УДК [1:[351:004.056]]:355.48(470+571:477)
DOI: https://doi.org/10.21564/2663-5704.65.331715

Прудникова Олена Вікторівна, доктор філософських наук, професор, професор кафедри культурології, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
e-mail: elenvikprud@ukr.net
ORCID ID: 0000-0003-4610-908X

ІНФОРМАЦІЙНА БЕЗПЕКА ВІТЧИЗНЯНОГО СУСПІЛЬСТВА В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

У статті досліджується інформаційна безпека українського суспільства в інформаційно-технічному та ціннісно-світоглядному контекстах під час російської агресії. Стверджується, що розвиток системи інформаційної безпеки України в умовах російсько-української війни має спиратись на новітні інформаційно-комунікаційні технології, вітчизняний програмний продукт, висококваліфікованих фахівців у цій царині. Констатується, що в світоглядному сенсі з початком російсько-української війни набули трансформацій змістовні характеристики антиукраїнських наративів, що використовуються як «смислова» та «інформаційна» зброя.

Ключові слова: *інформаційна безпека, російсько-українська війна, інформаційна зброя, медіаграмотність, інформаційна війна, наративи.*

Постановка проблеми. Інформаційна безпека є важливим складником загальної системи національної безпеки в реаліях сьогодення, коли інформаційно-комунікаційні технології, штучний інтелект та віртуальна реальність стали визначальними чинниками суспільного буття. Проблематика інформаційної безпеки набуває нового звучання під час війн, суспільних криз, соціальних протистоянь. Зокрема, в Україні в умовах широкомасштабної російської агресії інформаційна безпека потребує особливої уваги з боку держави як у комунікаційно-технологічному контексті, так і в світоглядно-ціннісному значенні. Забезпечення належного рівня інформаційної безпеки Української держави, вітчизняного суспільства та окремих громадян є невідкладним завданням, від вирішення якого залежить збереження державного суверенітету нашої країни, її національного культурного простору, споконвічних ціннісних орієнтирів українства.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки України під час російської агресії аналізуються вченими з різних галу-

зей знань. Зупинімось на наукових роботах, які стали підґрунтям для нашої статті.

Концептуальні ідеї щодо розуміння сутності інформаційної безпеки в умовах розвитку інформаційного суспільства знайшли відображення в науковому доробку А. Гетьмана, О. Данильяна, О. Дзьобаня, Ю. Калиновського [1]. Натомість у науковій праці Л. Мазуренко аналізується структура інформаційної безпеки та виокремлюються її складники [2]. Конкретизації інформаційно-технічного складника інформаційної безпеки України під час російської агресії присвячено роботи І. Залєвської та Г. Удренас [3] і Д. Смотрича та Л. Браілко [4].

Окрема група наукових праць репрезентує дослідження законодавчої бази функціонування системи інформаційної безпеки українського суспільства в довоєнні та воєнні часи: роботи К. Владімірової та В. Стрелкова [5] й наукова розвідка В. Новородовського [6]. Інформаційно-психологічні та світоглядно-ціннісні складники інформаційної безпеки вітчизняного соціуму в умовах інформаційного та військового протистояння з РФ подано в наукових розвідках Д. Гончаренко [7], О. Курбана [8], Ю. Калиновського та С. Жданенко [9], Ю. Горбаня [10], О. Косогова [11], Є. Архипової [12] та ін.

Формулювання мети. Статтю присвячено особливостям буття інформаційної безпеки вітчизняного соціуму під час російської агресії.

Виклад основного матеріалу. У наш час науковці констатують, що інформаційна безпека – це одна з актуальних соціокультурних проблем сучасного суспільства, яка має системний характер і торкається діяльності основних інститутів і підсистем. Зокрема, у поле її впливу потрапляють ключові соціокультурні процеси, що відбуваються в суспільстві, системні зміни в політичній, правовій та духовній сферах. Ключовим фактором ризику для інформаційної підсистеми соціуму виступають масштабні соціокомунікативні та соціокультурні трансформації, що несуть у собі низку негативних соціальних наслідків. В останні роки чітко фіксуються дезорганізаційно-дисфункційні тенденції, безпосередньо пов’язані з високими швидкостями інформаційних змін [1, p. 12].

