероризмом. Як один із результатів роботи, фахівцями центру було розроблено освітній курс «Дезінfакція твого інфопростору».

Відповідно до дослідження Центру, кожна людина знаходяться в так званій «інформаційній бульбашці». Це стан інтелектуальної ізоляції, тобто явище, що спричинене результатами персоналізованого пошуку, в якому алгоритм вебсайту вибірково припускає, яку інформацію ти хотів би бачити, базуючись на інформації про тебе ж (як-от розташування, поведінка «після кліка» та історія пошуку). Як наслідок, їх відділяють від інформації, яка не відповідає твоїм поглядам, фактично ізолюючи тебе у власній культурній або ідеологічній бульбашці. Це відбувається двома шляхами – алгоритм і персоналізація. Алгоритм – це лайки, коментарі, шери, хештеги

та пошукові слова: алгоритм соцмережі завжди аналізує твою мережеву активність і на її основі формує стрічку новин, рекомендує активності чи товари, життєво необхідні виключно тобі. Так працюють усім нам відомі Instagram, TikTok та навіть Google. Персоналізація – деякі соціальні медіа дозволяють тобі персоналізувати контент, тобто самостійно пройти процес створення контенту, що буде релевантним, цікавим та корисним виключно для тебе. Так, до прикладу, працює популярний Telegram. Також, аналітичним відділом виділяють три стани людини під час перебування в «інформаційній бульбашці»:

1. «Спіраль мовчання» – ситуація, коли ти відчуваєш зростаючу потребу приховувати свої погляди, якщо вони не підтримуються більшістю. Перед тим, як висловити свою думку зору щодо якогось явища або ситуації, ти схильний несвідомо перевіряти, чи поділяє твої погляди більшість. Якщо так, то у тебе з'являється вища мотивація та бажання вільно висловлювати свої переконання. Якщо ж його точка зору підтримується невеликою частиною аудиторії, тобто меншістю, то ти, найімовірніше, не матимеш стимулу відкрито говорити непопулярні переконання на публіці.

2. Ефект ехокамери – ефект, що утворюється під час обговорення новин та посилається на ситуації, коли переконання посилюються або підсилюються спілкуванням і повторенням всередині закритої системи та ізолюються від спростування.

3. «Підтвердження упередження» – тенденція шукати або інтерпретувати інформацію таким чином, щоб вона підтверджувала твої власні переконання або гіпотези. «Підтвердження упередження» проявляється тоді, коли ти збираєш або запам'ятовуєш інформацію вибірково чи інтерпретуєш її упереджено. І чим емоційно напруженіше питання або сильніше переконання, тим сильніше проявляється ефект. Також ти схильний до інтерпретування неоднозначної інформації з певного питання так, щоб підтримати власну усталену позицію щодо такого питання.

Після того, як твоя персональна інформаційна бульбашка сформувалася, при чому неважливо яким саме чином – завдяки алгоритмам чи завдячуючи персоналізації, до неї починає «просочуватися» ворожа пропаганда. І потрапляє вона до інформаційної бульбашки конкретної людини різними шляхами, наприклад через:

– Рекламу та рекомендації.
– Ботів, що враховують твої вподобання.
– Блогерів та псевдоекспертів.
– Псевдомісцеві медіа.
– Псевдопатріотичні медіа.

Розглянемо їх більш детально.

Реклама та рекомендації – зважаючи на дані щодо активності користувача в мережі, котрі акумулюють алгоритми різних соцмереж, пропа-

гандисти можуть налаштувати таргетовану рекламу таким чином, що вона зможе проникнути саме в ту інформаційну бульбашку, яку бажають зловмисники. Якщо ж над змістом реклами попрацюють не тільки пропагандисти, а ще й психологи, то людина обов'язково на неї відреагує. Це ж стосується і контенту, рекомендованого різними соцмережами та месенджерами.

Боти, що враховують вподобання. Вивчивши інформацію про конкретну людину, зокрема список друзів, музичні чи спортивні вподобання, хобі, перелік спільнот, в яких перебуває користувач, чи навіть відомості про подорожі, пропагандист може створити або скоригувати профіль бота таким чином, що він зацікавить цю людину та, відповідно, потрапить до її інформаційної бульбашки. Тому, чим більше даних відкрито для всіх користувачів мережі, тим вища ймовірність потрапити «на гачок» до такого бота.

