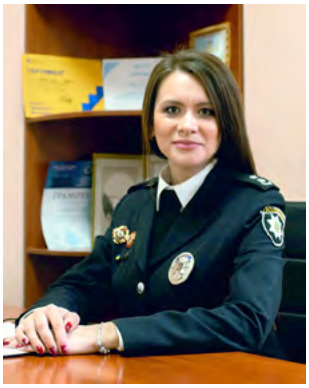
ПІДГОТОВКА ФАХІВЦІВ СИСТЕМИ ПРОФЕСІЙНОЇ ЮРИДИЧНОЇ ОСВІТИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

УДК 342.7:347.121.2:004
DOI 10.32782/2523-4269-2023-83-61-66

Сопілко Ірина Миколаївна,
доктор юридичних наук, професор
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-9594-9280



Мердова Ольга Миколаївна,
кандидат юридичних наук, доцент, підполковник поліції
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0003-0769-2364

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ НА ТЛІ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ: ПРАВОВИЙ АСПЕКТ

Актуальність дослідження визначається та підтверджується роллю інформаційної безпеки держави, достатній рівень якої є «щитом» проти агресивних і зловмисних дій ворога щодо розповсюдження фейкових новин, дезінформації, ворожої пропаганди задля сіяння страху, занепокоєння серед українського населення з метою досягнення реваншистських намірів. У статті розкрито сутність та особливості поняття «інформаційна безпека» та пов'язаних із ним термінів, проаналізовано наявні нормативно-правові інструменти забезпечення належного рівня інформаційної безпеки як невіддільного елементу національної безпеки, проведено їх критичну оцінку та надано рекомендації щодо подолання відповідних прогалин у правовому регулюванні й політиці держави. Авторами вказано на відсутність чітко визначених методів і теоретичних праць у сфері забезпечення інформаційної безпеки України як невіддільного структурного елементу безпеки національної, що є реальною перепоною для реалізації нею такого обов'язку. На думку авторів, нині актуалізуються питання необхідності створення і реалізації чіткої та дієвої державної політики в інформаційно-безпековому полі з метою розбудови ефективної системи протидії інформаційним порушенням із боку країни-агресора. У процесі дослідження використано загальновизнані методи наукового пізнання, а саме аналітичний, формальний, порівняльно-правовий, системно-структурний та інші.

Ключові слова: *повномасштабне вторгнення, інформаційна безпека, національна безпека, кібербезпека, державна інформаційна політика.*

Постановка проблеми. Мабуть, кожному з нас відомий вислів про те, що той, хто володіє інформацією, володіє світом. Він повною мірою актуальний і нині, коли наше суспільство за період незалежності держави пройшло всеосяжну трансформацію і стало так званим інформаційним суспільством. Так, ми продукуємо контент, ми усіляко використовуємо та накопичуємо дані, обробляємо інформацію для того, щоб далі перетворити її на якісно новий продукт (актив) – знання. Саме актив або відомості та знання за правильного підходу можуть перетворюватися на важливий ресурс, необхідний для розвитку державної економіки.

Як відомо, ще з 2014 року російська федерація веде проти незалежної суверенної держави Україна гібридну війну. П. Мартон так охарактеризував цей феномен: це така форма ворожих дій, за якої завойовник-агресор не вдається до класичного військового вторгнення, а усілякими засобами намагається пригнітити, послабити свого опонента-жертву, для чого застосовує секретні операції, кібервійну, підтримує повстанців. Що ж стосується безпосереднього застосування зброї та ведення воєнних дій у традиційному розумінні, то такого може не бути взагалі, а тому формально гібридна війна може мати місце і в офіційному стані миру [1, с. 32].

Але 24 лютого 2022 року агресивно налаштована держава росія почала повномасштабне вторгнення в Україну, застосувавши вже саме воєнні методи, не гребуючи і методами інформаційної війни, кібервійни, психологічного тиску тощо. Саме тому інформаційна безпека нашої держави постійно зазнає серйозних загроз: ворожа пропаганда, засилля фейків, злонамірні ігри зі свідомістю інформаційних суб'єктів – це лише мала частка того, як діє ворог для досягнення своїх злочинних намірів.