Відповідно, під час війни ризики для всієї системи інформаційної безпеки значно зростають, оскільки суттєво збільшуються спроби деструктивних впливів на всі її складники та інститути. Необхідно підкреслити, що до початку широкомасштабного вторгнення РФ в Україну проти нашої країни була розв’язана безпрецедентна інформаційна війна, яка лише посилилася з 24 лютого 2022 р.

Для всебічного аналізу феномену інформаційної безпеки зупинімося на її сутнісних характеристиках. На думку Л. Мазуренко, можна виокремити такі складники інформаційної безпеки:

– інформаційно-технічний: створення системи надійного захисту – від несанкціонованого втручання, хакерських атак до інформаційно-комп'ютерних систем та окремих сайтів; блокування комп'ютерних вірусів та радіоелектронних атак, недопущення незаконного використання телерадіомовних частот тощо;

– інформаційно-психологічний захист соціуму та країни від деструктивних інформаційних впливів. Ця проблема особливо «гостро відчувається у воєнний час, бо тоді емоції заважають критично оцінювати та аналізувати ситуацію і ту інформацію, що поширюється в соціальних мережах. Інформація під час воєнних конфліктів стає ще одним видом зброї ворога, враховуючи інформаційно-психологічний аспект інформаційної безпеки» [2, с. 53].

Конкретизуючи загрози інформаційно-технічному складнику інформаційної безпеки, І. Залєвська та Г. Удренас доводять, що на сьогодні одним із найважливіших об'єктів безпеки в оборонній сфері є інформаційні ресурси та інформаційна структура оборонного потенціалу країни (Збройних Сил та військово-промислового комплексу). Автори підкреслюють, що це найсучасніші засоби озброєння, військової техніки, систем управління зброєю та військами, які оснащені системами критичних додатків із високим рівнем комп'ютеризації. Такі системи можуть бути особливо вразливими для інформаційної зброї ворога як у мирний, такі особливо у воєнний час. «Останнє може призвести до того, що до загрозливого періоду зброя стримування країни виявиться повністю або частково заблокованою за рахунок прихованого впровадження ворогом у програмне забезпечення систем управління програмних закладок. Про реальність такої ситуації свідчить досвід локальних воєн останніх років» [3, с. 24].

У продовження вищеозначеного Д. Смотрич та Л. Браілко переконливо стверджують, що «технічні загрози інформаційного характеру стосуються як функціонування інформаційних систем, що використовуються у військах, у тому числі систем управління, так і збереження конфіденційної інформації, що передається військовими каналами зв'язку. Види технічних загроз діяльності Збройних Сил можуть бути різного характеру: від умисного пошкодження систем і крадіжки інформації до недбалості окремих співробітників. Заходи захисту в цьому випадку передбачатимуть підвищення рівня безпеки автоматизованих систем управління та навчання персоналу необхідним вимогам захисту інформації» [4, с. 123].

Отже, забезпечення інформаційної безпеки України під час війни потребує захисту та подальшого розвитку інформаційно-комунікаційних систем держави, створення новітнього вітчизняного програмного продукту, підготовку висококваліфікованих фахівців, здатних обслуговувати складні технологічні комплекси управління оборонним сектором країни тощо.

Аналізуючи вищеозначені проблеми щодо зміцнення інформаційної безпеки нашої держави в умовах російсько-української війни, К. Владімірова та В. Стрелков зауважують, що український уряд прийняв декілька законодавчих актів необхідних для зміцнення кібербезпеки та спрямованих на подолання інформаційних загроз. Так, було прийнято національні стратегії з кібербезпеки та інформаційної безпеки, у яких означено пріоритетні напрями діяльності щодо захисту інформаційного простору України. Відповідно, це сприяє створенню структурованої системи протидії інформаційним атакам. Зокрема, «реалізація технічних заходів включає впровадження сучасних систем кіберзахисту та моніторингу, що дозволяють виявляти і нейтралізувати загрози на ранніх етапах. Українські державні органи та великі приватні компанії поступово переходять на використання більш захищених програмних продуктів і протоколів зв'язку, що значно підвищує рівень кібербезпеки. Також створено спеціальні кіберпідрозділи в структурах Міністерства оборони та Служби безпеки України, які займаються виключно питаннями кіберзахисту» [5, с. 9].