Блогери та псевдоексперти. Отримавши інформацію про вподобання, пропагандисти враховують людину як одиницю тієї чи іншої цільової аудиторії, що є об'єктом «опрацювання» блогерів та псевдоекспертів. Через діяльність таких блогерів та псевдоекспертів до інформаційної бульбашки проникають необхідні пропагандистам деструктивні наративи. І зважаючи на те, що в роботі блогерів та псевдоекспертів від самого початку було враховано вподобання конкретної людини, такі наративи не сприйматимуться нею вороже.

Псевдомісцеві ресурси. Всім цікаво читати новини про власне місто чи регіон. І це правило працює в будь-якому куточку нашої планети. Тому, щоб бути ближче до людини пропагандисти створюють псевдомісцеві ресурси, які імітують роботу локальних медіа. У стрічках таких медіа, серед нейтральних чи навіть патріотичних публікацій, заховані необхідні пропагандистам меседжі та наративи. Таку роботу пропагандисти проводять для того, аби людина щось не запідозрила і продовжувала дивитися та читати.

Псевдопатріотичні та інсайдерські ресурси. Не можна заперечувати факт того, що людині завжди було цікаво знати щось трохи більше або трохи швидше за інших. Звісно, що такою особливістю на можуть не скористатися пропагандисти. І щоб задовольнити цю цікавість, вони створюють контрольовані інсайдерські медіа, які люди читають без найменшого докору сумління. Що ж до псевдопатріотичних медіа, то тут ситуація дещо схожа, адже за часів протистояння росії, ті чи інші патріотичні ресурси є у кожній персональній інформаційній бульбашці. Як, на жаль, і псевдопатріотичні.

Зважаючи на все вищезазначене, фахівці Центру розробили конкретні поради та рекомендації про те, як зруйнувати небезпечну інформаційну бульбашку:

1. Усвідомити, що ти в інформаційній бульбашці. У цьому людині

допоможе уважність під час перегляду контенту та критичне мислення (аналіз інформації з декількох абсолютно різних джерел дозволяє відшукати «спільну» інформацію, яка, скоріше за все, і є об'єктивною).

2. Отримуйте інформацію тільки з офіційних джерел. Це дозволить розуміти стан справ усередині нашої країни та завжди бути в курсі актуальних українських новин.

3. Диференціюйте джерела інформації, з яких люди споживають контент. Це дозволить населенню отримувати контент із різними точками зору та порівнювати його.

4. Налаштуйте власну інформаційну бульбашку таким чином, щоб отримувати різнорідну інформацію й аналізувати її.

Висновки. Підсумовуючи відзначимо, що нині інформація як зброя є доволі серйозним засобом ведення війни оскільки її технологічна інноваційність, потужність є небезпечними. Відповідно, інформаційна безпека України має базуватися на синхронізованих діях структур держави та громадянського суспільства. Під час війни суттєво зросла роль інформаційної культури як чинника підсилення опору дезінформаційній зброї громадянами та збереження державного суверенітету України. Нинішня війна добре демонструє, що інформація використовується і в якості зброї масового ураження. У зв'язку з цим потрібно побудувати ефективний механізм, котрий би гарантував інформаційну безпеку України, в основу якого, на нашу думку, важливо покласти такі складові: 1) технічну – створити належну технічну базу функціонування інформаційної безпеки; 2) політичну – державна політика повинна бути направлена на забезпечення інформаційної безпеки; 3) правову – оформлення всіх заходів інформаційної безпеки якісними нормативно-правовими актами.

Аналіз проблеми забезпечення інформаційної безпеки громадянина та держави під час бойових дій та конфліктів дозволяє дійти висновку, що інформаційна безпека відіграє надзвичайно важливу роль особливо під час війни. Адже дезінформація може викликати панічні настрої серед населення, негативно вплинути на перебіг подій, прискорювати внутрішню міграцію населення, що може негативно позначитись на даєздатності Збройних Сил України, а також на фізичному й психічному стані громадян. Ефективно протидіяти інформаційній агресії видається, на нашу думку, можливим за рахунок залучення до цього процесу міжнародних організацій, інституцій та міжнародної спільноти загалом. Практика показує – кордонів для ведення інформаційної війни не існує. Начасі захищати відкритий інформаційний простір країни від ворожих впливів та навіювань. Перспективами подальших досліджень є проведення аналізу зарубіжного досвіду протидії поширенню фейків в умовах інформаційних війн та висвітлення воєнних подій.