Зазначимо, що інформаційна війна є сукупністю методів і засобів подачі інформації для формування необхідної організаторам інформаційної пропаганди точки зору та відповідної громадської думки у певної групи людей. Через вказане у жертв формується необхідний маніпулятору світогляд з певного питання, щодо якого раніше виникали суперечності, а за відсутності таких – сумніви та інші домисли щодо наявних переконань [2, с. 337]. І сьогодні росія, головний ворог не тільки України, але й усього світу, активно використовує інформаційну зброю нарівні з конвенційною. Шляхом відповідних засобів і методів вона веде терористичну діяльність, насаджує свої реваншистські ідеї, вдається до усіляких порушень прав людини та правових засад існування цивілізованого світу загалом. Така злочинна поведінка спрямована на досягнення узурпаторських цілей шляхом сіяння розбрату в суспільстві країни-жертви (нині це Україна, до неї – Грузія, Сирія, Молдова та інші), плекання у ньому внутрішніх суперечностей (задля створення благодатного ґрунту з метою досягнення агресивних політичних цілей). Окремо зазначимо на важливості перемоги саме в інформаційному полі, точніше в інформаційно-психологічній війні, котру ворог веде досить жваво, не нехтуючи будь-якими засобами. Як зазначають О. Заячківська та інші, наука та мистецтво є одними з найголовніших інструментів у боротьбі України за свою незалежність, і саме вони є надчуттєвими маркерами подій у реальному часі як у нашій країні, так і по всьому світу [3, с. 14].

Саме тому важливо не дати ворогові досягти вказаного, треба усіма доступними засобами й методами підтримувати інформаційну безпеку країни на належному рівні. Це можливо саме завдяки дієвим правовим механізмам і якісному нормативно-правовому регулюванню у сфері забезпечення інформаційної безпеки країни, виробленню рекомендацій щодо покращення ситуації, про що і йтиметься у нашій науковій праці.

Аналіз останніх досліджень і публікацій. Проблематика вивчення правових засад забезпечення інформаційної безпеки є основою наукових пошуків таких учених, як Л. Бєлкін, І. Залєвська, В. Кравченко [15], І. Котерлін [9], А. Свінсицький та І. Сопілко [2], Р. Черниш [11], Ю. Юринець, В. Філінович та інших, проте дослідження в аспекті впливу війни на інформаційну безпеку не здійснювалися.

Мета статті. Автори ставлять собі за мету розкрити сутність та особливості поняття «інформаційна безпека» та інших, пов'язаних із ним термінів, проаналізувати наявні нормативно-правові засоби забезпечення належного рівня інформаційної безпеки як невіддільного елементу національної безпеки, надати їх критичну оцінку, а також рекомендації щодо подолання відповідних прогалин як у правовому регулюванні, так і в інформаційній політиці держави.

Виклад основного матеріалу. Задля кращого розуміння проблематики насамперед необхідно осягнути значення основних понять і категорій цієї сфери взаємодії. Першим із них розглянемо концепт інформаційної безпеки.

Інформаційна безпека (далі – ІБ), як вказує А.Т. Тунггал, опікується питанням захисту інформації (даних, відомостей) від несанкціонованого доступу. Вона є важливим елементом управління інформаційними ризиками та спрямована на запобігання неавторизованому доступу, а також на недопущення застосування, знищення, розголошення, модифікації даних. Якщо зарадити цьому не вдалося, то спеціалісти з ІБ намагаються усіма доступними засобами зменшити рівень негативного впливу відповідного інциденту. Всі програми та політики ІБ базуються на трьох принципах: захисту цілісності, доступності та конфіденційності інформації [4]. Це визначення дає чітке розуміння завдань і методів функціонування ІБ як системного утворення.

