УДК 342.6:342.922(477)

https://doi.org/10.52058/2786-6300-2025-6(36)-404-414

Бейкун Андрій Леонардович кандидат юридичних наук, доцент, доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки, Київський інститут Національної гвардії України, м. Київ, тел.: (098) 001-30-15, https://orcid.org/0000-0002-4895-1361

СУЧАСНЕ ПРАВОВЕ ПОЛЕ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СТРУКТУРІ ЗАБЕЗПЕЧУЮЧИХ ЕЛЕМЕНТІВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА У РАКУРСІ НЕОБХІДНОСТІ ПРОТИСТОЯННЯ ГІБРИДНИМ АСПЕКТАМ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ

Анотація. Вже протягом досить тривалого періоду термін «гібридна війна» став певним синонімом використання стороною збройного конфлікту нетрадиційних, асиметричних засобів ведення війни, що, як правило, передбачає певну стратегію «непрямих дій» щодо послаблення оборонного потенціалу іншої сторони збройного конфлікту, і здійснюється, як правило, шляхом того чи іншого ураження об’єктів, які, як правило, підпадають під захист норм міжнародного гуманітарного права. Фактично можна з значною долею вірогідності констатувати, що «гібридні» форми збройного протистояння є ключовою формою реалізації планів збройної агресії російської федерації проти України, а також варто погодитись зі ствердженнями, що означені форми ведення війни «стали тим підривним та безжальним монстром у руках росії, адже їх сила у тому, що вони поєднують у собі традиційні та нетрадиційні форми боротьби, військові та невійськові, насамперед, заборонені тактичні прийоми і методи реалізації намірів». Одним з проявів «гібридної війни» стала боротьба в інформаційному та кібернетичному просторі, ініційована та здійснювана російською федерацією ще задовго до прямої повномасштабної збройної агресії, до початку активної фази боротьби у лютому 2022 року. І у тому числі і цей фактор російсько-української війни став викликом не лише для України, а й для усієї демократичної міжнародної спільноти і наразі становить неабияку загрозу для чинного світового порядку, заснованому на певних узгоджених принципах співіснування.

Отже, констатація невід’ємності цифрових технологій нашого життя аксіомно іде поруч з констатацією, що питання кібербезпеки набувають критичного значення, насамперед, в умовах дії особливих правових режимів. Безумовно, захист інформаційних систем, персональних даних та національної

інфраструктури від кіберзагроз вимагає не лише технічних рішень, але й ефективного правового регулювання. Безумовно, що розвиток інформаційно-телекомунікаційних систем впливає як на форми взаємодії у суспільстві, так і на потенційні можливості супротивників завдавати ураження об'єктам критичної інфраструктури. Не є таємницею, що російсько-українська війна характерна і численними кібератаками, якими обмінюються наші спеціальні підрозділи з ворогом. Об'єктами таких атак є: і електронні засоби управління, і засоби регулювання технологічних процесів, і засоби масової інформації та телекомунікації тощо. За таких умов особливого значення набуває гарантування інформаційної та кібернетичної безпеки держави, суспільства і окремої особистості, у тому числі і шляхом удосконалення відповідної нормативно-правової бази.

Ключові слова: гуманітарні норми, інформаційні технології, система національної безпеки, кібербезпека, кібератаки, кібероперації, кіберзагрози, кіберпростір, кібершпигунство, гібридний конфлікт, об'єкти критичної інфраструктури, система життєзабезпечення.

