DOI 10.31558/2519-2949.2024.2.5
УДК 323.2+351]:004.77

ORCID ID: https://orcid.org/0000-0002-8758-5798
Віннічук О. В., Кам'янець-Подільський національний університет імені Івана Огієнка

ORCID ID: https://orcid.org/0000-0002-7700-972X
Маркітантов В. Ю., Кам'янець-Подільський національний університет імені Івана Огієнка

ВИМІРИ БЕЗПЕКИ В ЕПОХУ ЦИФРОВОГО СУСПІЛЬСТВА

У статті проаналізовано сутність безпеки як соціального, культурного, економічного та політичного явища. Актуалізовано, що в умовах сьогодення питання безпеки, безпечного середовища, безпекової політики в усіх сферах життя суспільства є нагальним.

Розкрито проблему взаємообумовленості безпекового простору для сучасного суспільства та дотримання прав людини. Взято до уваги аналітичні дані доповіді Моніторингової Місії ООН з прав людини, Управління Верховного комісара ООН з прав людини, розвідки відомих дослідників-практиків у галузі безпекової політики. Доведено, що в умовах розвитку сучасного «мережевого» суспільства посильну роль відіграють інформаційні технології нового покоління – хай-тек (високотехнологічні) та хай-сенсоро (високі сенсорно-технологічні) технології. Завдяки зазначеним технологіям формується нова модель безпекових взаємовідносин на рівні громадянин-громадянин, громадянин-держава, держава-держава тощо. Акцентовано увагу на тому, що в сучасному суспільстві новітні інформаційні технології сприяють розбудові демократії та водночас виступають інструментом її дестабілізації. До прикладу, в умовах інформаційної війни всі заходи в інформаційному просторі (фейки, пропаганда, маніпуляції) спрямовані проти критично мислячих членів суспільства. Доведено на прикладі російсько-української війни, що домінуючим у протистоянні агресору, окрім військового, залишається інформаційний простір. Цей факт засвідчує потужність нового формату управління суспільством у боротьбі за безпечне середовище. Важливим аспектом безпекової політики під час російсько-української війни стала активність онлайнових волонтерських рухів. У підсумку обґрунтовано про важливість посилення захисту українського кіберпростору, яка постала ще з 2014 року. Визначено пріоритетні напрями забезпечення інформаційної безпеки України

Ключові слова: *безпека, інформаційне суспільство, інформаційна безпека, хай-тек, хай-сенсоро, гібридна війна*

Постановка проблеми. Цифровізація суспільства є одним з найважливіших трендів нашого життя. Вона стосується не лише сфери сучасних інформаційних та комунікаційних технологій, але й економіки, політики, культури тощо.

Цифровий характер розвитку суспільства пропонує принципово нову модель взаємовідносин на різних рівнях: громадянин-громадянин, громадянин-держава, держава-держава, держава-міжнародна організація (ТНК) тощо.

Усвідомлюючи значущість формування необхідного для життя та розвитку суспільства безпечного простору, феномен «безпека» як соціальне, культурне, економічне, політичне явище в умовах сьогодення займає пріоритетне місце. Формування та утримання безпечного простору надають впевненості у майбутньому та стимулюють до революційних змін.

Мета статті передбачає розкриття сутності безпеки як явища постглобального світу та визначення її ролі в епоху цифрового суспільства.

Виклад основного матеріалу. В умовах сьогодення зусилля світових лідерів спрямовані на формування безпекового простору у всіх його проявах (військовому, політичному, економічному, цифровому тощо).

© Віннічук О. В., Маркітантов В. Ю., 2024

Серед основних трактувань безпеки як явища можна виокремити наступні:

1. Концепція, яка розглядає безпеку як теорію, що походить з необхідності реалізації основних потреб людини. Вона ґрунтується на «Програмі розвитку ООН». Основні положення підходу розкрито у таких твердженнях:

– суб'єктом безпеки особи є люди, а не держави чи суспільні групи;
– компоненти безпеки особи взаємозалежні;
– безпека особи пов'язана з якістю життя людей, суспільства, політичного процесу, а все, що знижує цю якість, загрожує безпеці.

