УДК 342.95:351.863

ГУРЖІЙ Тарас,
д. ю. н., професор, завідувач кафедри адміністративного, фінансового та інформаційного права Київського національного торговельно-економічного університету

ІНФОРМАЦІЙНЕ ПРАВО: ВИКЛИКИ ГІБРИДНОЇ ВІЙНИ

Проаналізовано сучасний стан та перспективи розвитку національного інформаційного права. На прикладі сучасної України визначено коло інформаційних загроз гібридної війни, проаналізовано їх вплив на сферу національної безпеки, окреслено напрями нейтралізації, зокрема – засобами інформаційного права. Виснувано, що концепція розвитку національного інформаційного права в умовах гібридної війни має ґрунтуватися на ідеях балансу між інтересами національної безпеки та ідеями верховенства права.

Ключові слова: гібридна війна, національна безпека, інформаційна безпека, інформаційна війна, кібербезпека, інформаційне право, свобода думки, право на інформацію.

Гуржий Т. Информационное право: вызовы гибридной войны. *Проанализированы современное состояние и перспективы развития национального информационного права. На примере современной Украины определен круг информационных угроз гибридной войны, проанализировано их влияние на сферу национальной безопасности, определены направления нейтрализации, в том числе – средствами информационного права. Сделан вывод о том, что концепция развития национального информационного права в условиях гибридной войны должна основываться на идеях баланса между интересами национальной безопасности и идеями верховенства права.*

Ключевые слова: гибридная война, национальная безопасность, информационная безопасность, информационная война, кибербезопасность, информационное право, свобода мысли, право на информацию.

Постановка проблеми. Сучасна парадигма міждержавних стосунків ґрунтується на безумовній повазі державного суверенітету та нетерпимості до випадків збройного тиску на членів світової спільноти. Будь-які акти збройної агресії підлягають загальному осуду та тягнуть за собою застосування широкого комплексу політичних і економічних санкцій, покликаних стати непідйомним тягарем для країни-агресора. За таких умов, коли відкрите збройне вторгнення загрожує нападнику міжнародною ізоляцією, втратою ринків і життєво важливих ресурсів, «груба та прямолінійна сила зброї» дедалі частіше поступається місцем завуальованим методам зовнішньо-політичного втручання (як-то

організація диверсій, проведення кібератак, підтримка сепаратистських рухів, поширення антидержавних настроїв, втручання у вибори тощо). Комплексне та координоване використання цих методів заведено іменувати «гібридною війною» (*hybrid warfare*), оскільки, на відміну від війни в класичному розумінні, вони передбачають не безпосередню збройну боротьбу, а багатоаспектну підривну діяльність, спрямовану проти ключових сфер життєдіяльності цільової (*targeted*) держави.

Масштабне розгортання такої діяльності чинить потужний вплив на всі аспекти суспільного життя. Воно обумовлює стрімку появу та зміну цілих пластів суспільних відносин, пов'язаних з участю країни в політичному, економічному та інформаційному протистоянні, мобілізацією населення, проведенням антитерористичних і військових операцій, організацією заходів безпеки, зміною статусу окремих територій, відсутністю контролю за ділянками державного кордону, запровадженням санкцій, стихійними соціальними процесами. Впорядкування цих відносин – першочергове завдання національної системи права та більшості її окремих галузей. Великою мірою саме від оперативності та якості правового реагування залежить стратегічний успіх протидії викликам гібридної війни.

Важлива роль у цьому процесі відводиться інформаційному праву, яке покликане гарантувати свободу думки та забезпечити надійний захист суспільства і держави від багатоаспектних інформаційних загроз. У сучасних умовах, коли основний вектор зовнішньо-політичної боротьби остаточно змістився до сфери інформації, інформаційне право стало необхідним інструментом забезпечення національної безпеки, зокрема – шляхом встановлення інформаційних обмежень. Одночасно воно лишається базовим індикатором рівня демократії, що змушує розглядати його розвиток крізь призму узгодження національних інтересів і громадянських свобод.