Beikun Andrii Leonardovich PhD in Law, Associate Professor, Associate Professor of the Department of Legal Support and Law Enforcement Activities, Faculty of State Security, Kyiv Institute of the National Guard of Ukraine, Kyiv, tel.: (098) 001-30-15, https://orcid.org/0000-0002-4895-1361

THE MODERN LEGAL FIELD OF INFORMATION SECURITY IN THE STRUCTURE OF NATIONAL SECURITY ENSURING ELEMENTS AND IN THE PERSPECTIVE OF THE NEED TO OPPOSE HYBRID ASPECTS OF FULL-SCALE ARMED AGGRESSION

Abstract. For quite a long period, the term «hybrid war» has become a synonym for the use by a party to an armed conflict of unconventional, asymmetric means of warfare, which, as a rule, involves a certain strategy of «indirect actions» to weaken the defense potential of the other party to the armed conflict, and is carried out, as a rule, by one way or another, by damaging objects that, as a rule, fall under the protection of the norms of international humanitarian law. In fact, it is possible to state with a high degree of certainty that «hybrid» forms of armed confrontation are a key form of implementing the plans of the Russian Federation's armed aggression against Ukraine, and it is also worth agreeing with the statements that these forms of warfare «have become that subversive and ruthless monster in the hands of russia, because their strength lies in the fact that they combine traditional and non-traditional forms of struggle, military and non-military, and above all, prohibited tactical techniques and methods of implementing intentions». One of the manifestations of «hybrid warfare»

was the struggle in the information and cyberspace, initiated and carried out by the russian federation long before direct full-scale armed aggression, before the beginning of the active phase of the struggle in February 2022. And including this factor of the Russian-Ukrainian war, it has become a challenge not only for Ukraine, but also for the entire democratic international community and currently poses a significant threat to the current world order, based on certain agreed principles of coexistence.

Thus, the statement of the indispensability of digital technologies in our lives axiomatically goes hand in hand with the statement that cybersecurity issues acquire critical importance, primarily under the conditions of special legal regimes. Of course, protecting information systems, personal data, and national infrastructure from cyber threats requires not only technical solutions, but also effective legal regulation. It is certain that the development of information and telecommunications systems affects both the forms of interaction in society and the potential capabilities of adversaries to damage critical infrastructure facilities. It is certain that the development of information and telecommunications systems affects both the forms of interaction in society and the potential capabilities of adversaries to damage critical infrastructure facilities. It is no secret that the Russian-Ukrainian war is also characterized by numerous cyberattacks exchanged between our special units and the enemy. The objects of such attacks are: electronic control devices, means of regulating technological processes, mass media and telecommunications, etc. Under such conditions, ensuring the information and cyber security of the state, society, and the individual becomes of particular importance, including by improving the relevant regulatory framework.

Keywords: humanitarian norms, information technology, national security system, cybersecurity, cyber attacks, cyber operations, cyber threats, cyberspace, cyber espionage, hybrid conflict, critical infrastructure facilities, life support system.

Постановка проблеми. Отже, як зазначено у Законі України: «Про основні засади забезпечення кібербезпеки України», кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Відповідно, так звану «тріаду» інформаційної та кібернетичної безпеки можна представити наступним чином: безпека держави, безпека суспільства, безпека особи. При цьому безпека особи, суспільства та держави може забезпечуватися як на національному, регіональному, так і міжнародному рівні.

Комплексний аналіз сучасного правового поля у сфері кібербезпеки виявляє низку суттєвих проблем, які потребують вирішення. Першочергово, слід

відзначити асинхронність розвитку законодавчої бази та технологічного прогресу, що призводить до утворення прогалин у правовому регулюванні новітніх форм кіберзагроз. Відповідно, означені форми також генеруються завдяки вдосконаленню прийомів, способів і засобів збройної боротьби. Ця аксіома посилюється ще й транскордонним характером кіберпростору, який у значній мірі нівелює національні юрисдикційні межі та ускладнює застосування національного законодавства до злочинів, що мають міжнародний масштаб.

Крім того, варто звернути увагу і на термінологічний апарат, що використовується у галузевій нормативно-правовій базі і програмних документах з питань національної взагалі та інформаційної і кібербезпеки, окрема. Навіть базові понятійні категорії з питань безпеки інформаційного простору та телекомунікаційних систем у різних нормативах мають або різні (хоча і синонімічні) назви, або розмитий та надмірно розгалужений зміст. Відповідно, означена термінологічна база навряд чи спроможна виконати функцію каталізатора формування та подальшого розвитку спеціалізованої нормативної основи, орієнтованої на охорону окресленої сфери національної безпеки та оборони та набути відповідного етимологічного та правового наповнення.