Є й інший підхід до визначення терміна. Так, до Верховної Ради України (далі – ВРУ) було внесено законопроєкт № 4949 від 28 травня 2014 року «Про засади інформаційної безпеки України», який під зазначеним терміном розуміє «стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якого запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» [5].

Визначення й основні засади ІБ містяться і в інших нормативно-правових актах. Розглянемо їх більш детально.

25 лютого 2017 року указом Президента України № 47/2017 було введено в дію рішення Ради національної безпеки і оборони України (далі – РНБО) «Про Доктрину інформаційної безпеки України». У п. 1 та 2 вказано на те, що Росія веде гібридну війну проти України, для чого застосовує передові інформаційні технології впливу на свідомість українців задля розпалювання ворожнечі, пропагування агресивної війни тощо. Доктрина визначила національні інформаційні інтереси нашої держави, загрози, які постають перед їх втіленням у життя, а також пріоритетні напрями державної інформаційної політики. Принципи, що є основою Доктрини: повага до гідності, додержання прав і свобод людини, захист законних інтересів її, а також суспільства та держави загалом і, звісно, забезпечення державного суверенітету та територіальної цілісності.

Національні інтереси країни в інформаційній сфері зазначено у п. 3 названого нормативно-правового акта, серед яких життєво важливі інтереси особи, суспільства та держави, у тому числі захист українців від агресивного впливу російської деструктивної пропаганди; розвиток національної інформаційної інфраструктури та безпосередньо інформаційного суспільства, а також

системи стратегічних комунікацій тощо. У свою чергу, п. 4 присвячений загрозам національним інтересам і загалом безпеці держави в інформаційному полі, серед яких: ведення ворогом спеціальних інформаційних операцій серед інших міжнародних суб'єктів задля створення у їхній уяві негативного образу України; ворожа інформаційна експансія й інформаційне домінування; пропаганда ізоляціоністських ідей тощо; п. 5 визначав пріоритети державної політики в інформаційній сфері, як от розробка інтегрованої системи оцінювання інформаційних загроз задля швидкого їх виявлення і реагування на них; розвиток технологічної інфраструктури забезпечення ІБ у країні; розвиток цифрового мовлення та механізмів взаємодії держави з іншими суб'єктами задля протидії ворожій інформаційній активності тощо [6].

Вищезазначена Доктрина втратила чинність на підставі того, що 28 грудня 2021 року В. Зеленський своїм Указом № 685/2021 ввів у дію рішення РНБО від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», яка визначила наявні та можливі загрози й виклики національній безпеці нашої держави в інформаційному полі, а також відповідні цілі та завдання, котрі допоможуть захистити права кожного на інформацію та захист персональних даних, досягти яких вбачається можливим через вчинення відповідних дій щодо стримування та протидії загрозам ІБ нашої країни, а також шляхом нейтралізації інформаційної агресії, що має за мету підрив державного суверенітету, територіальної цілісності держави. Крім того, задля вказаного мають застосовуватися методи щодо забезпечення інформаційної стійкості українського суспільства, має бути створена дієва система взаємодії між органами державної влади та місцевого самоврядування й українцями. Не забули нормотворці і про важливість розвитку міжнародної співпраці у відповідній сфері за принципами взаємопідтримки та партнерства. Реалізація цілей і завдань стратегії вбачається можливою у період до 2025 року.

Саме забезпечення ІБ визнане цією Стратегією як одна із найважливіших функцій держави, яка є елементом нацбезпеки України, відповідний стан захищеності її суверенітету та територіальної цілісності, демократичних засад та інших життєво важливих інтересів трьох головних інформаційних суб'єктів – самої держави, її громадян і безпосередньо суспільства. Саме за вказаного стану, відповідно до термінології Стратегії, якісно забезпечуються конституційні права та свободи кожного на розповсюдження, збір, застосування, зберігання даних, а разом із ними – і доступ до достовірних та об'єктивних відомостей. Також функціонує ефективна система захисту та протидії усілякій шкоді, що може бути завдана через розповсюдження негативного інформаційного впливу [7].