Аналіз останніх досліджень і публікацій. Через свою надзвичайну актуальність проблематика інформаційного права знайшла висвітлення в наукових працях багатьох сучасних правників, зокрема, Р. А. Калюжний, О. В. Копан та О. Г. Марценюк досліджують питання інформаційно-правового регулювання суспільних відносин та механізм реалізації права на інформацію [1]. В наукових працях А. В. Гуржій розкриваються організаційно-правові аспекти захисту персональних даних [2–4]. А. Ю. Нашинець-Наумова акцентує увагу на особливостях функціонування системи інформаційної безпеки та питаннях захисту інсайдерської інформації суб'єктів господарювання [5]. Зі свого боку, І. М. Сопілко аналізує процеси формування та реалізації інформаційної політики в умовах глобальної інформатизації та розвитку інформаційного суспільства [6].

Доводиться констатувати, що переважна більшість сучасних досліджень з інформаційного права здійснюється в контексті стабільної (мирної) зовнішньополітичної ситуації, яка не є властивою для сучасної України.

Мета статті – окреслення вихідних засад і перспектив розвитку національного інформаційного права в умовах гібридної війни.

Матеріали та методи. Поставлена мета обумовила комплексне використання загально-наукових і спеціально-юридичних методів пізнання, що уможливило охопити ключові аспекти інформаційного права як складової системи інформаційної безпеки та інструмента забезпечення інформаційних прав і свобод. Інформаційною базою дослідження стали закони України, укази Президента України, праці вітчизняних і зарубіжних науковців.

Результати дослідження. Одним з ключових компонентів гібридної війни є вторгнення в інформаційно-комунікаційний простір певної країни з метою придушення опору та формування світового політичного нормативу, узгодженого з інтересами агресора. Для цього використовуються найрізноманітніші інструменти маніпулювання громадською думкою: впровадження тенденційних медіа-проектів, створення, так би мовити, фабрик тролів, ботів, поширення фейкових новин та багато інших прийомів, які не мають нічого спільного з чесною журналістською практикою, заснованою на фактах і правді. Ці засоби передбачають таке само масштабне, як і цинічне спотворення реальності, тому особливо небезпечні для системи, що базується на ідеях справедливого інформування суспільства.

Не менш гостро в умовах гібридної війни постає питання кібербезпеки. В сучасному світі кібернетичний простір все частіше слугує для проведення широкого спектра підривних операцій: від викрадення цінної інформації до актів кібертероризму. Варто зазначити, що стрімке розширення інструментарію і масштабів кібернетичної війни відбулося саме за останнє десятиліття, упродовж якого багатьма країнами світу створено спеціалізовані підрозділи з централізованого проведення кібернетичних операцій. Тільки в Росії до складу Військ інформаційних операцій входять приблизно 1 тис. висококваліфікованих спеціалістів: математиків, програмістів, інженерів, криптографів, зв'язківців, фахівців з радіоелектронної боротьби та інших. Річний обсяг їх фінансування сягає 300 млн дол. США [7]. Про те, наскільки шкідливим та руйнівним може бути спрямування такого потужного потенціалу в гібридну війну, яскраво свідчать події, які мали місце під час президентської кампанії в США 2016 р. («*Hillary Clinton email controversy*»), атака на комп'ютерні системи Організації з безпеки та співробітництва в Європі (ОБСЄ) в 2016/2017 рр., серія хакерських атак в Україні, яка спричинила тривалий розлад у роботі багатьох органів влади, державних підприємств, установ, банків, ЗМІ тощо (квітень–червень 2017 р.) [8–10].

Протидія такому багатоаспектному інформаційному втручанню вимагає широкого комплексу політичних, технічних, економічних і правових заходів, покликаних забезпечити «чистоту» інформаційного простору, стійкість інформаційно-комунікаційних мереж, конфіденційність закритої

інформації, захищеність електронних ресурсів і безпеку програмного забезпечення в державному й приватному секторі. Максимально ефективна підготовка та реалізація таких заходів можлива лише у межах державної стратегії, яка б чітко визначила пріоритети державної політики кібербезпеки, окреслила коло її суб'єктів, узгодила діяльність щодо її забезпечення на всіх організаційних і територіальних рівнях.

Для сучасної України важливим кроком у цьому напрямі стало затвердження Стратегії кібербезпеки від 15 березня 2016 р. Поряд із визначенням ключових загроз у кібернетичній сфері цей документ заклав підвалини функціонування Національної системи кібербезпеки, інституційну основу якої становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, а також розвідувальні органи. Відповідно до профілю своєї діяльності кожен суб'єкт цієї системи наділений специфічним колом завдань і повноважень, підпорядкованих загальним стратегічним цілям, в яких проголошуються: захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі; забезпечення ефективної боротьби з кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом і кіберзлочинністю; забезпечення кіберзахисту державних електронних інформаційних ресурсів, критичної інформаційної інфраструктури тощо [11].