Особливої уваги заслуговує дилема балансування між нормативним посиленням заходів кібербезпеки та збереженням фундаментальних прав на приватність і свободу інформації. Ця проблема набуває особливої гостроти як в контексті зростаючої ролі цифрових технологій у повсякденному житті громадян, так і «природнім» обмеженням деяких прав і свобод громадян в умовах особливих правових режимів. Крім того, специфіка цифрового середовища створює значні виклики для традиційних методів збору, фіксації та представлення доказів, що, у свою чергу, потребує розробки нових правових та технологічних підходів.

Аналіз останніх досліджень і публікацій. Проблематикою структуризації сучасного правового поля інформаційної безпеки у системі забезпечуючих елементів національної безпеки та у ракурсі необхідності протистояння гібридним аспектам повномасштабної збройної агресії російської федерації та іншім загрозам зовнішнього характеру займається (або, принаймні, донедавна займалися) все більш зростаюча кількість дослідників, серед яких: Баранов О.А., Бєлєвцева В.В., Богуцький П.П., Веселова Л.Ю., Гаврильців М.Т., Горулько В.В., Діордіца І.В., Довгань О.Д., Золотар О.О., Козьміних А.В., Кундеус О.М., Леоненко Н.А., Настюк В.Я., Павленко В.С., Подорожна Т.С., Поступна О.В., Ткачук Т.Ю., Шемчук В.В. та інші.

Мета статті – окреслити організаційно-правову проблематику забезпечення безпеки інформаційного та кібер-середовища у структурі забезпечуючи елементів національної безпеки, що виникає в умовах чинності особливих правових режимів та у зв’язку із об’єктивним поступальним розвитком відповідного кола суспільних відносин.

Виклад основного матеріалу. Як зазначає Т.С. Подорожна, діяльність як вищого військово-політичного керівництва російської федерації, армії та інших силових структур росії, так і безпосередніх виконавців-кібертерористів зокрема, - перевищує граничні межі базових гуманітарних норм (у цьому аспекті російська федерація може розглядатися як надзвичайно небезпечний терористичний актор сучасної епохи). При цьому спостерігається як нехтування основними положеннями міжнародного гуманітарного права, так і загальними принципами людяності. За таких умов немає смислу апелювати до агресора з метою примусити його дотримуватись у збройній боротьбі прав людини, не нехтувати та не ігнорувати норми міжнародного гуманітарного права. Практично щоденно потужні кібератаки з використанням передових інформаційних технологій спрямовуються проти національних урядових інституцій, медіа, об'єктів критичної інфраструктури, систем життєзабезпечення тощо. Все це становить компонент організованої кібернетичної агресії російської федерації проти України [1, с. 493].

Водночас, застосування інформаційних технологій та телекомунікаційних мереж, особливо в системі національної безпеки та оборонній галузі, стає звичайною практикою повсякденної діяльності. Збройні Сили, військові формування, правоохоронні, розвідувальні органи, служби, інші державні органи виступають і як користувачі інформаційних технологій та телекомунікаційних систем, і як потенційні об'єкти (мішені) кібероперацій супротивника. Як зазначають Н.А. Леоненко та О.В. Поступна, використовуючи телекомунікаційні та комп'ютерні мережі, важливо розуміти супутні ризики: сучасні хакерські напади створюють небезпеку не тільки для окремих індивідуумів, але й для цілих країн. Кіберзброя, яку дедалі частіше порівнюють зі зброєю масового ураження через її ефективність та руйнівний потенціал, є ключовим джерелом занепокоєння. З прискоренням розвитку інформаційних технологій зростає актуальність проблеми захисту інформаційно-телекомунікаційних систем держави [2].