У процесі дослідження змісту Стратегії одразу стає зрозумілим бажання влади посилити відповідальність за поширення дезінформації. До 24 лютого 2022 року зазначені положення викликали занепокоєння у поборників цифрових прав, котрі вважали за необхідне не надавати державовладцям широких повноважень щодо оцінки правдивості даних і поновлення кримінальної відповідальності за дифамацію та вимагати від них врахування принципу пропорційності в аспекті суспільної небезпеки відповідних діянь. Вони пояснювали такі свої погляди вірогідною непропорційністю обмеження свободи вираження поглядів [8], але нині, з урахуванням ситуації, яка склалася у зв'язку із повномасштабним вторгненням і повсюдними спробами ворога усіляко дезінформувати наше населення й насадити йому свої агресивні ідеї, вважаємо суворість розробників Стратегії у вказаному аспекті такими, що є актуальними та необхідними.

І. Котерлін, досліджуючи вказану Стратегію та загалом стан ІБ в Україні, вказує на очевидність зміни акцентів щодо виявлення загроз і реакції на них у бік звуження прав людини та громадянина через необхідність реагування впливу на наявні та ймовірні загрози в умовах повномасштабного вторгнення. Дослідником зазначені чинні обмеження конституційних інформаційних прав, а саме: на таємницю листування (ст. 31); невтручання в особисте життя (ст. 3); свободу думки (ст. 34); володіння і розпорядження власністю (ст. 41). Він пояснює такі обмеження неможливістю забезпечення якісного захисту від свавілля ворога особам на території нашої держави [9, с. 153].

Тим не менш, невідповідність зазначених обмежень гарантіям прав людини у воєнний час одночасно дає можливість забезпечити основоположні права більшості шляхом забезпечення життєздатності самої української держави, однак, як вказано науковцем, воєнний стан не став «приводом для свавільного владного трактування прав та обов'язків суб'єктів із хаотичним встановленням обмежень і заборон», адже розробляються та приймаються відповідні зміни до чинних нормативно-правових актів із урахуванням реалій агресій ворога та ведення ним війни. Вони стосуються і деяких питань інформаційних правовідносин, наприклад, заборони розповсюдження певних відомостей із суспільно небезпечним характером; аспектів технічного фіксування контенту в умовах воєнного стану; процесуальних дій при вилученні даних тощо [9, с. 153].

Відзначимо, що у 2020 році Президент України В. Зеленський своїм Указом № 392/2020 від 14 вересня 2020 року ввів у дію Стратегію національної безпеки України. Пріоритетними для забезпечення національної безпеки цей нормативно-правовий акт визначає захист осіб, суспільства та загалом держави від правопорушень; забезпечення поновлення порушених прав; покращення спроможності нацсистеми кібернетичної безпеки (адже таке вбачається необхідним для ефективної протидії загрозам у тому безпековому середовищі, що склалося). Окремо зауважимо про такий важливий внутрішньополітичний напрямок, як забезпечення національних інтересів і безпеки, а разом із ним – і отримання повної, достовірної превентивної інформації щодо ситуації як у нашій державі, так і по всьому світу [10].

Як бачимо, Україна не зупиняється на шляху розвитку правового регулювання в інформаційній галузі, зокрема щодо інформаційної безпеки, але варто погодитися з думкою Р. Черниша, що чинна нормативно-правова база має відчутні недоліки, які ускладнюють якісні трансформації у цьому секторі суспільних відносин. Так, дослідники вказують на відсутність чітко визначених методів і теоретичних праць у сфері забезпечення інформаційної безпеки України, що значно перешкоджає якісній реалізації нею свого обов'язку із забезпечення ІБ як важливого структурного елементу безпеки національної, тому створення і реалізація чіткої та дієвої державної політики у цій сфері є єдиним засобом розбудови ефективної системи протидії інформаційним порушенням [11, с. 214].