Уже перші роки реалізації Стратегії засвідчили помітний прогрес у розвитку організаційного та правового забезпечення кібербезпеки. Протягом 2017 р. в межах Стратегії здійснено низку важливих заходів, спрямованих на інтеграцію інформаційно-телекомунікаційних систем органів державної влади, створення захищених дата-центрів у сфері публічного адміністрування та провідних галузях економіки, моніторингу терористичних загроз на об'єктах критичної інфраструктури, налагодження державно-приватної взаємодії у сфері кібербезпеки, розробку стандартного протоколу дій під час кібератак, імплементацію міжнародних стандартів у сфері інформаційної безпеки та кіберзахисту, утворення центру реагування на інциденти кібербезпеки в банківській системі та платіжному просторі.

На тлі позитивних зрушень дедалі чіткіше окреслилася проблема відсутності єдиного законодавчого акту з питань кібербезпеки. До сьогодні в Україні правове регулювання відповідної сфери суспільних відносин здійснюється тільки на підзаконному рівні. За відсутності базисного закону, що закладає підвалини державної політики в кіберпросторі, підзаконне регулювання в цій сфері до певної міри характеризується фрагментарністю та недостатньою узгодженістю. Концептуально невизначеними лишаються форми й методи забезпечення кібербезпеки, права та обов'язки уповноважених суб'єктів державної влади, межі їх відповідальності, механізми координації, а також багато інших аспектів формування та реалізації державної політики кібербезпеки. Майже

в зародковому стані перебуває спеціальний понятійний апарат. Попри широке використання таких термінів, як «кібербезпека», «кіберзагроза», «кібератака», «кіберзахист», «кіберзлочин», «кібертероризм» тощо, українське законодавство не дає їх чіткого тлумачення.

Цілком очевидним є те, що одним із важливих напрямів розвитку інформаційного законодавства в умовах гібридної війни й обумовлених нею кіберзагроз обов'язково має стати невідкладне прийняття спеціального закону, який би визначив фундаментальні засади кібербезпеки та сформував надійне підґрунтя для правотворчої діяльності в цій сфері.

Аналізуючи тенденції розвитку національного інформаційного права в умовах гібридної війни, неможливо обійти увагою проблему регулювання діяльності інформаційних ресурсів, належних до медіапростору країни-противника.

Як уже зазначалося, засоби масової інформації та соціальні мережі є чи не найфективнішою зброєю, яка використовується в сучасних гібридних війнах [12, с. 69]. Починаючи з перших інтернет-війн (події в Косово 1999 р., «Друга Ліванська війна» 2007 р., «Арабська весна» 2010 р.) та закінчуючи останніми подіями в Україні та Сирії, соціальні медіа використовуються для формування громадської думки, мобілізації прихильників, координації військової діяльності та збирання потрібної інформації [13–14].

Фахівці виділяють щонайменше шість способів використання масмедіа для цілей гібридної війни: збір розвідувальних даних, дискредитація, психологічний вплив, кібероперації, інформаційний захист, управління та контроль [15]. У своєму поєднанні ці способи чинять всеохоплюючий тиск на суспільство та підривають обороноздатність країни. За відсутності дієвої протидії підривна діяльність «недружніх» медіа може мати воістину катастрофічні наслідки, тому існує об'єктивна потреба в застосуванні щодо них різноманітних, зокрема правових обмежень, спрямованих на мінімізацію їх деструктивного впливу.

Однак у цієї проблеми є й інший бік. Як показує історія українсько-російського протистояння, не всі інформаційні ресурси, зареєстровані на території країни-агресора, використовуються як інструмент гібридної війни. Певна їх частина (зазвичай, це ЗМІ, що перебувають в опозиції до офіційного курсу влади) орієнтується на західні стандарти роботи мас-медіа, сповідуючи принципи об'єктивності, неупередженості та прозорості в своїй роботі. Вони – єдиний «інформаційний струмочок», який пробивається крізь нашарування офіційної пропаганди та подає населенню країни-агресора неспотворену інформацію про події, пов'язані з перебігом гібридної війни, а також про їх оцінку з боку світової громадськості. Обмеження діяльності таких ресурсів не тільки політично недоцільне, а й юридично необґрунтоване як таке, що порушує свободу слова та право на інформацію.