Слід акцентувати, що недоліки у нормативному регулюванні використання програмного забезпечення та автоматизованих комплексів викликають значне занепокоєння, і уповноважені органи постійно досліджують і впроваджують більш ефективні правові методи захисту інформації, веб-ресурсів та програмного забезпечення від кіберзагроз. Але, враховуючи транскордонний характер кіберпростору, національні форми правового впливу, безумовно, є недостатніми. Підтвердженням важливості цього питання стала зустріч на найвищому рівні керівників держав та урядів країн-учасниць НАТО у Варшаві 2016 року. Під час події було укладено історичну домовленість між ЄС і НАТО щодо співробітництва у сфері безпеки, зокрема стосовно гібридних загроз і кіберударів. Таким чином, кіберсфера офіційно визнана на міжнародному рівні новим операційним простором поряд із традиційними: сушею, морем,

повітряним та космічним простором, а кібероперації стали обов'язковим елементом сучасних гібридних конфліктів [3].

Згідно з дослідженнями Л.Ю. Веселової, провідні світові держави - США, Великобританія, Німеччина, Франція та інші - надають пріоритетного значення кібероперaціям. Ці країни інвестують суттєві фінансові ресурси у розбудову кібернетичних можливостей своїх збройних сил та військових формувань і впроваджують комплексні стратегії для гарантування державної безпеки, оборонної спроможності та захисту стратегічно важливої інфраструктури від кіберзагроз. Враховуючи, що абсолютно безпечні мережі поки що є недосяжною ціллю, питання кібербезпеки набуло статусу першочергового завдання для розвитку сучасних армій [4, с. 131].

Як вказує нам ряд сучасних дослідників, зокрема, В.В. Коцура, на сьогоднішній день Збройні Сили, військові формування України та інші суб'єкти сектору безпеки і сил оборони інтенсивно розбудовують підрозділи кібербезпеки. Їхній швидкий розвиток значною мірою обумовлений повномасштабною агресією, яку російська федерація здійснює проти України з 2022 року. Агресор систематично експлуатує кіберпростір для досягнення своїх завдань не тільки відносно України, але й щодо інших країн, передусім стратегічних союзників України. Російська федерація розширює обсяги кібершпигунства та цілеспрямовано маніпулює суспільною свідомістю через поширення дезінформації та пропагандистських матеріалів. Головною метою таких заходів є підрив стабільності всередині держави, розповсюдження безладу та панічних настроїв, викривлення світогляду населення, що формує основу для реалізації стратегічних намірів у рамках повномасштабної загарбницької «гібридної» війни [5, с. 71, 193-194].

Дослідники Центру Разумкова зауважують, що, незважаючи на те, що гібридні конфлікти, зазвичай, пов'язують із сучасними протистояннями, варто згадати історичний досвід Радянського Союзу як зразок традиційного гібридного методу боротьби проти національно-визвольних рухів поневолених народів. Події «Громадянської війни» 1918–1921 років на українських землях, яка фактично представляла собою російсько-український військовий конфлікт, демонструє класичний приклад гібридної війни. До її компонентів належали: широкомасштабна пропаганда, формування сепаратистських територіальних одиниць, масштабне військове втручання, організовані голодомори (1921–1922, 1932–1933, 1947 р.р.), етнічні репресії, переслідування опозиційно налаштованих осіб, «мовна агресія», а також терористичні дії та розпалювання страху у суспільстві [6].

Досліджуючи події 2014-2021 років, О.М. Кундеус акцентує увагу на тому, що безпосередньому вторгненню на українську територію передував тривалий підготовчий період, який містив активну фазу нарощування та концентрацію

військового потенціалу агресора, втручання у внутрішньодержавні процеси України, електоральні маніпуляції, провокування масових заворушень, формування підривних структур і, що найважливіше, планомірну інформаційну обробку українського населення та міжнародної спільноти, а також потужні кібератаки на державну інфраструктуру напередодні повномасштабного наступу. Саме вторгнення стало фінальною частиною цієї гібридної драми [7, с. 122].

Природно, що згаданий автор не міг у 2020 році передбачити масштабні кібератаки на сервери державних органів, зокрема Міністерства оборони, Генерального штабу ЗСУ, урядових інституцій тощо за тиждень до повномасштабного військового наступу, однак загальну аналітичну схему гібридних методів, підходів та інструментів агресора, особливо широке використання кібератак, він спрогнозував досить точно.