2. Модель розвитку в межах концепції безпеки особи пояснює його як основу для існування та розвитку людини. Модель розвитку передбачає активну взаємодію на рівні громадянин-громадянин, громадянин-держава, держава-держава, трансформуючись у модель безпекових взаємин. Фахівці наголошують, що дана модель сприятиме мінімізації негативних наслідків глобалізації та глобалізаційних процесів.

3. Підхід розглядає появу концепції безпеки особи, як наслідок зміщення акцентів у гарантуванні національної безпеки з традиційних на нетрадиційні загрози в умовах глобалізації та «розмивання» суверенітету [6, с. 70].

Аналізуючи безпеку як соціальне явище відомий німецький дослідник У. Бек у праці «Суспільство ризику. На шляху до другого модерну» доводить, що збільшення небезпек в умовах модернізації змушує трактувати суспільство нової епохи як «суспільство ризиків» [17]. Так, у доповіді Моніторингової Місії ООН з прав людини, яка охоплює період від серпня 2020 по січень 2021 року зазначається, що найбільші проблеми у сфері безпеки та порушення прав людини в Україні були зафіксовані через ведення бойових дій, кризу системи правосуддя та пандемію [2].

В контексті сучасний наукових досліджень безпека характеризується не лише у формально-інституційному аспекті, а й як сукупність цінностей , які забезпечують права, свободу, рівність.

Чимало дослідників звертають увагу на формування нової парадигми безпеки як явища, виводячи її з військової площини на новий рівень – технологічний (цифровий), адже стає зрозуміло на прикладі гібридної російсько-української війни, що так звані м'які чи невійськові аспекти ведення війни є пріоритетними.

В умовах гібридної війни держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає актуальних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки й ідеями верховенства права – це стратегічно важливе завдання для Української держави [4, с. 224].

Аналізом безпеки як інформаційного явища в умовах розвитку сучасного мережевого суспільства займається плеяда українських науковців, серед яких варто відзначити О. Курбана, який здійснює аналіз практичних аспектів сучасних інформаційних війн у мережевому он-лайн просторі [3], І. Руснака та О. Рупташ, які актуалізують питання безпекових аспектів сьогодення у різних вимірах та концептуалізують поняття «інформаційна безпека» [15], В. Новородовського, який актуалізує питання щодо оптимальних шляхів захисту інформаційного простору держави в умовах війни, підвищення рівня безпеки в епоху цифрового суспільства [7] та ін.

Розвиток цифрових технологій відкриває для України нове «вікно можливостей», сприяє підвищенню якості життя громадян та, водночас, породжує нові виклики щодо формування її безпекового простору в умовах сьогодення.

Основні аспекти забезпечення інформаційної безпеки в епоху цифрового суспільства відображаються в Законах України «Про національну безпеку України», «Про концепцію національної програми інформатизації», «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», Стратегії національної безпеки України, Стратегії інформаційної безпеки України тощо.

Досягнення цілей цифрового розвитку України стало пріоритетним в умовах сьогодення та усвідомлюються владною елітою та суспільством. Про це свідчать ухвалені такі нормативні акти як розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» [13] та Цифрова адженда України – 2020 [16], Отримав схвальних відгуків й Проект Закону України «Про цифровий порядок денний України» [14].

Серед пріоритетних напрямів зазначених нормативних документів є: 1) розвиток безпечного надійного кіберпростору; 2) захист державних електронних інформаційних ресурсів та інформаційної інфраструктури; 3) захист критичної інфраструктури; 4) розвиток потенціалу сектору безпеки і оборони у сфері кібербезпеки; 5) боротьба з кіберзлочинністю тощо [7, с. 165].