Зважаючи на це, державна політика в галузі інформаційного права має орієнтуватися не на загальне обмеження діяльності інформаційних ресурсів країни-противника, а на вибіркове застосування обмежень щодо конкретних мас-медіа, які зарекомендували себе недружніми, заангажованими та маніпулятивними. Такий підхід вимагає максимальної правової визначеності обмежувальних критеріїв, оскільки за їх відсутності існує ризик потрапляння під заборону незаангажованих і політично нейтральних мас-медіа (наприклад, у разі нецілеспрямованого поширення недостовірної інформації). Водночас, для згортання діяльності тих інформаційних ресурсів, які справді є «рупором» ворожої пропаганди, держава змушена вдаватись до опосередкованих (найчастіше – адміністративних) засобів тиску, зокрема, на резидентів – суб'єктів надання телекомунікаційних послуг. За цих обставин держава часто балансує на межі правового поля (а інколи її перетинає), що неможливо визнати прийнятною моделлю публічного адміністрування.

Саме такий стан справ спостерігався в Україні до прийняття низки законів щодо критеріїв визначення інформаційної продукції, яка шкодить національній безпеці України. До таких критеріїв (і водночас підстав відповідальності ЗМІ) віднесено популяризацію або пропаганду держави-агресора, її органів влади, представників таких органів, а також їхніх дій, що створюють позитивний образ держави-агресора, виправдовують чи визнають правомірною окупацію території України тощо [16–17].

Варто визнати, що й після цих кроків українського законодавця питання про «зіткнення» інтересів національної безпеки та гарантій демократичних свобод (зокрема – свободи інформаційної діяльності) не було зняте з порядку денного [18, с. 6]. І навіть більше: воно актуалізувалося в 2017 р. з прийняттям Указу Президента України від 15.05.2017 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)», яким запроваджено блокування низки російських інтернет-сервісів («Лабораторія Касперського», «Доктор Веб», «Яндекс», «МайлРу», «ВКонтакті»), спровокувавши гостру полеміку всередині країни і в міжнародних колах [19].

За твердженням прихильників запроваджених санкцій, перераховані інтернет-сервіси займають домінуюче становище в стратегічно важливих сегментах українського ринку інформаційних послуг та одночасно перебувають під щільним контролем спецслужб країни-агресора, що зумовлює загрозу їх використання для дестабілізації політичної, соціальної та економічної ситуації, збору конфіденційних даних, підриву окремих галузей економіки, нечесної конкуренції та витіснення з ринку національних інтернет-компаній. На міжнародному рівні блокування російських веб-сайтів підтримав Генеральний секретар

НАТО Йенс Столтенберг (*Jens Stoltenberg*), висловивши переконання в тому, що їх заборона в Україні «… є питанням безпеки, а не свободи слова» [20].

Водночас лунають численні голоси «проти». Широке коло громадських діячів та організацій наголошують, що встановлені заборони позбавлені фактичних підстав (по суті, вони спрямовані на ліквідацію суто гіпотетичних загроз), не мають правового обґрунтування, суперечать Конституції, утискають демократичні права і свободи. Наприклад, Голова Комітету Верховної Ради України Вікторія Сюмар зазначила, що рішення про блокування російських соціальних мереж перебуває поза правовим полем, а міжнародна організація «Репортери без кордонів» (*Reporters Without Borders*) розцінює такий крок як «несиметричний захід, який суттєво звужує право на інформацію та свободу думки [21–22]».

Не приміряючи на себе роль арбітра в питанні про те, де закінчується свобода слова і починаються інтереси державної безпеки, можна сміливо стверджувати, що навіть у разі превалювання останніх будь-які обмеження в інтернет-середовищі мають носити точковий характер і стосуватися лише тих ресурсів, які скомпрометували себе конкретними діями або ж є джерелом очевидних загроз для держави і суспільства. Видається необґрунтованим і неправомірним застосування санкцій за принципом юридичної належності, коли блокуванню піддаються всі без винятку інформаційні сервіси, належні до певної юридичної особи, безвідносно до характеру їх діяльності, контенту або тематичного спрямування. У цьому розумінні український досвід є вельми повчальним. З-понад сотні (105) інтернет-ресурсів, заблокованих відповідно до Указу Президента України від 15.05.2017 № 133/2017 «Про … застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», понад чверть – мають довідниковий, розважальний або побутовий характер і сумнівно, що можуть бути дієвою зброєю інформаційної війни (такі сайти: «*www.kinopoisk.ru*», «*www.auto.ru*», «*www.translate.yandex.ua*» та ін.). Їх заборону важко виправдати міркуваннями безпеки і тим паче – визнати допустимим обмеженням права інформаційної діяльності.