Необхідно зауважити, що посилення законодавчої бази України щодо захисту підвалин національної безпеки та інформаційної зокрема активізувалось починаючи з 2014 р. В умовах розгортання російсько-української війни було прийнято низку нормативно-правових актів, спрямованих на захист інформаційного простору та протидію ворожій пропаганді, спрямованої проти нашої держави. Загалом базовими законодавчими актами, які регулюють сферу інформаційної безпеки, є Конституція України, Закон України «Про ратифікацію Конвенції про кіберзлочинність», Закон України «Про національну безпеку», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки тощо. Важливе значення мав Указ Президента України № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», який зобов'язував українських провайдерів блокувати російські інформаційні ресурси – соціальні мережі, сайти («вконтактє», «однокласники», «mail.ru», «яндекс», «Лабораторія Касперського», «Dr. Web») та офіційного дистриб'ютора «1С» на території України терміном

на три роки [6, с. 163]. Такі кроки мали позитивний вплив щодо захисту інфопростору України, сприяли зміцненню інформаційної безпеки держави, утруднювали можливості ворога здійснювати інформаційно-психологічні операції у вітчизняному соціумі.

Продовжуючи аналіз інформаційної безпеки українського суспільства під час російської агресії, зупинімось на її сутнісних аспектах смислового характеру. В інформаційно-психологічному та когнітивному сенсі з початком широкомасштабного російського вторгнення набули певних трансформацій змістовні характеристики агресивних, антиукраїнських наративів, що використовуються проти України в якості «смислової» та «інформаційної» зброї.

Д. Гончаренко констатує, що лютий 2022 р. характеризується посиленням російських інформаційно-психологічних атак проти Української держави та західних країн. Наративи ворожих інформаційно-психологічних операцій маніпулятивного спрямування суттєво змінились. Так, до повномасштабної агресії РФ проти України головним пріоритетом інформаційних кампаній був історичний ревізіонізм. Із початком російсько-української війни абсурдний характер російської дезінформації набув нового смислового забарвлення. «Серед прикладів є «нацистський уряд в Україні», «сіоністські теорії змови», «українські біологічні лабораторії з тренування бойових комах» тощо. Російська дезінформація використовується для підриву діяльності суперників, заплутування та відволікання від важливіших, але менш приємних новин» [7, с. 388].

З точки зору О. Курбана, у сфері інформаційних війн наративи, які мають деструктивний характер, варто класифікувати як «бойові наративи». Їх природа має агресивний та атакувальний характер. Вищеозначений науковець визначає існування як ситуативних наративів, так і супернаративів, які застосовуються у значних часових межах та становлять дезінформаційну смислову базу інформаційно-гібридної, а починаючи з лютого 2022 року – широкомасштабної війни Росії проти України. Одним з основних «довготривалих наративів аналітична група «АМ & РМ» визначила ностальгію за СРСР. (Вперед у світле минуле). Цей наратив з'явився на початку 2000-х рр. як засіб ідеологічного обґрунтування претензій рф на спадок СРСР та спроби відтворити цю державу у форматі Єдиного економічного простору або Митного союзу. За визначенням експертів «АМ & РМ», основними субнаративами цього супернаративу стали такі: росія − це як СРСР, тільки краще; США та НАТО – це зло, проти якого бореться росія; росія перемогла нацизм і фашизм; росія, білорусь та Україна − братські країни; у росії гідне й заможне життя; культ особистості; захід загниває під вагою аморальності та безкультур'я» [8, с. 151].