Цифровий характер розвитку сучасного суспільства (суспільства епохи хай-сенсоро) посилює швидкими темпами потребу у застосуванні технологій штучного інтелекту у всіх сферах життя суспільства. Виміри безпеки такого середовища є невизначеними та потребують посилення спроможностей національної системи кібербезпеки, оскільки кіберпростір перетворився на ключовий транскордонний простір ведення інформаційного протистояння.

Різноманітні реальні й удавані «хактивісти», «кіберпартизани», «кіберополчення», а також спеціальні підрозділи різних безпекових відомств, зосереджених на протистоянні у кіберпросторі, стають важливим елементом кібератак, а також ведення спеціальних психологічних операцій у соціальних мережах.

У 2014 році на теренах України з метою протидії російській агресії було започатковано недержавний проєкт Інформаційний спротив (ІС). Його основним завданням стала протидія зовнішній ворожій інформаційній загрозі у різних сферах суспільного та державного життя. Фактично, від початку російської агресії ІС, шляхом верифікації інформаційних джерел сповіщав про хід російсько-української війни, а також викривав факти неправдивої інформації зі сторони проросійських ЗМІ.

Іншим проєктом, який протидіяв російській інформаційній агресії став StopFake. Починаючи з 2014 року організація спростувала ряд міфів, фейків, які поширювалися у ЗМІ та соцмережах. Також проєкт спрямований на формування рекомендацій щодо розпізнання неправдивої інформації (StopFake) [7, с. 166].

Не менш важливим проектом стало створення сайту «Інформаційних військ України». Його робота побудована на донесенні правдивих новин до суспільства та спростуванні фейкових новин у соціальних мережах. Важливо, що з метою протидії інформаційним загрозам, поширення правдивої інформації про перебіг російсько-української війни та посилення інформаційної безпеки, до зазначених проектів долучаються не лише аналітики міністерств, блогери, але й громадяни.

Початок відкритої фази російсько-української війни 24 лютого 2022 року значно актуалізував потребу в посиленні захисту українського кіберпростору. Адже за короткий час було зафіксовано ряд повідомлень про кібератаки на вебсайти державних органів, установ, організацій та ЗМІ. Так, наприклад, за результатами аналітичного звіту «Війна у цифровому вимірі і права людини», 7 повідомлень стосувалося кібератак на офіційні вебсайти органів державної влади та органів місцевого самоврядування, 23 – на сайти ЗМІ та на соціальні мережі, 2 – на вебсайти ГО [1, с. 7].

Напоширенішими форматами вторгнення в український кіберпростір з боку агресора стали кібератаки веб-сайтів органів державної влади, організацій, ЗМІ, фішинг-атаки, створення фейкових веб-ресурсів, поширення неправдивої інформації серед суспільства тощо.

Важливим фактором безпекової політики в умовах війни стало створення «ІТ-армії» як самоорганізованого волонтерського руху, який із 24 лютого долучився до блокування / ускладнення роботи російських вебресурсів пропагандистських ЗМІ, урядових сайтів, банків, корпорацій, підприємств авіаційної сфери та сфери обслуговування.

Зважаючи на стрімке впровадженням цифрових технологій та формуванням цифрових навичок громадян, важливим є процес формування інформаційного безпекового простору. Ще у 2019 році на Саміті G20 в м. Осака (Японія) світові лідери, аналізуючи питання цифровізації сучасного суспільства, визначили пріоритетним розвиток суспільства 5.0., орієнтованого на людину та вирішення проблем, пов’язаних з інформаційною безпекою. Так, вимірами безпеки в цифровому суспільстві є: базові цифрові навички, інформаційна компетентність, комунікація з допомогою цифрових технологій (з метою інтеграції в діджитал-простір; вираження своєї громадянської позиції), оцінка та інтерпретація даних, інформації та цифрового контенту, взаємодія на рівні «громадянин-громадянин», «громадянин-держава», захист особистих прав як мережевого споживача тощо.