За системними дослідженнями М.В. Цюрупи, з 2014 року російська федерація реалізує деструктивні стратегії, підсилюючи до критичного ступеня ризики для національної безпеки України за наступними ключовими векторами:

1. Інформаційна боротьба: агресор проводить масштабну пропагандистську операцію, формуючи альтернативну «зомбі-реальність»; дезінформація стала офіційно визнаним засобом для розпалювання ворожнечі. Через підконтрольні медіа, керованих журналістів і спеціальні підрозділи інформаційної боротьби, росія розповсюджує неправдиві та викривлені відомості, маніпулює суспільними настроями, дезорієнтує населення України та західних країн, послаблює підтримку українського керівництва всередині держави.
2. Дипломатичний примус: на міжнародному рівні через міжнародні організації російська федерація пред'являє категоричні вимоги, позиціонуючи дипломатію, насамперед, як низку агентурних спецоперацій.
3. Підривна діяльність: росія координує деструктивні операції спецслужб, формує «п'яті колони», здійснює терористичні атаки та прагне організувати кримінальний безлад на території України.
4. Економічне примушування: окрім маніпуляцій в енергетичній галузі (передусім, так звані «газові війни», що тривали з початку 2000-х років), росія використовувала масштабний економічний тиск, комбінуючи його з соціально-культурними втручаннями.
5. Гуманітарний напрямок: росія втручається в історичну свідомість, мовну стратегію, культурну сферу, нав'язує російські цінності, створює домінування низькоякісної масової культури в інформаційному середовищі України [8, с. 59-60].

Як функціонування країни в умовах правового статусу воєнного стану, так і безперервний прогрес сучасного українського соціуму та держави об'єктивно пов'язаний із постійною потребою попередження різноманітних ризиків. За твердженням В.В. Горулька, боротьба з гібридними ризиками в інформаційній

галузі, зокрема в кіберсередовищі, включає широкий спектр проблем, що стосуються національної безпеки. Це потребує поглибленого аналізу обстановки та вивчення чинників, які перешкоджають ефективному реагуванню на подібні ризики, особливо щодо охорони прав і свобод громадян, а також інтересів соціуму і держави. Водночас, об'єктивність і обґрунтованість висновків такого дослідження потребує відповідної методологічної бази, надійності використовуваних даних та верифікованості джерел, з яких ці дані здобуті [9, с. 106].

Процеси глобалізації суспільних процесів та інтенсивний технологічний прогрес свідчать про те, що інформаційне суспільство нині проникає у всі сфери функціонування людини та державних структур. Кіберпростір перетворився на фундаментальний ресурс економічного, політичного та соціального характеру. Разом з тим, технологічні досягнення в галузі інформаційних відносин, незважаючи на відкриття нових перспектив для розвитку, сформували підґрунтя для різноманітних зловживань. Особливо з розвитком інтернет-технологій з'явилася особлива категорія ризиків для національної безпеки. У зв'язку з цим, А.В. Козьміних підкреслює, що питання кібербезпеки набуває критичного значення, особливо коли наслідки втілення загроз у сферах застосування комп'ютерних та телекомунікаційних технологій досягають великих масштабів. Глобалізація інформаційних процесів характеризується посиленням кіберризиків, що корелюють із сучасними технологічними викликами [10, с. 205].

На погляд В.С. Павленко, беззаперечним є факт, що залежність соціуму, індивіда та національних інфраструктур (енергетична, транспортна, телекомунікаційна галузі тощо) від роботи інформаційно-телекомунікаційних технологій підвищує їхню вразливість перед кіберризиками. Це збільшує вірогідність виникнення кризових ситуацій, формує реальні ризики для життєдіяльності суспільства та держави, перешкоджає соціально-економічному прогресу та загрожує національній безпеці України [11, с. 30].