Для обґрунтування широкомасштабного вторгнення напередодні та вже під час російсько-української війни, РФ системно розповсюджувала у інформаційних ресурсах України та інших країн наративи, що ставлять під сумнів українську державність, європейський вибір України, підвалини української національно-культурної окремішності та ін. Для прикладу такими «бойовими наративами» є: «Україна недодержава; росіяни й українці – це один народ»; «Україна під впливом Заходу обрала неправильний цивілізаційний вектор розвитку»; «росіяни, українці та білоруси становлять єдиний національно-культурний організм тощо». Для обгрунтування вищенаведених наративів РФ використовувала всі наявні інформаційно-аналітичні ресурси, застосовувала технології перекручування історичних подій, «знецінення» національних героїв України, штучно загострювала дискусії щодо ролі російської мови у суспільному житті нашої держави, задіювала інститут церкви для антиукраїнської пропаганди тощо» [9, с. 31].

Відповідно під час російсько-української війни ворог практикує використання як попередніх «довоєнних» наративів, так і створює нові (як підкреслювалось вище), в залежності від політичних, військових, геополітичних реалій, що склались у певний період часу. Для нівелювання цих загроз інформаційній безпеці, Українська держава має розробити та втілювати системні заходи протидії, оскільки прогалини на інформаційному фронті суттєво впливають на здатність нашої країни чинити ефективний опір російській агресії.

Загалом, якщо порівнювати методи інформаційно-психологічних операцій, що здійснювались у довоєнні часи, з тими технологіями, які використовуються зараз, то цілком можна погодитись з думкою Ю. Горбаня, який досліджуючи «інформаційну війну Росії проти України розглядав п’ять основних методів її ведення: 1) дезінформація та маніпуляція; 2) пропаганда; 3) диверсифікація громадської думки; 4) психологічний тиск; 5) поширення чуток» [10, с. 138].

На переконання фахівців у сфері інформаційної безпеки, можна виокремити такі загрози для України у цій царині:

− послідовне формування недружніми іноземними державами негативного міжнародного іміджу України;

− посилення критики вищого політичного керівництва України;

− потужний інформаційний тиск з боку низки зарубіжних країн на Українську державу з метою підштовхування політичного керівництва до прийняття вигідних для цих держав рішень у внутрішньо та зовнішньополітичній сферах нашої країни;

– «посилення інформаційних заходів із перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проєктах, які в сучасних умовах не вигідні нашій державі;

– дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;

– зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї» [11, с. 128].

На індивідуальному рівні, під час російсько-української війни значно збільшився інформаційний та психологічний тиск на людину, що негативно впливає на характеристики особистої інформаційної безпеки. У такій ситуації людиною простіше маніпулювати, спрямовувати її думки та дії у відповідне русло.

Коментуючи психологічний та когнітивний стан людини як підґрунтя інформаційної безпеки в період значних соціальних потрясінь, Є. Архипова стверджує, що суттєве збільшення інформаційного навантаження, кардинальна трансформація соціокультурних умов, руйнування усталеної системи ціннісних та ідеологічних орієнтирів є причиною дезадаптації та дезорієнтації людини, виникнення проблем в оцінюванні соціальної дійсності. «В той же час сучасний світ вимагає постійного включення, інтелектуальної активності людини, адже кожний новий день може принести важливу інформацію та змінити "правила гри", а нетривале випадення з інформаційного потоку може призвести до серйозної і тривалої втрати позицій. Із збільшенням кількості інформаційних каналів розширюються можливості маніпулювання суспільною та індивідуальною свідомістю, розвиваються техніки та методи управління громадською думкою» [12, с. 11].

Російсько-українська війна показала, що людина, її емоційний стан та ментальне здоров'я у такій складній ситуації напряму залежать від якості, актуальності та систематичності інформаційних повідомлень. При цьому людина в період воєнного стану об'єктивно стає інфозалежною, чекаючи позитивних новин та важливих для її особистого простору повідомлень. На жаль, такою ситуацією психологічної розбалансованості особистості користується ворог, «вкидуючи» в інформаційний простір неправдиві, маніпулятивні повідомлення.

