**НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ІНФОРМАТИКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ**

ВЕРГОЛЯС ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ

УДК 342+327/008:351

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Київ – 2020

Дисертацією є рукопис.

Роботу виконано в Науково-дослідному інституті інформатики і права Національної академії правових наук України.

Науковий керівник: доктор юридичних наук,
старший науковий співробітник
ЗОЛОТАР Ольга Олексіївна,
Науково-дослідний інститут інформатики і права Національної академії правових наук України, завідувач науково-дослідного сектору прав і безпеки людини в інформаційній сфері.

Офіційні опоненти: доктор юридичних наук, доцент
ТКАЧУК Тарас Юрійович,
Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України, заступник завідувача кафедри організації захисту інформації з обмеженим доступом;

кандидат юридичних наук,
старший науковий співробітник
ОНОПРІЄНКО Станіслав Григорович,
Військовий інститут Київського національного університету імені Тараса Шевченка, старший викладач кафедри правового забезпечення.

Захист дисертації відбудеться 25 лютого 2020 року о 10 годині на засіданні спеціалізованої вченої ради К 26.501.01 у Науково-дослідному інституті інформатики і права Національної академії правових наук України за адресою: 03039, м. Київ, вул. Фрометівська, 2.

З дисертацією можна ознайомитися у бібліотеці Науково-дослідного інституту інформатики і права Національної академії правових наук України за адресою: 01032, м. Київ, вул. Саксаганського, 110-В.

Автореферат розіслано 24 січня 2020 року.

В.о. вченого секретаря
спеціалізованої вченої ради **М.В. Беланюк**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. Розвиток сучасного суспільства як інформаційного зумовлює використання інформаційного простору як середовища політичних, економічних, військових та інших процесів. Фактично безмежний потенціал інформаційного простору використовується провідними світовими державами у військових конфліктах як з метою оптимізації функціональних спроможностей власних безпекових і оборонних структур, так і для створення нових засобів реалізації власних геополітичних інтересів, зокрема й інформаційної зброї. То ж дослідження загроз національній безпеці, виникнення яких пов'язане з розвитком інформаційного протиборства, а також механізмів протидії таким загрозам, наразі належить до найбільш актуальних предметів наукових пошуків в галузі інформаційного права. Спеціальні інформаційні операції (далі – СІО) посідають особливе місце в системі заходів протидії сучасним загрозам національній безпеці України – як самостійний механізм реалізації заходів інформаційно-психологічного спрямування і як допоміжне знаряддя в реалізації політичних, економічних, військових та інших заходів. Втім, незважаючи на виняткову актуальність проблематики СІО, а відтак – їх правового забезпечення, у цій сфері наразі існує значна кількість проблемних питань, основним з яких є відсутність достатнього законодавчого унормування проведення СІО. Відповідно, відсутнє й достатнє законодавче підґрунтя для розробки методологічних засад інформаційно-правового забезпечення СІО. Це передусім зумовлює потребу у законодавчому визначенні заборон при здійсненні інформаційного впливу, в тому числі в ході проведення СІО, які визначатимуть межі їх проведення, адже в Україні, як у демократичній правовій державі, діяльність державних органів влади, відповідальних за забезпечення національної безпеки має ґрунтуватися на нормах закону, які забезпечують реалізацію конституційних прав та свобод.

Серед науковців, що займалися дослідженням проблематики СІО з різних точок зору, можуть бути названі О. Баранов, І. Бачило, К. Бєляков, Н. Брусніцин, Т. Вронська, О. Довгань, О. Дзьобань, І. Доронін, В. Голубко, Г. Грачов, О. Золотар, М. Ємельянов, Є. Єрофєєв, О. Копан, В. Копилов, Д. Ланде, О. Литвиненко, В. Лопатін, А. Манойло, В. Мельник, І. Мірошник, С. Онопрієнко, І. Панарин, І. Панова, В. Панченко, В. Пилипчук, Г. Почепцов, Ю. Просвирнин, М. Рассолов, Н. Савінова, О. Стрельцов, Т. Ткачук, Ю. Уфімцев, А. Фатьянов, А. Явтушенко та інші. Проблематиці інформаційних війн, інформаційних операцій, інформаційних впливів тощо буди присвячені дисертаційні дослідження К. Будиліна, В. Гарєва, О. Горбєнка, О. Губарєва, О. Денщикова, Г. Крилова, О. Потьомкіна, Д. Фролова, Д. Щербини тощо. Втім зазначені дослідження стосуються радше філософських, технічних, військових, політологічних, соціологічних тощо, аніж правових аспектів забезпечення інформаційної безпеки. Натомість актуальні підходи до визначення сутності і особливостей проведення СІО під кутом права висловлені у наукових працях О. Заруби, О. Кушнір,

В. Ліпкана, В. Петрика тощо. Слід згадати також дисертаційні дослідження О. Кубишкіна, В. Разуваєва, О. Тамодліна тощо.