Слід пам'ятати і про те, що інформаційна безпека – це важливий аспект безпеки не лише національної, а й міжнародної. Україні й іншим країнам слід усіляко розвивати міждержавне співробітництво у глобальному

інформаційному просторі задля своєчасного виявлення можливих загроз, їх обопільного подолання та превентизації. Саме всебічну кооперацію щодо інформаційних і кібернетичних питань науковці вбачають головним чинником подолання піднятих у дослідженні проблем.

Крім того, доцільно наголосити й на важливості співробітництва в інших правових напрямках, як от вкриття і покарання злочинців. Так, наприклад, зараз ідуть активні перемовини щодо створення спеціального міжнародного трибуналу для війни в Україні, можливого за спільних зусиль уряду України й ООН [12] або ж використання для цих цілей можливостей Міжнародного суду ООН [13, с. 431].

Окремо згадаємо про тезу науковців щодо важливої ролі науки та мистецтва у боротьбі з інформаційно-психологічними методиками ведення війни проти України російською федерацією. У цьому контексті важливим кроком у забезпеченні інформаційної та кібербезпеки держави є навчання населення основ кібергігієни й інформаційної гігієни. Не варто забувати і про роль освіти у вихованні та навчанні сучасної молоді. Як не дивно, два роки пандемії коронавірусу мали й позитивний результат – школярі, студенти, а з ними і науково-педагогічні працівники освоїли інструментарій і техніки онлайн-навчання. І саме це нині рятує Україну в освітньому полі, адже, незважаючи на воєнний стан, здобувачі освіти продовжують її отримувати. Як зазначають І. Костікова та інші, онлайн-викладання показало себе досить ефективним серед всіх студентів, адже у багатьох випадках такі заняття дуже подібні до традиційних очних пар. Також онлайн-навчання допомагає здобувачам освіти набувати навичок англійської мови. Окремо дослідники наголошують на можливості використовувати цифрові засоби, демонструвати відео й інші матеріали на екрані у кращій якості, аніж таке можливо було за традиційного очного навчання [14, с. 130].

На думку В. Кравченка, Україна також має проявити свою національну та політичну зрілість, і тоді її майбутнє буде значно перспективнішим за російське, адже саме наша держава набагато ближча за РФ до виходу «з порочного кола історії», де Україна довгий час була ізольована від зовнішнього світу. Незалежна наша держава бачить перед собою стимул – йти вперед на шляху національно-державного будівництва. Важливим є постійний і плідний діалог між політичними елітами та громадянським суспільством [15, с. 207].

Так, на жаль, війна все ще триває, але розумне поєднання нормативно-правових інструментів, державної інформаційної політики, навчання громадян основ інформаційної та кібернетичної грамотності, а також безпосередня освіта нашої молоді – це те, що допоможе забезпечити стійкий і надійний рівень інформаційної безпеки в Україні.

Висновки. Отже, сьогодні на тлі повномасштабного вторгнення російської федерації в Україну питання забезпечення інформаційної безпеки у державі є вкрай актуальним. Саме інформаційна безпека забезпечує захист доступності, конфіденційності, цілісності комп'ютерних систем та інформації як окремо взятого громадянина, так і суспільства загалом і держави від несанкціонованого доступу зловмисників.

Належний рівень такої безпеки – це справжній «щит» перед ворогом, котрий щоденно підступно вбиває українців, не нехтуючи застосуванням інформаційної зброї. Країна-агресор постійно розповсюджує фейкові новини, дезінформацію, ворожу пропаганду – все це (і навіть більше) необхідне їй для сіяння страху, занепокоєння серед нашого населення, насадження йому панічних і зневірених настроїв, для дестабілізації політичної та соціально-економічної ситуації у нашій незалежній суверенній державі.