Можна погодитися з П. Квіткіним, І. Дятловою, Л. Петровою, які підкреслюють, що в системі чинників, які впливають на інформаційну безпеку людини, основне місце посідають пропагандистсько-інформаційні та психологічно-інформаційні впливи. Вони спрямовані на розповсюдження дезінформації та здійснення негативного впливу на суспільну та індивідуальну свідомість,

що спричинює викривлене сприйняття соціальних подій. З точки зору даних науковців, найбільш значними інформаційними загрозами для інформаційної безпеки держави, суспільства та особистості є: «…такий інформаційний вплив (внутрішній або зовнішній), при якому створюється потенційна або актуальна (реальна) небезпека зміни напряму або темпів прогресивного розвитку держави, суспільства, індивідів; небезпека заподіяння шкоди життєво важливим інтересам особистості, суспільства, держави шляхом інформаційного впливу на свідомість, інформаційні ресурси й інфосферу комп'ютерно-технічних систем; сукупність чинників, що перешкоджають розвитку і використанню інформаційного середовища в інтересах особистості, суспільства і держави» [13, с. 52–53].

Для подолання негативних чинників впливу на інформаційну безпеку вітчизняного соціуму в умовах війни варто здійснювати комплекс заходів, одним із напрямів реалізації яких є підвищення якісного стану медіаграмотності населення.

На переконання Ю. Ніколаєць, такими векторами покращення медіаграмотності вітчизняних громадян є: формування негативного ставлення до інформації анонімного характеру та критичне ставлення до інформаційних оцінних повідомлень без обґрунтованих належним чином висновків; недопущення коментування чуток та неперевірених даних з метою здійснення висновків на їх підставі; недопустимість поширення меседжів з закритих джерел або джерел, походження яких приховується автором повідомлення; недоцільність використання джерел, походження яких не має можливості підтвердити за відповідними посиланнями. Також «ставлення з пересторогою має бути сформоване до раптової появи нових джерел контенту, які поширюють інсайдерську інформацію; до джерел, які подають інформацію незбалансовано, а також до інформації експертів, походження знань, умінь і навичок яких неможливо встановити або прогнози яких переважно не справджуються. Важливо переконати громадян у тому, що джерелом аналітики мають бути передусім визнані експерти-науковці» [14, с. 58].

Украй важливо, щоб, незважаючи на війну, постійно зростав інтелектуальний потенціал суспільства та інформаційна грамотність конкретного громадянина на основі сучасних знань і достовірної інформації.

Як стверджує Ю. Калиновський, «в умовах зростання рівня глобальної турбулентності й конфліктності, знання виконують функцію інтелектуального бар'єру, який захищає духовний простір країни від деградації. Суттєвою загрозою для інформаційної та духовно-ціннісної безпеки держави є поширення псевдонаукових даних та фейкового інформаційного контенту. Людина у XXI сторіччі незалежно від рівня освіти та характеру професійної діяль-

ності має постійно працювати над набуттям компетентностей з медіаграмотності та медіагігієни задля убезпечення власного духовного світу й ментального здоров'я від агресивних інформаційних впливів» [15, с. 37].

Висновки. Інформаційна безпека українського суспільства в умовах російсько-української війни є однією з ключових ланок різнорівневого захисту державного суверенітету. Для зміцнення її підвалин вітчизняна законодавча база в цій царині має постійно актуалізуватись, оперативно реагуючи на швидкоплинні зміни в умовах воєнного стану. При цьому заходи з інформаційної безпеки мають узгоджуватися з правом людини на достовірну та всебічну інформацію – неприпустимими є прояви невмотивованої цензури.

Досліджуючи зміни в інфопросторі України під час російської агресії, варто враховувати показники інформаційно-психологічного перевантаження як на рівні соціуму, так і на індивідуальному рівні. Також, плануючи систему заходів щодо зміцнення інформаційної безпеки нашої держави, необхідно ретельно аналізувати зміни в характері та змістовному наповненні інформаційно-психологічних операцій ворога, спрямованих проти України.

