УДК 342.9
DOI https://doi.org/10.32841/2307-1745.2021.54.1.11

Онопрієнко С. Г.,
кандидат юридичних наук,
старший викладач кафедри правового забезпечення
Військового інституту
Київського національного університету імені Тараса Шевченка

СОЦІАЛЬНЕ ПРИЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПЕРІОД «ГІБРИДНИХ ВІЙН»: ПРАВОВІ АСПЕКТИ

Анотація. Мета статті – визначити сутність соціального призначення інформаційної безпеки у період «гібридних» війн.

У статті з'ясовано, що епоха постмодерну суттєво змінила характер взаємодії на міжнародній арені, висуваючи на передній план інформаційно-психологічні способи досягнення державами своїх цілей. Розвиток інформаційних технологій дає змогу дистанційно впливати на великі аудиторії, у яких ефективно формуються бажані для суб'єктів впливів ціннісні установки, потреби та настрої. За таких умов змінюється характер війн, вони переміщуються в інформаційне середовище.

Обґрунтовано, що російська збройна агресія проти України поєднується з комплексним, системним та систематичним інформаційним впливом на противника на різні соціальні групи в Україні. Ефективна система забезпечення інформаційної безпеки в Україні ще не створена, що вимагає здійснення комплексу дій теоретико-методологічного, правового, організаційного, техніко-технологічного, соціально-психологічного та іншого характеру.

З'ясовано, що гібридний характер сучасних війн зумовлює підвищення значущості інформаційної безпеки для збереження сталих суспільних відносин, для забезпечення державного суверенітету та територіальної цілісності, створення сприятливих умов для розвитку громадянського суспільства та держави, реалізації прав і свобод людини та громадянина.

Визначено, що соціальне призначення інформаційної безпеки у період «гібридних війн» полягає перш за все у створенні, зміцненні та підтриманні інформаційного суверенітету. Крім того, соціальне призначення інформаційної безпеки пов'язано з наданням можливості громадянському суспільству в цілому, його інститутам, окремим громадянам реалізовувати своє право на участь у системі публічного управління. З'ясовано, що важливим елементом досліджуваного феномену є унеможливлення деструктивного впливу, спрямованого на формування некритичності у сприйнятті інформації, правового нігілізму тощо.

Зроблено висновок, що «гібридні війни» уявляють собою комплекс дій, пов'язаних із реалізацією військових, інформаційно-технологічних, інформаційно-психологічних, публічно-адміністративних, фінансово-економічних та інших засобів, за допомогою яких одні держави можуть впливати на інші без формального порушення державних кордонів. Це потребує від сучасних держав адекватного реагування на рівні створення систем інформаційної безпеки. Призначення таких систем полягає у нівелюванні інформаційних ризиків та попередженні деструктивного впливу на інформаційний суверенітет держави. Вказане потребує створення несуперечливого правового забезпечення інформаційної безпеки, яке маж відповідати принципам гнучкості і правової визначеності.

Ключові слова: військове право, право національної безпеки, інформаційні правовідносини, інформаційна безпека, «гібридні війни», інформаційні права, інформаційний суверенітет.

Постановка проблеми. Епоха постмодерну суттєво змінила характер взаємодії на міжнародній арені, висуваючи на передній план не силові, а інформаційно-психологічні способи досягнення державами та іншими суб'єктами міжнародних відносин своїх цілей. Розвиток інформаційних технологій дає змогу дистанційно впливати на великі аудиторії, у яких ефективно формуються бажані для суб'єктів впливів ціннісні установки, потреби та настрої. Із кожним роком зростають можливості таргетування реклами, коли інформаційні впливи застосовуються до окремих цільових груп залежно від їхнього соціального статусу, гендерних, вікових, національних, економічних та інших ознак, з урахуванням максимального можливого ефекту для кожного індивідуума. За таких умов змінюється характер війн, вони переміщуються в інформаційне середовище. Прикладом вдалого використання інформаційних технологій є захоплення влади в Афганістані рухом Талібан, який шляхом власної пропагандистської роботи в соціальних мережах, фінансування повідомлень в мережі інтернет відомих блогерів та інфлюєнсерів, а також вдалого поширення бажаної інформації через своїх агентів впливу в районах, де більшість населення є неписьменною, сформував у суспільстві бажане відношення до своєї діяльності, після чого швидко та практично без втрат узяв під контроль територію 39- мільонної держави.