Висновки. В умовах гібридної війни держава, що стала об’єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватись істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки та ідеями верховенства права – це стратегічно важливе завдання держави, вирішити яке можна тільки за умови чіткого визначення принципів, критеріїв і механізмів правових обмежень в інформаційній сфері. Вихідні засади цих обмежень мають знайти відображення як у фундаментальних актах інформаційного законодавства (насамперед, у Законі України «Про інформацію»),

так і в законодавстві щодо національної безпеки (Закон України «Про основи національної безпеки», Закон України «Про правовий режим надзвичайного стану», Закон України «Про правовий режим воєнного стану» тощо). Лише так інформаційна політика держави набуде аксіологічної цілісності, і лише так вона зможе стояти на варті демократичних цінностей, одночасно їм не зраджуючи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Калюжний Р. А., Копан О. В., Марценюк О. Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію. Київ : МП «Леся», 2013. 236 с.
2. Gurzhii A. V. Topical issues of personal data protection in Ukraine. European Reforms Bulletin. 2016. № 2. P. 15–17.
3. Gurzhii A. The system of public administration in the field of personal data protection. Development of National Law in the Context of Integration Into the European Legal Space. Warsaw : BMTEridiaSp. z o. o. Wydawnictwo Erida, 2018. P. 203–214.
4. Gurzhii A. Topical issues of personal data protection in Ukraine. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали наук.-практ. конф. (6 жовт. 2016 р.). Київ : НТУУ «КПІ імені Ігоря Сікорського», Політехніка, 2016. С. 196–201.
5. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.
6. Сопілко І. М. Державна інформаційна політика України: стан та шляхи реалізації. Київ : МП «Леся», 2014. 424 с.
7. Dolmatova M. Russian mass media: falling incomes of Russians and paradoxical optimism. BBC Russian Service (January 2017). URL : http://www.bbc.com/russian/features-38566253.
8. Sanger D. Putin Ordered «Influence Campaign» Aimed at U.S. Election, Report Says. The New York Times (January 2017). URL : https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.
9. Huggler J. Germany accuses Russia of cyberattack on Ukraine peace monitors, as Kremlin dismisses US intelligence claims as a «witchhunt». The Telegraph (January 2017). URL : http://www.telegraph.co.uk/news/2017/01/09/germany-accuses-russia-cyber-attack-ukraine-peace-monitors-kremlin.
10. Dearden L. Ukraine cyberattack: Chaos as national bank, state power provider and airport hit by hackers. The Independent (June 2017). URL : http://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html.
11. Про рішення Ради національної безпеки і оборони України від 27.01.2016 «Про стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. Офіц. вісн. Президента України. 2016. № 23. Ст. 899.
12. Deshko L. M. European Standards of Human Rights: Course book. Donetsk : Modern Printing (Suchasny Drook), 2013. 142 p.
13. Svetoka S. Social media as a tool of hybrid warfare. Riga: NATO Strategic Communications Centre of Excellence, 2016. 49 p.
14. Deshko L. Contemporary humanitarian law and Ukranian legislation on internally displaced persons. Міжнародне право: виклики сьогодення : матеріали Міжнар. наук.-практ. інтернет-конф. (20 груд. 2016 р.). Київ : Київ. нац. торг.-екон. ун-т, 2017. С. 89–90.
15. Nissen T. The Weaponization of Social Media. Copenhagen: Royal Danish Defense College, 2015. 150 p.

16. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України : Закон України від 05.02.2015 № 159-VIII. Офіц. вісн. України. 2015. № 27. Ст. 776.
17. Про внесення змін до деяких законів України щодо обмеження доступу на український ринок іноземної друкованої продукції антиукраїнського змісту : Закон України від 08.12.2016 № 1780-VIII. Офіц. вісн. України. 2017. № 4. Ст. 102.
18. Дешко Л. М. Конституційне право на звернення до міжнародних судових установ та міжнародних організацій. Ужгород : Гельветика, 2016. 486 с.
19. Про рішення Ради національної безпеки і оборони України від 28.04.2017 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : Указ Президента України від 15.05.2017 № 133/2017. Офіц. вісн. України. 2017. № 41. Ст. 1276.
20. Press conference by NATO Secretary General Jens Stoltenberg ahead of the Meeting of NATO Heads of State and Government. NATO (May 2017). URL : http://www.nato.int/cps/en/natohq/opinions_144081.htm?selectedLocale=en.
21. Рішення про блокування «ВКонтакте» та «Одноклассников» – поза правовим полем. Інтерв'ю з Головою Комітету Верховної Ради України з питань свободи слова та інформаційної політики Вікторією Сюмар. URL : http://zik.ua/tv/video/83547.
22. RS Furges Ukraine to scrap banon Russian social mediasites. Reporters Without Borders (May 2017). URL : https://rsf.org/en/news/rsf-urges-ukraine-scrap-ban-russian-social-media-sites.

Стаття надійшла до редакції 04.06.2018.

Gurzhiy T. Information Law: the Challenges of the Hybrid Warfare.

Background. *An important role in informational confrontation to hybrid aggression is given to information law, which is intended to guarantee freedom of thought and ensure reliable protection of society and state from multidimensional information threats. In modern conditions, when the main vector of foreign-political struggle has finally shifted to the sphere of information, information law became a necessary tool for ensuring national security, including ensuring by the way of establishing information restrictions. At the same time, it remains the basic indicator of the level of democracy, which forces to consider its development through the prism of coordination of national interests and civil liberties. Against this backdrop, national security and the idea of the rule of law in the regulation of information relations become particularly acute.*

Analysis of recent researches and publications. *The issues of information law have been highlighted in the scientific works of many modern lawyers due to its extreme urgency. It has to be noted that most of the modern research on information law issues are carried out in the context of a stable (peaceful) foreign policy situation that is not typical for modern Ukraine.*

The ***aim*** *of the article is to outline trends, patterns and prospects of national information law development in the context of hybrid warfare.*

Materials and methods. *The set goal has resulted in the comprehensive use of general scientific and special legal methods of cognition, which allowed covering the key aspects of information law as a component of the information security system and the tool for the provision of information rights and freedoms. The laws of Ukraine, the decrees of the President of Ukraine, the works of domestic and foreign scientists were the information basis of the study.*

Results. *The article is devoted to the consideration of the current state and prospects of national information law development in the context of hybrid warfare, which causes the rapid emergence and change of the entire layers of public relations associated with*

the country's participation in information confrontation, the organization of security measures, the introduction of sanction regimes. The range of information threats of the hybrid war is outlined; their influence on the sphere of national security is analyzed. A set of measures aimed at improving the quality of legal information security is proposed.

Conclusion. *The most effective preparation and realization of such measures is possible only within the framework of the state strategy, which would clearly define the priorities of the state information policy, outline the range of its subjects, and coordinate its activities at all organizational and territorial levels. Proceeding from the dualistic nature of information law, as an instrument of information restrictions and guarantees of information rights and freedoms, it is argued that the concept of its development in terms of hybrid warfare should include a mandatory search of a balance between the interests of national security and the ideas of the rule of law.*

Keywords: hybrid warfare, national security, information security, information warfare, cyber security, information law, freedom of thought, right to information.