Висновки. Безпека як соціальне, політичне, економічне, культурне явище є ключовою категорією епохи цифрового суспільства, оскільки гарантії безпечного простору забезпечують впевненість у завтрашньому дні та стимулюють розвиток.

З початку російсько-українського протистояння у 2014 році потреба у посиленні захисту українського кіберпростору зросла в рази, що спричинило актуалізацію питання врегулювання нормативно-правової бази задля сталого розвитку безпекового простору в сфері інформаційних технологій. Держава, зважаючи на виклики породжені російсько-українською війною, має також стимулювати розвиток ІТ-сфери, зокрема в системі безпеки.

Українська нормативно-правова база визначає наступні пріоритетні напрями забезпечення інформаційної безпеки: розвиток безпечного та надійного кіберпростору; захист державних електронних інформаційних ресурсів та інформаційної інфраструктури; захист критичної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері кібербезпеки; боротьбу з кіберзлочинністю тощо. Не менш важливим стало стимулювання функціонування недержавних проектів протидії російській інформаційній агресії проти України, які об'єднали аналітиків, блогерів та громадян країни.

Бібліографічний список:

1. Вдовенко О., Воробйов Є., Опришко Л. Аналітичний звіт «Війна у цифровому вимірі і права людини». Київ, 2022. 68 с.
2. Доповідь щодо ситуації з правами людини в Україні. 1 серпня 2020 – 31 січня 2021. URL : https://www.ohchr.org/Documents/Countries/UA/31stReportUkraine-ukr.pdf (дата звернення: 16.03.2024).
3. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник. Київ : ВІКНУ, 2016. 286 с.
4. Маркітантов В.Ю., Рибщун О.В., Віннічук О.В. Російська гібридна війна: від доктрини до тактики : навчальний посібник. Вид. 2-ге, перероб. і доп. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 248 с. URL : http://elar.kpnu.edu.ua:8081/xmlui/bitstream/handle/123456789/7393/Rosiiska-hibrydna-viina-vid-doktryny-do-taktyky.pdf?sequence=1&isAllowed=y (дата звернення: 21.03.2024).
5. Медіаспоживання українців в умовах повномасштабної війни. Опитування ОПОРИ. ОПОРА. 01.06.2022. URL : https://www.oporaua.org/report/polit_ad/24068-mediaspozhivannia-ukrayintsiv-v-umovakh-povnomasshtabnoyi-viini-opituvannia-opori (дата звернення: 21.03.2024).
6. Мельник В. Безпека особи, як категорія політичної науки та суспільно-політичне явище. Політична наука в Україні: стан і перспективи : матеріали всеукраїнської наукової конференції. Львів : ЦПД, 2008. С. 69-73.
7. Новородовський В. Інформаційна безпека України в умовах російської агресії. *Соціум. Документ. Комунікація. Серія «Історичні науки».* 2020. № 9. С. 150-179. URL : https://sdc-journal.com/index.php/journal/article/view/285/228 (дата звернення: 16.03.2024).
8. Про концепцію національної програми інформатизації : Закон України від 01.01.2022 р. № 75/98-ВР. URL : https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (дата звернення: 16.03.2024).
9. Про національну безпеку України : Закон України від 15.06.2022 р. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text(дата звернення: 16.03.2024).
10. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 20.01.2007 р. № 537-V. URL : https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 15.03.2024)
11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України №447/2021. URL : https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 18.03.2024).
12. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України № 685/2021. URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 18.03.2024).
13. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 13.03.2024).
14. Про цифровий порядок денний України : Проект Закон України. URL : https://www.rada.gov.ua/uploads/documents/40009.pdf (дата звернення: 15.03.2024).
15. Феномен безпеки: соціально-гуманітарні виміри / за заг. наук. редакцією В. Мудракова. Хмельницький : ФОП Мельник А.А., 2022. 332 с.
16. Цифрова адженда України – 2020 : проект. URL : https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf (дата звернення: 20.03.2024).
17. Beck U. Risikogesellschaft. Auf dem Weg in eine andere Moderne. URL https://webarchiv-ulrich-beck.soziologie.uni-muenchen.de/wp-content/uploads/2017/10/Risikogesellschaft-Auf-dem-Weg-in-eine-andere-Moderne.pdf