Російська збройна агресія проти України також поєднується з комплексним, системним та систематичним впливом на противника на різні соціальні групи в Україні. За вісім років в нашій державі було сприйнято велику кількість спроб побудувати систему протидії інформаційним впливам Російської Федерації, спрямованих на дестабілізацію суспільних відносин, дискредитацію органів публічної влади та окремих посадових осіб, виникнення панічних настроїв та штучного розшарування регіонів України за мовними, релігійними та іншими ознаками. Однак нині ефективна система забезпечення інформаційної безпеки в Україні ще не створена, що вимагає здійснення комплексу дій теоретико-методологічного, правового, організаційного, техніко-технологічного, соціально-психологічного та іншого характеру, що слугує підтвердженням актуальності теми цієї статті.

Мета статті – визначити сутність соціального призначення інформаційної безпеки у період «гібридних» війн.

Аналіз останніх публікацій і досліджень. Питання розвитку законодавства про інформаційну безпеку та протидії інформаційним впливам під час ведення «гібридних» війн розглядали у своїх роботах такі науковці, як І. Арістова, К. Бєляков, В. Горбулін, О. Довгань, О. Дзьобань, О. Золотар, Р. Калюжний, Б. Кормич, Є. Магда, А. Марущак, О. Олійник, Є. Скулиш, О. Соснін, М. Требін, В. Цимбалюк, Л. Чекаленко, Г. Яворська та інші науковці. Разом із тим складність та багатоплановість проблем розвитку правового забезпечення інформаційної безпеки зумовлює необхідність наукових розвідок за даним напрямом.

Виклад основного матеріалу. Кожна сучасна цивілізована правова держава для виконання своїх функцій потребує додержання низки умов, серед яких найважливішими є територіальна цілісність та недоторканість, суверенітет (у тому числі інформаційний), демократичний лад, сталість громадянського суспільства, стабільні економічні відносини, належний стан публічної безпеки та громадянського порядку та низка інших. Розвиток інформаційних технологій уможливлює спричинення шкоди можливості держави виконувати свої функції без прямого порушення її територіальності цілісності (хоча, як це мало місце з окупацією Російською Федерацією Автономної Республіки Крим, інформаційна агресія може передувати збройній, полегшуючи здійснення останньої). Виникнення феномену «гібридних» війн є властивістю суспільства епохи постмодерну, для якого характерними є зміна традиційних механізмів адаптації особистості до умов соціуму, втім, як і зміни самого соціуму. Як справедливо вказують О. Соснін і О. Дзьобань, нині віртуальні світи як невід'ємна частина життя беруть безпосередню участь у соціалізації людини. Неможливість максимально плідно пройти процес соціалізації в силу багатьох причин і проблем, що містяться як у наявній дійсності, так і в самій людині, змушує її звернутися за допомогою до віртуальних світів. Перебування у віртуальних світах, а також саме переміщення з актуального світу у віртуальні й назад, здатні дати людині можливість досягнення власної повноти буття. Сучасна особистість постмодерну часто балансує між життєвими позиціями, втіленими в активних соціальних перетвореннях (всупереч усьому або співвідносячи з наявною дійсністю) або зневагою до актуальної реальності на користь віртуальної [1, с. 69].

Це полегшує формування в особистості бажаних цінностей, відношень та настроїв за допомогою системи інформаційних впливів, до ознак яких відносять цілеспрямованість. Усі суб'єкти інформаційних впливів намагаються досягти однієї мети – формування бажаної поведінки індивіда. При цьому цілі деяких з них не перетинаються (наприклад, формування електоральної, споживчої та професійної поведінки в певних випадках може здійснюватися без особливих суперечностей між суб'єктами впливу, якщо кожен з них має свою обмежену сферу інтересів). Проте усередині кожної групи суб'єктів такі цілі можуть значно диференціюватися (як це відбувається під час виборчих або рекламних кампаній, наприклад). Ознака цілеспрямованості може бути наявна, навіть якщо цілі на вербальному рівні не усвідомлюються (наприклад, у родинних сценаріях виховання жертовної або агресивної поведінки). Крім того, інформаційні впливи завжди несуть у собі певне повідомлення, призначене наблизити поведінку індивіда до бажаної [2, с. 136]. Крім того, індивідуальний характер активності особистості в інформаційній сфері зумовлює відсутність можливості оперативного моніторингу наслідків таких впливів: необхідні спеціальні дослідження для отримання актуальної інформації щодо наявності чи відсутності деструктивних тенденцій та інших негативних явищ, що не завжди уявляється можливим. Вказані ознаки інформаційних впливів перетворюють їх в ефективну зброю «гібридних» війн.

Вважається, що термін «гібридна війна» з'явився ще у 2005 році й став застосовуватися для опису стратегії Хезболли в Ліванській війні 2006 року. Із того часу лексема «гібридна» є домінуючою під час обговорення сучасних і майбутніх воєнних дій до такого ступеня, що вище військове керівництво взяло його на озброєння й використовує як основу сучасних воєнних стратегій. Аналізуючи ступінь наукової розробки дослідження проблеми, дослідники підкреслюють, що загалом науці міжнародного права бракує розуміння поняття «гібридна війна» [3, с. 49].