ЛІТЕРАТУРА

1. Getman A., Danilyan O., Dzeban A., Kalinovsky Y., Hetman Y. Information security in modern society: sociocultural aspects. *Amazonia Investiga.* 2020. Vol. 9, №25. P. 6–14.
2. 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. Вип. 42. С. 50–57.
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. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 77, ч. 2. С. 121–127.
5. Владімірова К. П., Стрелков В. В. Інформаційна безпека України в умовах повномасштабного вторгнення. *Acta securitatae volynienses*. 2024. №4. С. 5–10.
6. Новородовський В. Інформаційна безпека України в умовах російської агресії. *Соціум. Документ. Комунікація*. 2020. Вип. 9. С. 150–179.
7. Гончаренко Д. Ю. Стратегічні підходи до забезпечення інформаційної безпеки в умовах інформаційної війни України з РФ. *Політологічний вісник*. 2024. №92. С. 383–397.
8. Курбан О. В. Бойові наративи в системі сучасних геополітичних інформаційних війн (досвід російсько-української гібридної інформаційної війни 2014–2021 рр.). *Синопсис: текст, контекст, медіа*. 2021. №27 (3). С. 149–158.

9. Калиновський Ю. Ю., Жданенко С. Б. Роль цивілізаційно-ціннісних наративів у глобальному інформаційному протиборстві. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2023. №3 (58). С. 23–38.
10. Горбань Ю. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України.* 2015. Вип. 1. С. 136–141.
11. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. *Збірник наукових праць Харківського університету Повітряних Сил*. 2014. Вип. 3. С. 127–130.
12. Архипова Є. О. Соціально-філософське осмислення поняття «інформаційна безпека». *Вісник НТУУ «КПІ». Філософія. Психологія. Педагогіка*. 2011. Вип. 3. С. 7–11.
13. Квіткін П., Дятлова І., Петрова Л. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник НЮУ імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія*. 2021. №4 (51). С. 46–62.
14. Ніколаєць Ю. Державна інформаційна політика України в умовах повномасштабного воєнного вторгнення Російської Федерації: суспільно-мобілізаційний потенціал і ефективність. *Політичні дослідження*. 2024. №1 (7). С. 42–67.
15. Калиновський Ю. Ю., Жданенко С. Б. Трансформація ролі знань у соціокультурних процесах сучасності: аксіологічний та безпековий контексти. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія.* 2024. №1 (60). С. 23–42.

REFERENCES

1. Getman, A., Danilyan, O., Dzeban, A., Kalinovsky, Y., Hetman, Y. (2020). Information security in modern society: sociocultural aspects. *Amazonia Investiga, Vol. 9, 25, 6–14.*
2. Mazurenko, L. I. (2022). Informatsiina bezpeka v umovakh rosiisko-ukrainskoi viiny: vyklyky ta zahrozy. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina, seriia «Pytannia politolohii" – Bulletin of V. N. Karazin Kharkiv National University. Series: «Problems of Political Science"*, *issue 42, 50–57* [in Ukrainian].
3. Zalievska, I. I., Udrenas, H. I. (2022). Informatsiina bezpeka Ukrainy v umovakh rosiiskoi viiskovoi ahresii. *Pivdennoukrainskyi pravnychyi chasopys – Southern Ukrainian Law Journal, 1–2, 20–26* [in Ukrainian].
4. Smotrych, D., Brailko, L. (2023). Informatsiina bezpeka v umovakh voiennoho stanu. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu,* Seriia Pravo – *Scientific Scientific Bulletin of Uzhhorod National University. Series: Law, issue 77 (2), 121–127* [in Ukrainian].
5. Vladimirova, K. P., Strelkov, V. V. (2024). Informatsiina bezpeka Ukrainy v umovakh povnomasshtabnoho vtorhnennia. *Acta securitatae volynienses, 4, 5–10* [in Ukrainian].