Однак, не зважаючи на значну кількість наукових доробок, до цього часу недостатньо вивченими лишаються питання правового забезпеченні СІО та обґрунтування інформаційно-правових засад СІО, що визначає актуальність цього дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до Пріоритетних напрямів розвитку правової науки на 2016–2020 рр., затверджених Постановою Загальних зборів Національної академії правових наук України від 03.03.16., а також в рамках планових дослідницьких тем Науково-дослідного інституту інформатики і права Національної академії правових наук України "Теоретичні та організаційно-правові основи забезпечення кібербезпеки в Україні" (№ державної реєстрації 0116U007745) та «Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері» (№ державної реєстрації 0117U007745).

Результати дослідження було розглянуто та обговорено на науково-практичному семінарі в Науково-дослідному інституті інформатики і права Національної академії правових наук України, протокол від 29 жовтня 2019 року.

Мета і завдання дослідження. *Мета дослідження* полягає у теоретичному визначенні, обґрунтуванні й розкритті сутності правового забезпечення СІО, а також у напрацюванні конкретних пропозицій щодо його удосконалення.

Досягнення мети здійснюється шляхом вирішення таких *завдань*:

– розкрити генезис теоретико-прикладного осмислення проблематики правового забезпечення СІО і визначити на цій основі головні напрями дослідження;

– виявити сутність основних категорій інформаційного права, які характеризують понятійно-категоріальний апарат дослідження;

– визначити методологію дослідження;

– дослідити організаційно-правові засади проведення СІО та теоретико-методологічні засади їх інформаційного забезпечення;

– визначити місце СІО в системі заходів протидії загрозам національній безпеці України;

– окреслити основні проблеми правового забезпечення СІО та напрацювати конкретні пропозиції щодо їх подолання.

Об'єкт дослідження – суспільні відносини, що складаються у процесі проведення СІО.

Предмет дослідження – правове забезпечення СІО.

Методи дослідження ґрунтуються на законах діалектики, розробленій на їхній основі теорії пізнання, що поєднує в собі загально філософські, загальнонаукові та спеціальні методи пізнання. Так, теоретико-прикладна частина дослідження здійснювалась із застосуванням комплексу загальнонаукових методів:

– індукції та дедукції – для зіставлення окремих наукових понять і категорій (інформаційна безпека, інформаційна війна, інформаційні операції тощо) (підрозділи 1.2, 1.3);

– аналізу та синтезу – з метою визначення сутності та змісту інформаційно-правових засад СІО в сучасних умовах, оцінки вітчизняного та іноземного досвіду в цій сфері, формулювання правових та організаційних засад удосконалення інформаційно-правового забезпечення СІО (підрозділ 1.2, 1.3, 2.2, 2.3, 3.1, 3.2, 3.3);

– аналогії та компаративістики – для поглибленого дослідження теоретичних, організаційних та правових засад проведення СІО та їх інформаційного забезпечення в Україні та зарубіжних державах, вироблення шляхів оптимізації інформаційно-правового забезпечення СІО (розділи 2, 3);

– тлумачення – для аналізу та розкриття змісту основних категорій інформаційного права, які характеризують понятійно-категоріальний апарат дослідження (розділ 1).

– логіко-семантичного методу – для уточнення понятійного апарату, з'ясування сутності інформаційно-правового забезпечення СІО (розділи 1, 2).

Зі спеціальних методів під час дослідження використано:

– історичний – для розгляду становлення інформаційно-правових засад СІО та наукових поглядів у зазначеній сфері (розділ 1);

– системно-структурний – для аналізу стану інформаційно-правових засад СІО на рівні міжнародного та національного законодавства (розділ 2, 3);

– порівняльно-правовий – при аналізі норм галузей права України, зарубіжного законодавства, міжнародних документів про забезпечення інформаційної та національної безпеки (розділи 2, 3);

– структурно-функціональний – для дослідження системного взаємозв'язку та взаємодії суб'єктів проведення СІО, а також стадій проведення СІО як елементів єдиної системи (розділи 2, 3);

– соціологічний і статистичний – у процесі вивчення кількісних та якісних параметрів, що вказують на необхідність покращання інформаційно-правового забезпечення СІО, характеризують його стан, процес забезпечення національної безпеки в цілому (розділи 2, 3);

– прогнозування – з метою формулювання пропозицій щодо удосконалення інформаційно-правового забезпечення СІО (розділ 3).