Саме тому розроблення нових і вдосконалення наявних основ забезпечення інформаційної безпеки у країні є одним із найважливіших завдань владних структур, так само як і захист національного інформаційного простору загалом. Нині в Україні вже діють нові Стратегії національної, інформаційної та кібернетичної безпеки, але цього регулювання не достатньо з урахуванням постійного агресивного впливу росії в українському інформаційному полі. Серед основних недоліків Стратегії інформаційної безпеки слід назвати відсутність конкретних механізмів моніторингу ефективності впровадження її заходів, кількісно-якісних показників для вимірювання такого впровадження тощо.

Враховуючи європейський політичний вектор України, важливим є розвиток діалогу з Євросоюзом щодо забезпечення інформаційної безпеки. Також необхідно досконально проаналізувати практичний досвід країн ЄС, що вже сформували у себе організаційно-правову основу забезпечення інформаційної безпеки, а після такого – імплементувати їх позитивний досвід у національній законотворчій діяльності.

Список використаних джерел

1. Marton P. Evolution in military affairs in the battlespace of Syria and Iraq. *Corvinus Journal of International Affairs.* 2017. Vol. 2. № 2–3. P. 30–41. URL: https://doi.org/10.14267/cojourn.2017v2n2a3 (дата звернення: 05.05.2023).

2. Information wars as a threat to the information security of Ukraine / I. Sopilko et al. *Conflict Resolution Quarterly*. 2021. T. 39. № 3. P. 333–347. URL: https://doi.org/10.1002/crq.21331 (дата звернення: 05.05.2023).

3. Zayachkivska O., Smiechowska T., Souchelnytskyi S. The war and science in Ukraine: we can contribute to victory. *Proceedings of the Shevchenko Scientific Society. Medical Sciences.* 2022. T. 66. № 1. C. 14–21. URL: https://doi.org/10.25040/ntsh2022.01.02 (дата звернення: 05.05.2023).

4. Tunggal A. T. What is Information Security?. Third-Party Risk and Attack Surface Management Software – UpGuard. URL: https://www.upguard.com/blog/information-security (дата звернення: 05.05.2023).

5. Про засади інформаційної безпеки України : проєкт Закону України від 28 травня 2014 року № 4949. URL: https://ips.ligazakon.net/document/JG3TH00A (дата звернення: 05.05.2023)

6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 05.05.2023)

7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення 05.05.2023)

8. Стратегія інформаційної безпеки-2025 прийнято: що зміниться у сфері цифрових прав? / Лабораторія цифрової безпеки. URL: https://dslua.org/publications/stratehiiu-informatsiynoi-bezpeky-2025-pryyniato-shcho-zminytsia-u-sferi-tsyfrovykh-prav/ (дата звернення: 05.06.2023).

9. Котерлін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 1. С. 150–155. URL: http://apnl.dnu.in.ua/1_2022/25.pdf (дата звернення: 06.05.2023).

10. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 06.05.2023)

11. Черниш Р., Ігнатюк М. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти. *Юридичний науковий електронний журнал.* 2022. Т. 1. С. 213–216. URL: https://doi.org/10.32782/2524-0374/2022-1/54 (дата звернення: 06.05.2023).

12. Figura J. International criminal justice and the war in Ukraine. *Beyond the Horizon*. 2023. URL: https://behorizon.org/international-criminal-justice-and-the-war-in-ukraine/ (дата звернення: 06.05.2023).

13. Lanza G. The Fundamental Role of International (Criminal) Law in the War in Ukraine. *Orbis*. 2022. Т. 66. № 3. С. 424–435. URL: https://doi.org/10.1016/j.orbis.2022.05.010 (дата звернення: 06.05.2023).

14. Real Country Experiences: On-line Teaching in Wartime after Pandemic in Ukraine / I. Kostikova et al. *International Journal of Interactive Mobile Technologies (iJIM)*. 2023. Vol. 17. № 03. P. 123–134. URL: https://online-journals.org/index.php/i-jim/article/view/36419/12643 (дата звернення: 06.05.2023).