6. Novorodovskyi, V. (2020). Informatsiina bezpeka Ukrainy v umovakh rosiiskoi ahresii. *Sotsium. Dokument. Komunikatsiia – Society. Document. Communication, issue 9, 150–179* [in Ukrainian].
7. Honcharenko, D. Yu. (2024). Stratehichni pidkhody do zabezpechennia informatsiinoi bezpeky v umovakh informatsiinoi viiny Ukrainy z RF. *Politolohichnyi visnyk – Political Science Bulletin, 92, 383–397* [in Ukrainian].
8. Kurban, O. V. (2021). Boiovi naratyvy v systemi suchasnykh heopolitychnykh informatsiinykh viin (dosvid rosiisko-ukrainskoi hibrydnoi informatsiinoi viiny 2014–2021 rr.). *Synopsys: tekst, kontekst, media – Synopsis: text, context, media, 27(3), 149–158* [in Ukrainian].
9. Kalynovskyi, Yu.Yu., Zhdanenko, S. B. (2023). Rol tsyvilizatsiino-tsinnisnykh naratyviv u hlobalnomu informatsiinomu protyborstvi. *Visnyk Natsionalnoho yurydychnoho universytetu imeni Yaroslava Mudroho. Seriia: filosofiia, filosofiia prava, politolohiia, sotsiolohiia – The Bulletin of Yaroslav Mudryi National Law University. Series:Philosophy, philosophy of law, political science, sociology, 3(58), 23–38* [in Ukrainian].
10. Horban, Yu. (2015). Informatsiina viina proty Ukrainy ta zasoby yii vedennia. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy – Bulletin of the National Academy of Public Administration under the President of Ukraine, Issue 1, 136–141* [in Ukrainian].
11. Kosohov, O. M. (2014). Priorytetni napriamky derzhavnoi polityky shchodo zabezpechennia bezpeky natsionalnoho kiberprostoru. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl – Collected Scientific Works of the Kharkiv Air Force University, Issue 3, 127–130* [in Ukrainian].
12. Arkhypova, Ye.O. (2011). Sotsialno-filosofske osmyslennia poniattia «informatsiina bezpeka». *Visnyk NTUU «KPI». Filosofiia. Psykholohiia. Pedahohika – Bulletin of NTUU «KPI». Philosophy. Psychology. Pedagogy, Issue 3, 7–11* [in Ukrainian].
13. .Kvitkin, P., Diatlova, I., Petrova, L. (2021). Informatsiina bezpeka osobystosti: teoretyko-metodolohichnyi analiz. *Visnyk NIuU imeni Yaroslava Mudroho. Seriia: Filosofiia, filosofiia prava, politolohiia, sotsiolohiia – The Bulletin of Yaroslav Mudryi National Law University. Series:Philosophy, philosophy of law, political science, sociology, 4(51), 46–62* [in Ukrainian].
14. Nikolaiets, Yu. (2024). Derzhavna informatsiina polityka Ukrainy v umovakh povnomasshtabnoho voiennoho vtorhnennia Rosiiskoi Federatsii: suspilno-mobilizatsiinyi potentsial i efektyvnist. *Politychni doslidzhennia – Political research, 1(7), 42–67* [in Ukrainian].
15. Kalynovskyi, Yu.Yu., Zhdanenko, S. B. (2024). Transformatsiia roli znan u sotsiokulturnykh protsesakh suchasnosti: aksiolohichnyi ta bezpekovyi konteksty. *Visnyk Natsionalnoho yurydychnoho universytetu imeni Yaroslava Mudroho. Seriia: filosofiia, filosofiia prava, politolohiia, sotsiolohiia – The Bulletin of Yaroslav Mudryi National Law University. Series:Philosophy, philosophy of law, political science, sociology, 1(60), 23–42* [in Ukrainian].

Prudnykova Olena Victorivna, Doctor of Philosophy, Professor, Professor of the Department of Culturology, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

INFORMATION SECURITY OF THE DOMESTIC SOCIETY IN THE CONTEXT OF THE RUSSIAN-UKRAINIAN WAR

The article explores the information security of Ukrainian society in the informational-technical and value-worldview contexts during the Russian aggression. It is argued that the development of Ukraine's information security system under the conditions of the Russian-Ukrainian war must rely on advanced information and communication technologies, domestic software products, and highly qualified specialists in this field. It is noted that, in the worldview dimension, the onset of the Russian-Ukrainian war has led to the transformation of the substantive characteristics of anti-Ukrainian narratives, which are used as «semantic» and «informational» weapons.

Keywords: *information security, Russian-Ukrainian war, informational weapons, media literacy, information warfare, narratives.*