«Гібридна війна», як влучно зауважують фахівці з військових наук, ведеться як внутрішніми силами, що мають на меті послабити або повалити владу, так і зовнішніми. Дії зовнішніх сил полягають у сприянні сепаратистам та терористам у вербуванні прихильників і їх підготовці, впливі на економіку та соціальну сферу, координації дипломатичних зусиль, а також проведенні окремих силових акцій. Для таких цілей залучають сили спеціальних операцій, розвідки, сформовані заздалегідь формування сепаратистів, терористів, групи бойовиків, групи організованої злочинності, які також здійснюють масштабний інформаційно-психологічний вплив на населення, особовий склад збройних сил і правоохоронних органів, органи влади з використанням усього діапазону інформаційно-комунікаційних технологій. Вказаний підхід дав змогу авторам визначити досліджуване поняття як сукупність заздалегідь підготовлених та оперативно реалізованих дій військового, дипломатичного, економічного, інформаційного характеру, спрямованих на досягнення стратегічних цілей. Її ключове значення полягає в підпорядкуванні інтересів однієї держави іншій в умовах формального збереження політичного устрою країни. До базових компонентів «гібридної війни» вони відносять традиційні та нестандартні загрози, тероризм, підривні дії, новітні і нешаблонні інформаційні технології для протидії супротивникові, який є більш могутнім військово та політично [4, с. 126–128]. Додамо, що інформаційні технології, як свідчить, зокрема, досвід України, не обов'язково використовуються у протиборстві з більш могутніми у військовому відношенні державами, втім, безумовно, їх використання дозволяє вирішити частину військових завдань невійськовими методами.

Гібридний характер сучасних війн зумовлює підвищення значущості інформаційної безпеки для збереження сталих суспільних відносин, для забезпечення державного суверенітету та територіальної цілісності, створення сприятливих умов для розвитку громадянського суспільства та держави, реалізації прав і свобод людини та громадянина. Інформаційна безпека як складне соціальне явище постає в багатьох аспектах, серед яких найбільше значення, на нашу думку, мають правовий, технологічний та соціально-психологічний. У правовому аспекті інформаційна безпека уявляє собою комплекс інформаційно-правових засобів, у першу чергу правових норм, сукупність яких дозволяє поєднувати теорію і практику правового

регулювання, досягаючи його цілей. Із точки зору правової ґенези норми, призначені регулювати відносини із забезпечення інформаційної безпеки, мають комплексний характер та поєднують у собі елементи норм інформаційного та адміністративного права, права національної безпеки та військового права [5]. У технологічному аспекті інформаційна безпека уявляє собою сукупність виробничих операцій, які змінюють наявний стан захищеності інтересів людини, суспільства та органів публічної влади в інформаційній сфері, завдяки перетворенню існуючих або запровадження нових способів та методів інформаційної діяльності. У соціально-психологічному аспекті інформаційна безпека має розумітися як сукупність особистісних характеристик індивідуальних суб'єктів інформаційних відносин, які зумовлюють збільшення або зменшення інформаційних ризиків під час вибору ними варіантів поведінки під час здійснення діяльності в інформаційній сфері. Крім того, можна виокремити публічно-управлінський аспект інформаційної безпеки (наприклад, шляхом убезпечення правовідносин, пов'язаних зі здійсненням громадського нагляду (контролю) за діяльністю органів публічного адміністрування [6, с.195]), фінансово-економічний, пов'язаний із забезпеченням сталості економічних відносин.

Отже, соціальне призначення інформаційної безпеки в період «гібридних війн» полягає перш за все у створенні, зміцненні та підтриманні інформаційного суверенітету як властивості системи публічного управління певної держави забезпечувати додержання верховенства права, законності, прав і свобод людини та громадянина, безперешкодне здійснення інформаційної діяльності органів публічного адміністрування, фізичних та юридичних осіб в інформаційних правовідносинах, що виникають, змінюються та припиняються в межах державних кордонів. Крім того, соціальне призначення інформаційної безпеки пов'язано з наданням можливості громадянському суспільству в цілому, його інститутам, окремим громадянам реалізовувати своє право на участь у системі публічного управління шляхом доступу до публічної інформації, вільного збирання, накопичення, аналізу, обробки, поширення різноманітних відомостей та даних, а також здійснення громадського нагляду (контролю) без шкоди для національної безпеки. Не менш важливим елементом досліджуваного феномену є те, що за допомогою засобів та інструментів інформаційної безпеки унеможливлюється деструктивний вплив зацікавлених у дестабілізації суспільних відносин суб'єктів, спрямований на формування особистості з бажаними для них якостями, як-то: некритичність у сприйнятті інформації, правовий нігілізм, навіюваність, нестійкість, легкість виникнення панічних настроїв тощо.