Стратегія кібербезпеки України під назвою «Безпечний кіберпростір – запорука успішного розвитку країни», прийнята Указом Президента України від 26 серпня 2021 року № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», акцентує увагу на тому, що інформаційні технології забезпечують можливості для соціально-економічного прогресу, реалізації права на доступ до інформації та результативного державного управління. Водночас, ці технології роблять урядові, військові, фінансові та інші системи винятково вразливими до кіберзагроз. Більше того, сучасні технології істотно спрощують здійснення злочинної діяльності, гарантуючи конфіденційність і легкий доступ для порушників. Розширення застосування інформаційних технологій супроводжується зростанням кіберризиків, включно з кіберзлочинністю, що значно впливає на безпеку численних користувачів.

Таким чином, кіберзагрози не тільки порушують роботу певних технологічних систем, але й здатні дестабілізувати функціонування державного апарату та суспільство в цілому, розповсюджуючи панічні настрої та безлад, що є типовою ознакою застосування «гібридних» форм боротьби у збройному протистоянні чи інших видах міждержавного конфлікту. Показовим прикладом цього служить російсько-українська війна, де кіберпростір перетворився на значуще поле протистояння. Росія застосовує: кібершпигунство, поширення неправдивої інформації, економічний тиск і інші підривні дії для досягнення своїх стратегічних завдань.

У відповідь на ці проблеми, Україна разом із країнами-стратегічними партнерами, серед яких: Велика Британія, Німеччина, Франція, Фінляндія, Польща, - інтенсивно розробляють системи кіберзахисту. Пріоритетним завданням стає гарантування безпеки інформаційних систем і мереж, а також формування дієвих стратегій протистояння кібератакам з боку російської федерації. Ефективне втілення таких стратегій вимагає міжнародного співробітництва, суттєвих капіталовкладень у розвиток кіберзахисту, підготовку професійних кадрів та впровадження новітніх технологій.

Висновки. Базуючись на результатах проведеного аналізу, можна констатувати, що в умовах протидії повномасштабній збройній агресії, подальших геополітичних трансформацій та комп'ютеризації всіх суспільних сфер, посилились зовнішні виклики і ризики, а також небезпеки в інформаційному середовищі. На сучасному рівні розвитку суспільства і держави серед найбільш актуальних ризиків для національної інформаційної безпеки, враховуючи динамічний характер інформаційної сфери, варто виділити: неправомірний вплив на національні інформаційні ресурси, інформаційно-телекомунікаційні системи та інформаційну інфраструктуру; застосування засобів та способів розповсюдження хибної інформації для введення в оману людей, використовуючи при цьому, зокрема, техніки психологічного впливу для дезорганізації та пригнічення волі; неавторизоване проникнення в національний інформаційний простір; кібератаки на державні автоматизовані системи керування, комунікацій, банківську та промислову галузі, корпоративні та персональні бази даних. З урахуванням цього, трансформація інформаційного та кіберпросторів в сучасних умовах існування нашої держави визначили новий напрям розвитку правового регулювання інформаційної безпеки в Україні з урахуванням міжнародних стандартів у цій галузі.

Література:

1. Подорожна Т.С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. *Аналітично-порівняльне правознавство*. 2023. № 6. С. 491–497. URL: https://app-journal.in.ua/wp-content/ uploads/2023/12/87.pdf.

2. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України*. Серія: Державне управління. 2022. Вип. 2 (17). URL: http://repositsc.nuczu.edu.ua/ handle/123456789/16883.

3. НАТО та ЄС підписали угоду про співпрацю у сфері кіберзахисту. 10 лютого 2016. [Інформаційний портал: Європейська правда. Міжнародна безпека та євроінтеграція України]. URL: https:// www.eurointegration.com.ua/ news/2016/02/10/7044661/.

4. Веселова Л.Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади / *Монографія*: «Видавничий дім Гельветика», 2021. 488 с. URL: https://oldiplus.ua/ kibernetychna-bezpeka-v-umovah-gibrydnoyi-vijny-administratyvno-pravovi-zasady/?srsltid=Afm BOorK94nc2dFIrOen7mfFB0 e2jNIS4ZjgA2Z_sBKccsce5vwJioPl.