15. Kravchenko V. The Russian War against Ukraine: Cyclic History vs Fatal Geography. *East/West: Journal of Ukrainian Studies*. 2022. Т. 9. № 1. P. 201–208. URL: https://doi.org/10.21226/ewjus711 (дата звернення: 06.05.2023).

References

1. Marton, P. (2018). Evolution in military affairs in the battlespace of Syria and Iraq. Corvinus Journal of International Affairs. 2(2–3). 30–41. https://doi.org/10.14267/cojourn.2017v2n2a3 (data zvernennya: 05.05.2023) [in English].

2. Sopilko, I., Svintsytskyi, A., Krasovska, Y., Padalka, A., & Lyseiuk, A. (2021). Information wars as a threat to the information security of Ukraine. Conflict Resolution Quarterly. 39(3). 333–347. https://doi.org/10.1002/crq.21331(data zvernennya: 05.05.2023) [in English]

3. Zayachkivska, O., Smiechowska, T., & Souchelnytskyi, S. (2022). The war and science in Ukraine: we can contribute to victory. Proceedings of the Shevchenko Scientific Society. Medical Sciences. 66(1). https://doi.org/10.25040/ntsh2022.01.02 (data zvernennya: 05.05.2023) [in English]

4. Tunggal, A. T. (n.d.). What is Information Security? Third-Party Risk and Attack Surface Management Software – UpGuard. Retrieved from https://www.upguard.com/blog/information-security (data zvernennya: 05.05.2023) [in English].

5. Pro zasadi Informatsiynoyi bezpeki Ukrayini: proekt Zakonu Ukrayini vid 28 travnya 2014 roku №4949 [On the principles of information security of Ukraine: draft Law of Ukraine dated May 28, 2014 № 4949]. URL: https://ips.ligazakon.net/document/JG3TH00A (data zvernennya: 05.05.2023) [in Ukrainian].

6. Pro rishennya Radi natsionalnoyi bezpeki i oboroni Ukrayini vid 29 grudnya 2016 roku "Pro Doktrinu Informatsiynoyi bezpeki Ukrayini": Ukaz Prezidenta Ukrayini vid 25 lyutogo 2017 roku №47/2017 [On the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On the Information Security Doctrine of Ukraine": Decree of the President of Ukraine dated February 25, 2017 № 47/2017]. URL: https://www.president.gov.ua/documents/472017-21374 (data zvernennya: 05.05.2023) [in Ukrainian].

7. Pro rishennya Radi natsionalnoyi bezpeki i oboroni Ukrayini vid 15 zhovtnya 2021 roku "Pro Strategiyu Informatsiynoyi bezpeki": Ukaz Prezidenta Ukrayini vid 28 grudnya 2021 roku №685/2021 [On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On Information Security Strategy": Decree of the President of Ukraine dated December 28, 2021 № 685/2021]. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (data zvernennya: 05.05.2023) [in Ukrainian].

8. Strategiya Informatsiynoyi bezpeki-2025 priynyato: scho zminitsya u sferi tsifrovih prav? Laboratoriya tsifrovoyi bezpeki. [Information security strategy-2025 adopted: what will change in the field of digital rights? – Laboratory of digital security]. URL: https://dslua.org/publications/stratehiiu-informatsiynoi-bezpeky-2025-pryyniato-shcho-zminytsia-u-sferi-tsyfrovykh-prav (data zvernennya: 05.05.2023) [in Ukrainian].

9. Koterlin, I.B. (2022). Informatsiyna bezpeka v umovah voennogo stanu u aspekti zabezpechennya Informatsiynih prav ta svobod [Information security in the conditions of martial law in the aspect of ensuring informational rights and freedoms]. Aktualni problemi vitchiznyanoyi yurisprudentsiyi. № 1. S. 150–155. URL: http://apnl.dnu.in.ua/1_2022/25.pdf (data zvernennya: 06.05.2023) [in Ukrainian].