Особливу роль у дослідженні відіграє тензорна методологія, яка дозволяє обґрунтовано пов'язувати процес і структуру, що набуває особливого значення для організації та проведення СІО як складової системи стратегічних комунікацій. Застосування її принципів дозволяє представляти будь-яку систему з низки аналогічних систем як проекцію узагальненої системи, найбільш ефективно використовуючи метод моделювання та поширюючи на СІО закономірності правового регулювання стратегічних комунікацій. Це забезпечує єдність методів, практичної діяльності й теорії, емпіричних і наукових знань.

Емпіричну базу дослідження становлять матеріали навчальної, навчально-методичної літератури з проблематики інформаційного права та забезпечення національної безпеки, публікацій у ЗМІ, аналітичні матеріали, статистичні дані тощо. Збирання, оброблення й аналіз статистичної та соціологічної інформації здійснювалися із дотриманням вимог репрезентативності, що висуваються до

подібних досліджень. Нормативно-правовою основою роботи стали Конституція та законодавство України, законодавство зарубіжних країн, міжнародно-правові акти, що регулюють питання безпеки, інформаційного протиборства тощо.

Наукова новизна отриманих результатів полягає у теоретичному визначенні, обґрунтуванні й розкритті сутності правового забезпечення СІО, зокрема:

уперше:

– надано правову дефініцію СІО як складової стратегічних комунікацій – скоординованого і належного використання комунікативних можливостей держави з метою проведення розвідувальних або контррозвідувальних заходів, спрямованих на досягнення стратегічних (оперативних) цілей в інформаційному просторі та просування цілей держави;

– розкрито зміст правового забезпечення СІО, під яким розуміється комплекс заходів, пов’язаних з розробкою та реалізацією норм права, що регламентують проведення СІО, а також із забезпеченням правового супроводу проведення СІО та профілактикою порушень вимог законодавчих та інших нормативно-правових актів в ході їх проведення;

– правове забезпечення СІО визначено як комплекс заходів організаційно-правового та теоретико-методологічного характеру щодо задоволення потреб суб’єктів СІО у правовій та іншій інформації, необхідній для проведення СІО відповідно до вимог чинного законодавства;

– розроблено теоретичні засади правового забезпечення синергетичної СІО.

удосконалено:

– наукове уявлення про СІО;

– класифікацію СІО за типом і видом;

– теоретичні напрацювання у сфері законодавчого підґрунтя проведення СІО на міжнародному та національному рівнях з обґрунтуванням доцільності:

передбачення на рівні міжнародного договору відповідно до підходів, окреслених в Резолюції 60/45 Генеральної Асамблеї ООН «Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», зобов'язань учасників не вдаватися в інформаційному просторі до дій, метою яких є завдання збитків інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо, заради здійснення підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення, що здатні дестабілізувати життєдіяльність суспільства й держави;

визначення серед функцій Служби безпеки України та розвідувальних органів (у проекті Закону України Про внесення змін до Закону України “Про Службу безпеки України” та у проекті Закону України «Про розвідку» відповідно) такої функції, як «участь у забезпеченні загальнодержавної системи стратегічних комунікацій»; передбачення серед повноважень Служби безпеки України у проекті Закону України Про внесення змін до Закону України “Про Службу безпеки України” повноваження «проводити спеціальні інформаційні операції; протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і

територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій»; у проекті Закону України «Про розвідку» передбачення серед повноважень розвідувальних органів України повноваження «проводити спеціальні інформаційні операції з метою сприяння реалізації національних інтересів України та протидії зовнішнім загрозам національній безпеці України у визначених законом сферах»;

розробки РНБО України за участю інших державних органів, що входять до складу сектору безпеки і оборони України, загальнодержавної Концепції стратегічних комунікацій, із закріпленням у ній запропонованого визначення СІО.

дістали подальший розвиток:

– сучасні наукові погляди на розвиток інформаційного суспільства, інформаційного права, сутність та природу інформаційної безпеки, інформаційної війни та інформаційної зброї;

– підходи до визначення алгоритму СІО та спектру методів, що можуть використовуватись в ході СІО;

– концепція мережної боротьби в інформаційному просторі.