5. Війна росії проти України: від гібридних форм до геноцидних практик: *матеріали Міжнародної науково-практичної конференції* (9 грудня 2024 року) / за заг. ред. В.В. Коцура. Укладач Л.М. Переяслав, 2024. 340 с. URL: http://repositsc.nuczu.edu.ua/ bitstream/123456789/ 23766/1/Збірник.pdf.

6. «Гібридна» війна Росії – виклик і загроза для Європи. *Національна безпека і оборона*. № 9-10 (167-168). Український центр економічних і політичних досліджень імені Олександра Разумкова. 2016. URL: https://razumkov.org.ua/uploads/journal/ukr/NSD167-168_ 2016_ukr.pdf.

7. Кундеус О.М. Теоретичні аспекти гібридної війни РФ проти України / *Регіональні студії*. Ужгород, Видавничий дім «Гельветика». Вип. 20. 2020. С.120-124. URL: https://dspace. uzhnu.edu.ua/jspui/handle/lib/39665.

8. Цюрупа М.В. Питання визначення сутності «гібридної війни»: на прикладі збройної боротьби на сході України (середина 2014 – кінець 2015 рр.) / *Наукові записки Інституту політичних і етнонаціональних досліджень*. 2015. Випуск 5/6 (79/80). ІПіЕНД імені І.Ф. Кураса НАН України. С. 56-65. URL: https://ipiend.gov.ua/wp-content/uploads/2018/ 07/tsurupa_ pytannia.pdf.

9. Горулько В.В. Роль і місце інформаційної безпеки в загальній системі національної безпеки держави. *Вісник Харківського національного університету імені В.Н. Каразіна.* Серія «Право». 2022. Вип. 34. С. 103–108.

10. Козьміних А.В. Кібербезпека та кібератаки в умовах гібридної війни / Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): у 2 т.: *матеріали Міжнародної науково-практичної конференції* (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т. 1. С. 204-205. URL: https://dspace.onua.edu.ua/items/def63c74-7a11-4c75-9789-6671cab4e57e.

11. Павленко В.С. Сутність кібербезпеки у теорії інформаційного права. *Право та державне управління*. 2021. № 2. С. 28–33.

References:

1. Podorozhna , T.S. (2023). Zabezpechennja informacijnoї bezpeki Ukraïni v umovah suchasnih viklikiv ta zagroz z boku RF [Ensuring information security of Ukraine in the context of modern challenges and threats from the Russian Federation]. *Analitichno-porivnjal'ne pravoznavstvo - Analytical and comparative jurisprudence,* 6, 491–497. Retrieved from https://app-journal.in.ua/wp-content/ uploads/2023/ 12/87.pdf. [in Ukrainian].

2. Leonenko, N.A., Postupna , O.V. (2022). Informacijna bezpeka Ukraïni: mehanizmi, suchasni vikliki ta zagrozi v umovah informacijnogo globalizmu [Postupna O.V. Information security of Ukraine: mechanisms, modern challenges and threats in the context of information globalism]. *Visnik Nacional'nogo universitetu civil'nogo zahistu Ukraïni. Serija: Derzhavne upravlinnja -Bulletin of the National University of Civil Defense of Ukraine. Series: State Administration,* 2 (17). Retrieved from http://repositsc.nuczu. edu.ua/handle/123456789/16883. [in Ukrainian].

3. NATO ta ЄS pidpisali ugodu pro spivpracju u sferi kiberzahistu. 10 ljutogo 2016. [Informacijnij portal: Євropejs'ka pravda. Mizhnarodna bezpeka ta євrointegracija Ukraïni]. [NATO and the EU signed an agreement on cooperation in the field of cyber defense. February 10, 2016. [Information portal: European Truth. International Security and European Integration of Ukraine]]. *www.eurointegration.com.ua* Retrieved from https:// www.eurointegration.com.ua/ news/2016/02/ 10/7044661/. [in Ukrainian].