Список використаних джерел:

1. Бодрук О.С. Структури воєнної безпеки: національний та міжнародний аспекти: Монографія. Київ: НІПМБ. 2001.

2. Гончаренко О., Джангужин Р., Лисицин Е. Громадянськй контроль і система національної безпеки, Національна безпека України. 2003. № 1. С. 39-46.

3. Залєвська, І.І., Удренас, Г.І. Інформаційна безпека України в умовах російської військової агресії, Південноукраїнський правничий часопис. 2022. № 1-2. С. 20–26.

4. Конституція України. 2019. URL: https://zakon.rada.gov.ua/laws/show/27-20#n2

5. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса. 2015. № 3. С. 220-237.

6. Мазуренко Л.І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. Вісник Харківського національного університету імені В.Н. Каразіна, серія «Питання політології». 2022. № 42. С. 50-57. https://doi.org/10.26565/2220-8089-2022-42-08.

7. Пархоменко-Куцевіл, О. І. Забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні: м-ли Всеукр. наук.-практ. конф. у 3х т. Київ: ДЗВО «Університет менеджменту освіти» НАПН України. 2022. № 1. С. 39-43.

8. Писаренко, Л.М. Фейки як інструменти інформаційної війни. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття»: у 2 т.: м-ли Міжнар. наук.-практ. конф. Одеса: Видавничий дім «Гельветика». 2022. № 1. С. 859-861.

9. Про Доктрину інформаційної безпеки України: Указ Президента України №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017- 21374.

10. Про рішення Ради національної безпеки і оборони України 2021: Указ Президента України № 685/2021 від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://www.president.gov.ua/documents/6852021-41 069.

11. Цимбалюк В.С. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики, Адміністративне право і процес. 2014. № 2(8). С. 22–30.

References:

1. Bodruk, O. 2001. Structures of military security: national and international aspects: Monograph. Kyiv: NIPMB.
2. Ghoncharenko, O., Dzhanghuzhyn, R., Lysycyn, E. 2003. Civil control and the system of national security, National security of Ukraine. 1: 39–46.
3. Zaljevsjka, I., Udrenas, Gh.. 2022. Information security of Ukraine in the conditions of Russian military aggression, South Ukrainian legal journal. 1-2: 20–26.
4. Constitution of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96- %D0%B2%D1%80.
5. Kochubej, L. 2015. State information security. tools for the protection of the Ukrainian information field (on the example of the features of information and communication technologies in modern Donbas), Scientific notes of the Institute of Political and Ethnonational Studies named after I.F. Kurasa. 3: 220- 237.
6. Mazurenko, Lyudmila. 2022. Information Security in the Terms: The Russian-Ukrainian War: Challenges and Threats. The journal of V. N. Karazin Kharkiv National University. Series «Issues of Political Science» 42: 50-57. https://doi.org/10.26565/2220-8089-2022-42-08.
7. Parkhomenko-Kucevil, O. 2022. Ensuring information security during military operations and hostilities. Public management and administration in the conditions of war and in the post-war period in Ukraine: materials of Vseukr. science and practice conf. in three volumes. Kyiv: DZVO «University of Education Management» National Academy of Sciences of Ukraine 1: 39-43.
8. Pysarenko, L.2022. Fakes as tools of information warfare, The European choice of Ukraine, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century: in 2 volumes: materials of International Sciences.- practice conf. Ukraine, Odesa: «Helvetika» publishing house 1: 859-861.
9. About the Doctrine of Information Security of Ukraine: Decree of the President of Ukraine No. 47/2017 «On the Decision of the National Security and Defense Council of Ukraine dated December 29, 2016 «On the Doctrine of Information Security of Ukraine». URL: https://www.president.gov.ua/documents/472017- 21374.
12. About the decision of the National Security and Defense Council of Ukraine 2021: Decree of the President of Ukraine No. 685/2021 dated October 15, 2021 «On Information Security Strategy». URL: https://www.president.gov.ua/documents/6852021- 41069.
10. Cymbaljuk, V. 2014. Legal regulation of information security in Ukraine: problems of theory and practice, Administrative law and process 2(8): 22-30.

дата надходження статті: 26.04.2024
дата прийняття статті: 23.05.2024
дата публікації: 28.06.2024