Практичне значення отриманих результатів визначається прикладною спрямованістю дисертації, а також тим, що подані в ній пропозиції сприятимуть не лише підвищенню ефективності інформаційно-правового забезпечення СІО, але й розвитку інформаційного права в цілому. У результаті дослідження вироблено та сформульовано конкретні правові норми, пропозиції, прикладні моделі, що можуть бути використані:

– у науково-дослідній сфері – викладені в дисертації положення, узагальнення, висновки і рекомендації мають теоретичне і прикладне значення для науки та практики інформаційного права, а також забезпечення національної безпеки. Основні результати закладають фундамент проведення подальших наукових досліджень із проблем інформаційного протиборства аспірантами, здобувачами та докторантами навчальних закладів органів сектору безпеки і оборони України та для науково-методичного забезпечення проведення СІО (*акт впровадження Науково-дослідного інституту інформатики і права Національної академії правових наук України від 11.07.19*);

– у сфері правотворчості – висновки, пропозиції та рекомендації, сформульовані в дисертації, можуть бути використані у подальшому розвиткові інформаційного права як відповідної галузі права та законодавства, а також для підготовки й уточнення положень конкретних законодавчих та підзаконних актів, зокрема, при розробці: нової редакції Закону України «Про Службу безпеки України»; Закону України «Про розвідку»; загальнодержавної Концепції стратегічних комунікацій, міжвідомчих та відомчих нормативних актів, що регламентують питання проведення СІО сектором безпеки і оборони України (*довідка про апробацію та впровадження від Апарату Голови СБ України від 20.06.2019*);

– у правозастосовній сфері – використання одержаних результатів дасть змогу покращити практичну діяльність складових сектору безпеки і оборони України щодо проведення СІО та сприятиме розвитку інформаційного права;

– в освітньо-науковому процесі – матеріали дисертації можуть використовуватися при проведенні лекцій, семінарських та практичних занять з навчальної дисципліни «Інформаційне право», «Інформаційна безпека держави» («Основи інформаційної безпеки держави»), «Основи національної безпеки», «Забезпечення державної безпеки України» тощо.

Особистий внесок. Дисертаційна робота виконана самостійно з використанням останніх досягнень науки інформаційного права. Всі сформовані у роботі положення та висновки обґрунтовано на основі особистих досліджень автора. При використанні наукових праць інших вчених для обґрунтування власних міркувань автора на них зроблено відповідні посилання.

Апробація результатів дисертації. Основні положення та результати дисертаційного дослідження оприлюднено на міжнародних та всеукраїнських науково-практичних конференціях з проблематики інформаційного права та забезпечення національної безпеки, зокрема: XV Міжнародна науково-практична конференція «Інформаційні технології і безпека» (21 жовтня 2015 р., Київ); Міжнародна науково-практична конференція «Юридична наука: виклики і сьогодення» (7-8 червня 2019 р., Одеса); International scientific and practical conference «Legal practice in EU countries and Ukraine at the modern stage» (25–26 липня 2019 р., Арад, Румунія).

Публікації. За темою дисертації автором опубліковано 9 наукових праць, зокрема: 6 одноосібних статей у наукових фахових виданнях, з яких 2 статті опубліковано в міжнародних виданнях, а також 3 тези наукових повідомлень.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, які поділяються на дев’ять підрозділів, висновків, списку використаних джерел (262 найменування на 22 сторінках), 8 додатків (на 56 сторінках). Повний обсяг дисертації становить 287 сторінок, із них основний текст – 207 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовується актуальність, доцільність і ступінь розробленості проблеми дослідження, вказується зв’язок з науковими програмами, планами, темами, визначається мета та завдання, об’єкт, предмет та методи дослідження, наукова новизна, практичне значення отриманих результатів дослідження, апробація результатів дисертації та її структура, наводяться наукові публікації, у яких відображені результати дисертації.

У першому розділі «Становлення та формування наукового знання з проблематики правового забезпечення спеціальних інформаційних операцій» розглядаються історіографія та сучасний стан наукової розробки проблематики інформаційно-правових засад СІО, здійснюється визначення понятійно-категоріального апарату дослідження, методології дослідження тощо.

У підрозділі 1.1 «Історична ретроспектива становлення та сучасний стан наукового знання з проблематики правового забезпечення спеціальних інформаційних операцій» зазначається, що не зважаючи на те, що інформаційний вплив використовувався в ході соціальних конфліктів (в тому числі збройних) з давніх давен, хвиля технічного прогресу внесла істотні зміни в методи вирішення

геополітичних, військових, економічних, торговельних і інших конфліктів, тож силові методи наразі поступаються місцем методам інформаційним.