4. Veselova , L.Ju. (2021). *Kiberbezpeka v umovah gibridnoï vijni: administrativno-pravovi zasadi [Cybersecurity in the context of hybrid warfare: administrative and legal principles]*. K.: «Vidavnichij dim Gel'vetika». Retrieved from https://oldiplus.ua/ kibernetychna-bezpeka-v-umovah-gibrydnoyi-vijny-administratyvno-pravovi-zasady/?srsltid=Afm BOorK94nc2dFIrOen7mfFB0 e2jNIS4ZjgA2Z_sBKccsce5vwJioPl. [in Ukrainian].

5. V.V. Kocura. Ukladach L.M. (2024). *Vijna rosiï proti Ukraïni: vid gibridnih form do genocidnih praktik [Russia's War Against Ukraine: From Hybrid Forms to Genocide Practices*]. Retrieved from http://repositsc.nuczu.edu.ua/ bitstream/123456789/23766/1/Zbirnik.pdf. [in Ukrainian].

6. «Gibridna» vijna Rosiï – viklik i zagroza dlja Євropi [Russia's "Hybrid" War - a Challenge and Threat to Europe]. *Nacional'na bezpeka i oborona - National Security and Defense,* 9-10, 167-168. Retrieved from https://razumkov.org.ua/uploads/journal/ukr/NSD167-168_ 2016_ukr.pdf. [in Ukrainian].

7. Kundeus , O.M. (2020). Teoretichni aspekti gibridnoï vijni RF proti Ukraïni [Theoretical aspects of the hybrid war of the Russian Federation against Ukraine]. *Regional'ni studiï - Regional studies* , 20, 120-124. Retrieved from https://dspace.uzhnu.edu.ua/jspui/handle/lib/39665. [in Ukrainian].

8. Cjurupa , M.V. (2015). Pitannja viznachennja sutnosti «gibridnoï vijni»: na prikladi zbrojnoï borot'bi na shodi Ukraïni (seredina 2014 – kinec' 2015 rr.) [The question of defining the essence of "hybrid war": on the example of armed struggle in eastern Ukraine (mid-2014 - end of 2015)]. *Naukovi zapiski Institutu politichnih i etnonacional'nih doslidzhen' - Scientific notes of the Institute of Political and Ethno-National Studies* , 5/6 (79/80), 56-65. Retrieved from https://ipiend. gov.ua/wp-content/uploads/ 2018/07/tsurupa_pytannia.pdf. [in Ukrainian].

9. Gorul'ko , V.V. (2022). Rol' i misce informacijnoï bezpeki v zagal'nij sistemi nacional'noï bezpeki derzhavi [The role and place of information security in the general system of national security of the state]. *Visnik Harkivs'kogo nacional'nogo universitetu imeni V.N. Karazina. Serija «Pravo»- Bulletin of the V.N. Karazin Kharkiv National University. Series "Law"* , 34, 103–108 [in Ukrainian].

10. Koz'minih, A.V. (2022). *Kiberbezpeka ta kiberataki v umovah gibridnoï vijni [Cybersecurity and cyberattacks in the conditions of hybrid war]*. Євropejs'kij vibir Ukraïni, rozvitok nauki ta nacional'na bezpeka v realijah masshtabnoï vijs'kovoï agresiï ta global'nih viklikiv HHI stolittja» (do 25-richchja Nacional'nogo universitetu «Odes'ka juridichna akademija» ta 175-richchja Odes'koï shkoli prava): u 2 t.: materiali Mizhnarodnoï naukovo-praktichnoï konferenciï (m. Odesa, 17 chervnja 2022 r.) / za zagal'noju redakcієju S. V. Kivalova. Odesa: Vidavnichij dim «Gel'vetika», 2022. T. 1. S. 204-205. URL: https://dspace.onua.edu.ua/items/def63c74-7a11-4c75-9789-6671cab4e57e. [in Ukrainian].

11. Pavlenko, V.S. (2021). Sutnist' kiberbezpeki u teoriï informacijnogo prava [The essence of cybersecurity in the theory of information law]. *Pravo ta derzhavne upravlinnja -Law and public administration,* 2, 28–33 [in Ukrainian].