References:

1. Vdovenko O., Vorobyov YE., Opryshko L. (2022). Analitychnyy zvit «Viyna u tsyfrovomu vymiri i prava lyudyny» (Analytical report «War in the digital dimension and human rights»). Kyiv, 68 p.
2. Dopovid′ shchodo sytuatsiyi z pravamy lyudyny v Ukrayini. 1 serpnya 2020 – 31 sichnya 2021 (Report on the human rights situation in Ukraine. August 1, 2020 – January 31, 2021). URL : https://www.ohchr.org/Documents/Countries/UA/31stReportUkraine-ukr.pdf (Access date: 16.03.2024).
3. Kurban O.V. (2016). Suchasni informatsiyni viyny v merezhevomu on-layn prostori : navchal′nyy posibnyk (Modern information wars in the network and online space: a study guide). Kyyiv : VIKNU, 286 p.
4. Markitantov V.YU., Rybshchun O.V., Vinnichuk O.V. (2023). Rosiys′ka hibrydna viyna: vid doktryny do taktyky : navchal′nyy posibnyk (Russian hybrid warfare: from doctrine to tactics: a study guide). Vyd. 2-he, pererob. i dop. Kam″yanets′-Podil′s′kyy : Kam″yanets′-Podil′s′kyy natsional′nyy universytet imeni Ivana Ohiyenka, 248 p. URL : http://elar.kpnu.edu.ua:8081/xmlui/bitstream/handle/123456789/7393/Rosiiska-hibrydna-viina-vid-doktryny-do-taktyky.pdf?sequence=1&isAllowed=y (Access date: 21.03.2024).
5. Mediaspozhyvannya ukrayintsiv v umovakh povnomasshtabnoyi viyny. Opytuvannya OPORI (Media consumption of Ukrainians in conditions of full-scale war. OPORA survey). OPORA. 01.06.2022. URL : https://www.oporaua.org/report/polit_ad/24068-mediaspozhivannia-ukrayintsiv-v-umovakh-povnomasshtabnoyi-viini-opituvannia-opori (Access date: 21.03.2024).
6. Mel′nyk V . (2008). Bezpeka osoby, yak katehoriya politychnoyi nauky ta suspil′no-politychne yavyshche (Personal security as a category of political science and a socio-political phenomenon). Politychna nauka v Ukrayini: stan i perspektyvy : materialy vseukrayins′koyi naukovoyi konferentsiyi (Political science in Ukraine: state and prospects: materials of the All-Ukrainian scientific conference). L′viv : TSPD, P. 69-73.
7. Novorodovs′kyy V . (2020). Informatsiyna bezpeka Ukrayiny v umovakh rosiys′koyi ahresiyi (Information security of Ukraine in the conditions of Russian aggression). Sotsium. Dokument. Komunikatsiya (Society. Document. Communication). Seriya «Istorychni nauky». № 9. P. 150-179. URL : https://sdc-journal.com/index.php/journal/article/view/285/228 (Access date: 16.03.2024).
8. Pro kontseptsiyu natsional′noyi prohramy informatyzatsiyi (About the concept of the national informatization program) : Zakon Ukrayiny vid 01.01.2022 r. № 75/98-VR. URL : https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (Access date: 16.03.2024).
9. Pro natsional′nu bezpeku Ukrayiny (About the national security of Ukraine) : Zakon Ukrayiny vid 15.06.2022 r. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text (Access date: 16.03.2024).
10. Pro osnovni zasady rozvytku informatsiynoho suspil′stva v Ukrayini na 2007-2015 roky (About the main principles of information society development in Ukraine for 2007-2015) : Zakon Ukrayiny vid 20.01.2007 r. № 537-V. URL : https://zakon.rada.gov.ua/laws/show/537-16#Text (Access date: 15.03.2024).
11. Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku «Pro Stratehiyu kiberbezpeky Ukrayiny» (About the decision of the National Security and Defense Council of Ukraine On the decision of the National Security and Defense Council of Ukraine «On the Cybersecurity Strategy of Ukraine») : Ukaz Prezydenta Ukrayiny №447/2021. URL : https://www.president.gov.ua/documents/4472021-40013 (Access date: 18.03.2024).
12. Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 15 zhovtnya 2021 roku «Pro Stratehiyu informatsiynoyi bezpeky» (About the decision of the National Security and Defense Council of Ukraine «About Information Security Strategy») : Ukaz Prezydenta Ukrayiny № 685/2021. URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text (Access date: 18.03.2024).
13. Pro skhvalennya Kontseptsiyi rozvytku tsyfrovoyi ekonomiky ta suspil′stva Ukrayiny na 2018-2020 roky ta zatverdzhennya planu zakhodiv shchodo yiyi realizatsiyi (About the approval of the Concept of Development of the Digital Economy and Society of Ukraine for 2018-2020 and the approval of the plan of measures f or its implementation) : Rozporyadzhennya Kabinetu Ministriv Ukrayiny vid 17 sichnya 2018 r. № 67-r. URL : https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (Access date: 13.03.2024).
14. Pro tsyfrovyy poryadok dennyy Ukrayiny (About the digital agenda of Ukraine) : Proekt Zakon Ukrayiny. URL : https://www.rada.gov.ua/uploads/documents/40009.pdf (Access date: 15.03.2024).
15. Fenomen bezpeky: sotsial′no-humanitarni vymiry (The phenomenon of security: social and humanitarian dimensions); za zah. nauk. redaktsiyeyu V. Mudrakova (2022). Khmel′nyts′kyy : FOP Mel′nyk A.A., 2022. 332 p.
16. Tsyfrova adzhenda Ukrayiny – 2020 (Digital agenda of Ukraine – 2020) : proekt. URL : https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf (Access date: 20.03.2024).
17. Beck U. Risikogesellschaft. Auf dem Weg in eine andere Moderne. URL: https://webarchiv-ulrich-beck.soziologie.uni-muenchen.de/wp-content/uploads/2017/10/Risikogesellschaft-Auf-dem-Weg-in-eine-andere-Moderne.pdf