Сучасний інформаційний вплив пропонують розглядати в рамках теорії й практики ведення війн четвертого покоління (4th generation warfare), або «стратегії 4GW» – самостійного виду впливу, ефективної зброї, спрямованої на позбавлення супротивника волі до опору, щоб відмовитися від військової сили. Теорія й практика ведення війн четвертого покоління, або стратегії 4 GW, була реалізована, зокрема, в операціях збройних сил США в Іраку, Афганістані, Лівії тощо, а також реалізується Російською Федерацією у гібридній війні проти України.

У міру накопичення досвіду практичного здійснення інформаційного впливу на цільову аудиторію у військових конфліктах, економічних суперечках, політичній боротьбі тощо виникла потреба в його теоретичному осмисленні, що викликало до життя науковий інтерес до питань інформаційної війни та застосування інформаційної зброї, проведення СІО тощо. Втім, наразі в науці інформаційного права лишаються практично недослідженими проблеми правового забезпечення та інформаційно-правових засад СІО.

У підрозділі 1.2 «Понятійно-категоріальний апарат дослідження проблематики правового забезпечення спеціальних інформаційних операцій» розглядається понятійно-категоріальний апарат дослідження, який формується переважно категоріями інформаційного права. Ключовими поняттями при цьому слугують наступні: інформаційна безпека, інформаційна загроза, інформаційна війна, інформаційна зброя, інформаційні операції, інформаційно-правове забезпечення тощо.

Під інформаційними загрозами, які слід виокремлювати із загального кола загроз інформаційній безпеці, розуміються інформаційні впливи технічного або психологічного характеру, що унеможливлюють чи ускладнюють (можуть унеможливлювати чи ускладнювати) збереження національних цінностей, реалізацію національних інтересів та досягнення національних цілей України.

Інформаційна війна з урахуванням існуючих точок зору на її природу визначена як сукупність цілеспрямованих інформаційних впливів, що здійснюються суб‘єктом впливу на інформаційні системи або соціальні процеси з використанням засобів інформаційних технологій, інформаційних ресурсів і комунікацій шляхом створення факторів гальмування сталого розвитку або трансформації стабільності держави, суспільства, людини з метою втримання (досягнення) панування, переваги, монополії в різних сегментах людського буття.

Інформаційну зброю характеризує передусім її цільове призначення і адресний контекст, адже відсутній вичерпний та фіксований перелік форм та змісту інформаційної зброї. Інформація «стає» інформаційною зброєю в разі включення до цілеспрямованої програми впливу на інформаційну систему, здатної призвести до досягнення запланованих суб‘єктом впливу результатів. Як інформаційна зброя можуть використовуватися й інформаційні технології. Інформаційна зброя є засобом здійснення СІО.

Оскільки СІО можуть проводитись не лише в ході наступальної інформаційної війни, але й з метою забезпечення національної безпеки, СІО у

функціональному аспекті доцільно розглядати як алгоритм застосування інформаційної зброї/нейтралізації загрози в інформаційній сфері, використання якого забезпечує досягнення мети інформаційної війни/забезпечення інформаційної безпеки.

Правове забезпечення СІО визначено як комплекс заходів, пов'язаних з розробкою та реалізацією норм права, що регламентують проведення СІО, а також із забезпеченням правового супроводу проведення СІО та профілактикою порушень вимог законодавчих та інших нормативно-правових актів в ході їх проведення. Із цим поняттям тісно пов'язане поняття інформаційно-правового забезпечення СІО, під яким розуміється комплекс заходів організаційно-правового та теоретико-методологічного характеру щодо задоволення потреб суб'єктів СІО у правовій та іншій інформації, необхідній для проведення СІО відповідно до вимог чинного законодавства.

У підрозділі 1.3 «Методологія дослідження проблематики правового забезпечення спеціальних інформаційних операцій» зазначається, що головна ідея і основні положення концепції дослідження відображені в гіпотезі,відповідно до якої належне інформаційно-правове забезпечення СІО на основі норм та принципів інформаційного права дозволить підвищити ефективність проведення СІО, що сприятиме забезпеченню національної безпеки України та досягненню нашою державою інформаційних переваг у реальних та потенційних інформаційних конфліктах, в т.ч. в ході гібридної війни. Зазначене дослідження базується на використанні комплексу загальнонаукових і спеціальних методів, притаманних дослідженням з інформаційного права. Особливу роль у дослідженні відіграє тензорна методологія, яка дозволяє обґрунтовано пов'язувати процес і структуру, що набуває особливого значення для організації та проведення СІО як складової системи стратегічних комунікацій. Застосування тензорної методології також дозволяє представляти будь-яку систему з низки аналогічних систем як проекцію узагальненої системи, найбільш ефективно використовуючи метод моделювання та поширюючи на СІО закономірності здійснення стратегічних комунікацій. Це забезпечує єдність методів, практичної діяльності й теорії, емпіричних і наукових знань.