Висновки. «Гібридні війни» як комплекс дій, пов'язаних із реалізацією військових, інформаційно-технологічних, інформаційно-психологічних, публічно-адміністративних, фінансово-економічних та інших засобів, за допомогою яких одні держави можуть впливати на інші без формального порушення державних кордонів, потребують від сучасних держав адекватного реагування на рівні створення систем інформаційної безпеки. Призначення таких систем полягає в нівелюванні інформаційних ризиків та попередженні деструктивного впливу на інформаційний суверенітет держави. Вказане потребує створення несуперечливого правового забезпечення інформаційної безпеки, достатньо гнучкого, щоб відповідати викликам часу, і такого, що відповідає принципу правової визначеності (для попередження довільного тлумачення змісту правових норм та відмови від їх виконання внаслідок надмірної складності використовуваних правових конструкцій і термінології). Це визначає спрямованість подальших наукових пошуків, метою яких мають стати формулювання сутності та характеристики змісту правових засобів забезпечення інформаційної безпеки в умовах «гібридних війн».

Література:

1. Дзьобань О.П., Соснін О.В. Віртуальна реальність суспільства постмодерну як соціокультурне тло соціалізації «людини інформаційної». *Гуманітарний вісник Запорізької державної інженерної академії.* 2017. № 69(1). С. 69–76.
2. Шопіна І.М. Інформаційно-психологічні впливи як категорія інформаційного права: поняття, ознаки, особливості дослідження. *Наука і правоохорона.* 2017. № 4. С. 134–140.
3. Комарчук О. Гібридна війна: сутність та структура феномену. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2018. № 1(3). С. 48–54.
4. Міхєєв Ю.І., Чернявський Г.П., Турченко Ю.В., Пінчук, О.І. Дефініції поняття «гібридна війна». *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.* 2016. № 51. С. 124–130.
5. Шопіна І.М., Гущин О.О. Актуальні проблеми сучасного стану розвитку воєнного (військового) права як науки і навчальної дисципліни. *Форум права.* 2017. № 2. С. 144–148. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2017_2_24 (дата звернення: 11.12.2021).
6. Shopina, I, Kobets, M., Tarasov, S., «Non-Governmental Control in the Sphere of National Security of Ukraine». Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021). *Advances in Economics, Business and Management Research*, volume 188, pp. 194–199. URL: https://dx.doi.org/10.2991/aebmr.k.210826.034 (дата звернення: 11.12.2021).

Onopriienko S. Social purpose of information security in the period of "hybrid wars": legal aspects

Summary. The purpose of the article was to determine the essence of the social purpose of information security in the period of "hybrid wars".

The article establishes that the postmodern era has significantly changed the nature of interaction in the international arena, bringing to the fore information and psychological ways to achieve their goals by states. The development of information technologies makes it possible to remotely influence large audiences, in which value attitudes, needs and moods desired by the subjects of influence are effectively formed. Under such conditions, the nature of wars is changing, they are moving into the information environment.

The rationale is provided that the Russian armed aggression against Ukraine is combined with the complex, systemic and systematic informational influence of the enemy on various social groups in Ukraine. An effective information security system has not been created in Ukraine, which requires the implementation of a set of actions of a theoretical, methodological, legal, organizational, technical, technological, socio-psychological and other nature.

Arguments are given that the hybrid nature of modern wars causes an increase in the importance of information security to preserve established social relations, to ensure state sovereignty and territorial integrity, create favorable conditions for the development of civil society and the state, the realization of human and civil rights and freedoms.

The article found that the social purpose of information security in the period of "hybrid wars" is primarily to create, strengthen and maintain information sovereignty. In addition, the social purpose of information security is associated with providing an opportunity for civil society as a whole, its institutions, and individual citizens to exercise their right to participate in the public administration system. It was found that an important element of the phenomenon under study is the prevention of destructive impact aimed at the formation of non-criticality in the perception of information, legal nihilism, etc.

The conclusion is drawn that "hybrid wars" are a set of actions related to the implementation of military, information technology, information and psychological, public administrative, financial and economic and other means by which some states can influence others without a formal violation of state borders. This requires modern states to adequately respond at the level of creating information security systems. The purpose of such systems is to level information risks and prevent a destructive impact on the information sovereignty of the state. The above requires the creation of a consistent legal framework for information security, which must comply with the principles of flexibility and legal certainty.

Key words: military law, national security law, information legal relations, Information Security, "hybrid wars", information rights, information sovereignty.