Vinnichuk O., Markitantov V. Security dimensions in the digital age

The article analyzes the essence of security as a social, cultural, economic and political phenomenon. The author emphasizes that the issue of security, safe environment, and security policy in all spheres of society are urgent today. The problem of interdependence of the security space for modern society and

the observance of human rights are revealed. The analytical data of the report of the UN Human Rights Monitoring Mission, the Office of the UN High Commissioner for Human Rights, and the research of well-known researchers and practitioners in the field of security policy are taken into account. It is proved that in the context of the development of a modern "networked" society, a new generation of information technologies – hi-tech (high-tech) and hi-sensor (high sensor-technology) technologies – play a significant role. These technologies are creating a new model of security relations at the level of citizen-citizen, citizen-state, state-state, etc. It is emphasized that in modern society, the latest information technologies contribute to the development of democracy and at the same time act as a tool for its destabilization. For instance, in the context of information warfare, all measures in the information space (fakes, propaganda, manipulations) are aimed at critically thinking members of society. The author proves, using the example of the russian-Ukrainian war, that the information space remains dominant in confronting the aggressor, in addition to the military one. This fact demonstrates the power of the new format of public administration in the fight for a safe environment. An important aspect of security policy during the Russian-Ukrainian war was the activity of online volunteer movements. As a result, the importance of strengthening the protection of Ukrainian cyberspace, which has emerged since 2014, is substantiated. The author identifies the priority areas of ensuring information security of Ukraine.

Keywords: *security, information society, information security, hi-tech, hi-sensor, hybrid warfare*