У другому розділі «Теоретико-методологічні та організаційно-правові засади спеціальних інформаційних операцій» з'ясовується роль СІО у веденні інформаційної війни та забезпеченні національної безпеки, розглядаються організаційно-правові засади проведення СІО та теоретико-методологічні засади інформаційного забезпечення СІО.

У підрозділі 2.1 «Спеціальні інформаційні операції у веденні інформаційної війни та забезпеченні національної безпеки», – з'ясовується, що концепція інформаційної війни, у становленні якої наразі вирізняють чотири покоління, передбачає використання інформаційної зброї шляхом проведення інформаційних операцій, різновидом яких є СІО.

СІО можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки інформаційного протиборства. СІО обох типів, а так само комплексні СІО можуть проводитися на оперативно-

тактичному, стратегічному й глобальному рівнях з метою оперативної або стратегічного маскування конфліктуючими сторонами своїх реальних військових, геополітичних, політичних, економічних задумів, завдань і намірів, а також з метою дискредитації дій імовірного супротивника, його державної політики, економічних структур тощо. Класичним прикладом використання СІО в оборонній інформаційній війні, тобто, у забезпеченні національної безпеки, можуть вважатися антитерористичні СІО. Важливою складовою антитерористичних СІО є інформаційно-психологічний вплив не тільки на терористів, але й на цивільне населення, у тому числі на суспільну думку як у власній, так і у закордонних країнах. Виходячи з того, що на світовій арені відбувається геополітичне інформаційне протиборство, можна констатувати, що силові маневри держав, у сферу стратегічних інтересів яких входить Україна (мова йде в першу чергу про РФ, що вступила у відкриту фазу силового протистояння з нашою країною), спрямовані на нав'язування нашій незалежній державі своєї політичної волі й бачення майбутнього, установлення й досягнення стратегічних обріїв, які визначаються геоекономічною конкуренцією. Сили країни-агресора переважно перевершують вітчизняний потенціал, що змушує Україну звертатися до ідеї асиметричної протидії, у якій СІО відіграє одну з першорядних ролей.

У підрозділі 2.2 «*Організаційно-правові засади проведення спеціальних інформаційних операцій*» досліджується нормативно-правовий базис та організаційне підґрунтя проведення СІО. Слід констатувати, що правове підґрунтя проведення СІО окреслено наступними напрямками: нормативно-правові акти, що визначають обмеження і заборони при проведенні СІО (міжнародно-правові акти з питань протидії інформаційним загрозам, забезпечення інформаційної безпеки й регулювання інформаційного протиборства, а також акти національного інформаційного законодавства, присвячені регламентації інформаційних правовідносин та інформаційної сфери); нормативно-правові акти, що регламентують порядок і процес проведення СІО (внутрішньодержавні нормативно-правові акти відомчого характеру, які переважно мають закритий характер).

У сучасному міжнародному праві однозначно не вирішене питання про співвідношення між транскордонним характером інформаційних мереж і принципом державного суверенітету, а також відсутнє чітке розмежування таких понять як збройний напад, застосування сили, акт агресії й інших дотичних понять, відтак невизначеним лишається статус СІО, передусім здійснюваних в мирний час. Вочевидь, міжнародне співтовариство має знайти загальне розуміння підходів, згаданих в Резолюції 60/45 Генеральної Асамблеї ООН «Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», і розглядати його надалі як основу багатостороннього договору (конвенції), що створює універсальний режим міжнародної інформаційної безпеки. Основною ідеєю такого договору має стати визначення обмежень на проведення деструктивних СІО, зокрема, зобов'язання учасників не вдаватися в інформаційному просторі до дій, метою яких є завдання збитків інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо,

заради здійснення підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення, що здатні дестабілізувати життєдіяльність суспільства й держави.