10. Pro rishennya Radi natsionalnoyi bezpeki i oboroni Ukrayini vid 14 veresnya 2020 roku "Pro Strategiyu natsionalnoyi bezpeki Ukrayini": Ukaz Prezidenta Ukrayini vid 14 veresnya 2020 roku № 392/2020 [On the decision of the National Security and Defense Council of Ukraine dated September 14, 2020 "On the National Security Strategy of Ukraine": Decree of the President of Ukraine dated September 14, 2020 № 392/2020]. URL: https://www.president.gov.ua/documents/3922020-35037 (data zvernennya: 06.05.2023) [in Ukrainian].

11. Chernish, R., Ignatyuk, M. (2022). Protidiya destruktivnomu Informatsiynomu vplivu v Ukrayini: pravovi ta organizatsiyni aspekti [Countering destructive information influence in Ukraine: legal and organizational aspects]. Yuridichniy naukoviy elektronniy zhurnal. T. 1. S. 213–216. URL: https://doi.org/10.32782/2524-0374/2022-1/54 (data zvernennya: 06.05.2023) [in Ukrainian].

12. Figura, J. (2023). International criminal justice and the war in Ukraine. *Beyond the Horizon*. Retrieved from https://behorizon.org/international-criminal-justice-and-the-war-in-ukraine/ (data zvernennya: 06.05.2023) [in English].

13. Lanza, G. (2022). The Fundamental Role of International (Criminal) Law in the War in Ukraine. *Orbis*, 66(3), 424–435. https://doi.org/10.1016/j.orbis.2022.05.010 (data zvernennya: 06.05.2023) [in English].

14. Kostikova, I., Holubnycha, L., Marmaza, O., Budianska, V., & Pochuieva, O. (2023). Real country experiences: On-line teaching in wartime after pandemic in ukraine. *International Journal of Interactive Mobile Technologies (iJIM)*, 17(03), 123–134. https://doi.org/10.3991/ijim.v17i03.36419 (data zvernennya: 06.05.2023) [in English].

15. Kravchenko, V. (2022). The Russian War against Ukraine: Cyclic History vs Fatal Geography. *East/West: Journal of Ukrainian Studies*, 9(1), 201–208. https://doi.org/10.21226/ewjus711 (data zvernennya: 06.05.2023) [in English].

Sopilko Irina,
Doctor of Legal Sciences, Professor
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-9594-9280

Merdova Olha,
PhD in Law, Associate Professor, Police lieutenant colonel
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0003-0769-2364

INFORMATION SECURITY OF UKRAINE IN THE CONTEXT OF A LARGE-SCALE INVASION: LEGAL ASPECT

The relevance of this scientific research is determined and confirmed by the role of the information security of the state, the sufficient level of which is a "shield" against the aggressive and malicious actions of the enemy regarding the spread of fake news, disinformation, enemy propaganda to sow fear and anxiety among the Ukrainian population in order to achieve revanchist intentions. The article reveals the essence and features of the concept of "information security" and related terms, analyzes the existing regulatory and legal instruments for ensuring the appropriate level of information security as an inseparable element of national security, conducts a critical assessment of them, and provides recommendations for overcoming relevant gaps in legal regulation and state policy. The authors pointed out the lack of clearly defined methods and theoretical works in the field of information security of Ukraine as an inseparable structural element of national security, which is a real obstacle to its implementation of such an obligation. According to the authors, the issue of the need to create and implement a clear and effective state policy in the information security field in order to build an effective system for countering information violations by the aggressor country is currently being updated. The importance of developing a dialogue with the European Union regarding ensuring information security, the need to analyze the practical experience of EU countries that have already formed an organizational and legal basis for ensuring information security, with its further implementation in national law-making activities is emphasized. In the process of research, the authors used generally recognized methods of scientific knowledge, namely analytical, formal, comparative-legal, systemic-structural and others.

Key words: *full-scale invasion, Information Security, National security, cybersecurity, State information policy.*

Надійшла до редколегії 20.05.2023