REFERENCES

1. Kaljuzhnyj R. A., Kopan O. V., Marcenjuk O. G. Teoretyko-metodologichni zasady informacijnogo prava Ukrai'ny: realizacija prava na informaciju. Kyi'v : MP «Lesja», 2013. 236 s.
2. Gurzhii A. V. Topical issues of personal data protection in Ukraine. European Reforms Bulletin. 2016. № 2. P. 15–17.
3. Gurzhii A. The system of public administration in the field of personal data protection. Development of National Law in the Context of Integration Into the European Legal Space. Warsaw : BMTEridiaSp. z o. o. Wydawnictwo Erida, 2018. P. 203–214.
4. Gurzhii A. Topical issues of personal data protection in Ukraine. Zapobigannja novym vyklykam ta zagrozam informacijnij bezpeci Ukrai'ny: pravovi aspekty : materialy nauk.-prakt. konf. (6 zhovt. 2016 r.). Kyi'v : NTUU «KPI imeni Igorja Sikors'kogo», Politehnika, 2016. S. 196–201.
5. Nashynec'-Naumova A. Ju. Informacijna bezpeka: pytannja pravovogo reguljuvannja : monografija. Kyi'v : Gel'vetyka, 2017. 168 s.
6. Sopilko I. M. Derzhavna informacijna polityka Ukrai'ny: stan ta shljahy realizacii'. Kyi'v : MP «Lesja», 2014. 424 s.
7. Dolmatova M. Russian mass media: falling incomes of Russians and paradoxical optimism. BBC Russian Service (January 2017). URL : http://www.bbc.com/russian/features-38566253.
8. Sanger D. Putin Ordered «Influence Campaign» Aimed at U.S. Election, Report Says. The New York Times (January 2017). URL : https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.
9. Huggler J. Germany accuses Russia of cyberattack on Ukraine peace monitors, as Kremlin dismisses US intelligence claims as a «witchhunt». The Telegraph (January 2017). URL : http://www.telegraph.co.uk/news/2017/01/09/germany-accuses-russia-cyber-attack-ukraine-peace-monitors-kremlin.
10. Dearden L. Ukraine cyberattack: Chaos as national bank, state power provider and airport hit by hackers. The Independent (June 2017). URL : http://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html.
11. Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 27.01.2016 «Pro strategiju kiberbezpeky Ukrai'ny» : Ukaz Prezydenta Ukrai'ny vid 15.03.2016 № 96/2016. Ofic. visn. Prezydenta Ukrai'ny. 2016. № 23. St. 899.

12. Deshko L. M. European Standards of Human Rights: Course book. Donetsk : Modern Printing (Suchasny Drook), 2013. 142 p.
13. Svetoka S. Social media as a tool of hybrid warfare. Riga: NATO Strategic Communications Centre of Excellence, 2016. 49 p.
14. Deshko L. Contemporary humanitarian law and Ukranian legislation on internally displaced persons. Mizhnarodne pravo: vyklyky s'ogodennja : materialy Mizhnar. nauk.-prakt. internet-konf. (20 grud. 2016 r.). Kyi'v : Kyi'v. nac. torg.-ekon. un-t, 2017. S. 89–90.
15. Nissen T. The Weaponization of Social Media. Copenhagen: Royal Danish Defense College, 2015. 150 p.
16. Pro vnesennja zmin do dejakyh zakoniv Ukrai'ny shhodo zahystu informacijnogo teleradioprostoru Ukrai'ny : Zakon Ukrai'ny vid 05.02.2015 № 159-VIII. Ofic. visn. Ukrai'ny. 2015. № 27. St. 776.
17. Pro vnesennja zmin do dejakyh zakoniv Ukrai'ny shhodo obmezhennja dostupu na ukrai'ns'kyj rynok inozemnoi' drukovanoi' produkcii' antyukrai'ns'kogo zmistu : Zakon Ukrai'ny vid 08.12.2016 № 1780-VIII. Ofic. visn. Ukrai'ny. 2017. № 4. St. 102.
18. Deshko L. M. Konstytucijne pravo na zvernennja do mizhnarodnyh sudovyh ustanov ta mizhnarodnyh organizacij. Uzhgorod : Gel'vetyka, 2016. 486 s.
19. Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 28.04.2017 «Pro zastosuvannja personal'nyh special'nyh ekonomichnyh ta inshyh obmezhuval'nyh zahodiv (sankcij)» : Ukaz Prezydenta Ukrai'ny vid 15.05.2017 № 133/2017. Ofic. visn. Ukrai'ny. 2017. № 41. St. 1276.
20. Press conference by NATO Secretary General Jens Stoltenberg ahead of the Meeting of NATO Heads of State and Government. NATO (May 2017). URL : http://www.nato.int/cps/en/natohq/opinions_144081.htm?selectedLocale=en.
21. Rishennja pro blokuvannja «VKontakte» ta «Odnoklasnykiv» – poza pravovym polem. Interv'ju z Golovoju Komitetu Verhovnoi' Rady Ukrai'ny z pytan' svobody slova ta informacijnoi' polityky Viktorijeju Sjumar. URL : http://zik.ua/tv/video/83547.
22. RS Furges Ukraine to scrap banon Russian social mediasites. Reporters Without Borders (May 2017). URL : https://rsf.org/en/news/rsf-urges-ukraine-scrap-ban-russian-social-media-sites.