З урахуванням положень Закону України «Про оборону України» СІО можуть розглядатися як сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем та часом спеціальних дій підрозділів Сил спеціальних операцій Збройних Сил України, спрямованих на створення умов для досягнення стратегічних (оперативних) цілей в інформаційному просторі, які проводяться за єдиним задумом самостійно або у взаємодії з військовими частинами, іншими підрозділами Збройних Сил України, інших військових формувань, правоохоронних органів України та інших складових сил оборони для виконання завдань. У ч.2 ст.4 вказаного Закону СІО (в числі інших спеціальних операцій) розглядаються як форма воєнних дій. У Воєнній доктрині України і Доктрині інформаційної безпеки України СІО (які є специфічним видом інформаційних операцій) опосередковано визначаються як елемент стратегічних комунікацій, що в цілому відповідає загальносвітовому тренду. Правові межі для проведення стратегічних комунікацій визначені у п.2.7 Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України, де, зокрема, зазначено, що інформаційні та психологічні операції (в т.ч. й СІО) не проводяться стосовно громадян України (крім тих, які є членами терористичних угруповань та незаконних збройних формувань), а також на території України поза межами території, на якій введено правовий режим воєнного стану, поза межами району проведення антитерористичної операції або інших місць (районів) підготовки та застосування Збройних Сил. Слід також зауважити, що відсутність правової регламентації проведення СІО у мирний час ускладнює можливість проведення СІО не лише Збройними Силами України та іншими військовими формуваннями, але й правоохоронними органами України та іншими складовими сил оборони для виконання завдань. Крім того, залишається фактично позбавленим належного правового підґрунтя проведення СІО силами безпеки відповідно до їх компетенції, в тому числі й з метою протидії деструктивним СІО.

У підрозділі 2.3 «Теоретико-методологічні засади інформаційного забезпечення спеціальних інформаційних операцій» відзначається, що теоретико-методологічні засади інформаційного забезпечення СІО наразі характеризуються розгалуженим інструментарієм, який може успішно використовуватись як у військовий, так і у мирний час для різної цільової аудиторії.

При інформаційно-технічній боротьбі головними об'єктами впливу й захисту є інформаційно-технічні системи (системи зв'язку, телекомунікаційні системи, радіоелектронні засоби тощо). Інформаційно-технічний вплив є цілеспрямованим виробництвом і поширенням спеціальної інформації, яка безпосередньо впливає на функціонування й розвиток інформаційно-технічного середовища суспільства, тобто комп'ютери, засоби зв'язку й програмне забезпечення, що відіграють роль зброї масового знищення, за допомогою якої можна проникати в комп'ютерні системи й порушувати їхню роботу. Основна роль у цьому приділяється руйнівним атакам на критичну інфраструктуру супротивника. При проведенні СІО

інформаційно-психологічного характеру основними об'єктами впливу стають психіка представників політичної еліти й населення конфронтуючих держав, а також система формування суспільної свідомості, думки й прийняття державно-управлінських рішень у сфері національної безпеки.

При цьому принципами планування та проведення СІО є наступні: застосування «ефект-орієнтованого» підходу, який передбачає комбінацію летальних і нелетальних засобів з акцентуванням уваги в інформаційній сфері на причинах та наслідках; особиста участь командування СІО у її проведенні з метою забезпечення контролю за всією інформаційною діяльністю; координація та впорядкування дій команди виконавців СІО з метою забезпечення оптимальної послідовності, синхронізації та уникнення внутрішніх суперечностей; належне інформаційно-аналітичне забезпечення, в тому числі інтелектуальну розвідку, а також взаємодія між елементами команди виконавців СІО, які здійснюють збирання первинної інформації та її наступну обробку і оцінювання; поєднання централізованого планування і децентралізованого виконання; детальне встановлення цілей та можливих ефектів інформаційних дій на стадії планування; завчасна підготовка та забезпечення інформацією; безперервність інформаційної функції щодо місця, часу, аудиторії, конфліктної або постконфліктної фази.

Проведення СІО за стандартами НАТО передбачає врахування особливостей інформаційного середовища, як середовища, у якому «люди і автоматизовані системи спостерігають, орієнтують, вирішують та реагують на інформацію, відтак це є основне середовище прийняття рішень». Зокрема, стандарти НАТО передбачають такі основні інструменти та методи, що використовуються в ході СІО: психологічні операції, покликані впливати на сприйняття, ставлення та поведінку обраних цільової аудиторії; демонстрація присутності (сили), статусу та соціального профілю; забезпечення інформаційної безпеки (комунікаційної безпеки, комп'ютерної безпеки, безпеки мереж, включно) та власне безпеки операції; введення в оману (маніпуляція, викривлення інформації, фальсифікація тощо) супротивника на всіх рівнях; «радіоелектронна війна», в тому числі з метою підтримання психологічних операцій, введення в оману та інших методів, що застосовуються (у ході СІО «захисного спрямування» використовуються радіоелектронні захисні заходи); фізичне руйнування з метою створення інформаційного ефекту (за умови врівноваження потенційного негативного впливу та очікуваних переваг); забезпечення лідером (керівником СІО) визначення ролей та адаптивних взаємовідносин між виконавцями СІО; комп'ютерні мережеві операції (комп'ютерна мережева атака; експлуатація і захист комп'ютерних мереж); зв'язки з громадськістю та військово-цивільне співробітництво задля встановлення довірчих стосунків між збройними силами, цивільними агентствами та мирним населенням; участь у виконанні завдань зв'язку, розвідки, наданні консультативної допомоги, координації управління інфраструктурними проектами, рятувальних операціях з метою забезпечення доступу до джерел інформації. Взяття відповідних теоретико-методологічних напрацювань «на озброєння» сектором безпеки і оборони України та його нормативно-правове

закріплення на рівні відомчих актів значно посилить спроможності нашої держави у веденні інформаційного протиборства в умовах гібридної війни.

У третьому розділі «Правове забезпечення спеціальних інформаційних операцій: сучасний стан та напрями_вдосконалення» визначається місце СІО в системі заходів протидії загрозам національній безпеці України, аналізуються актуальні проблеми правового забезпечення СІО та окреслюються напрями його вдосконалення.

У підрозділі 3.1 «Спеціальні інформаційні операції в системі заходів протидії загрозам національній безпеці України» за результатами аналізу актуальних загроз національній безпеці України визначено та систематизовано основні заходи протидії таким загрозам: політико-дипломатичні; військові; правові (законодавчі); інформаційно-психологічні; економічні; науково-технологічні; організаційні (адміністративні й процедурні); фізичні; технічні (апаратні й програмні) тощо. Кожна з груп заходів протидії загрозам національній безпеці залежно від характеру джерел загроз має зовнішній і внутрішній аспекти. Залежно від об'єкту національної безпеки, життєво важливі інтереси якого захищаються від внутрішніх і зовнішніх загроз, відповідні заходи реалізуються у площині забезпечення безпеки особистості, суспільства, держави тощо. Слід враховувати, що правові заходи мають подвійну природу, і можуть розглядатися як з точки зору форми (тоді мова йде про логічний взаємозв'язок: «правові-організаційні-технічні й фізичні заходи», за якого презюмується, що правове підґрунтя повинні мати політичні, військові, економічні та інші заходи), так і з точки зору змісту (як самостійна за змістовним наповненням група заходів). Це ж стосується також і заходів інформаційного характеру, які не лише становлять самостійну групу заходів протидії загрозам національній безпеці, але й забезпечують та супроводжують реалізацію інших заходів, а також забезпечують обмін інформацією між різними елементами системи відповідних заходів.

У підрозділі 3.2 «Актуальні проблеми правового забезпечення спеціальних інформаційних операцій» зазначається, що основною проблемою правового забезпечення СІО є відсутність достатнього законодавчого унормування проведення СІО. Відповідно, відсутнє й належне підґрунтя розробки методологічних засад інформаційного забезпечення СІО. Це зумовлює потребу у законодавчому визначенні заборон при здійсненні інформаційного впливу, в тому числі в ході проведення СІО, які визначатимуть межі їх проведення, адже в Україні, як у правовій державі, діяльність органів влади, відповідальних за забезпечення національної безпеки має ґрунтуватися на нормах закону.

Оскільки спеціальні операції в цілому (інформаційні та психологічні), в т.ч. СІО, наразі розглядаються за законодавством України як форма воєнних дій, фактично унеможливлюється проведення контррозвідувальних СІО на території України, зокрема проведення СІО стосовно громадян України (крім тих, які є членами терористичних угруповань та незаконних збройних формувань – хоча цими категоріями не вичерпується коло осіб, причетних до протиправних дій; так, як потенційна «аудиторія» СІО можуть розглядатися, наприклад, також учасники організованих злочинних угруповань), а також проведення СІО на території

України поза межами території, на якій введено правовий режим воєнного стану, поза межами району проведення антитерористичної операції або інших місць (районів) підготовки та застосування Збройних Сил.

У підрозділі 3.3 «Напрями вдосконалення правового забезпечення спеціальних інформаційних операцій» визначається, що напрями вдосконалення правового забезпечення СІО залежать передусім від формування належного правового підґрунтя проведення СІО.

Оскільки як розвідувальний, так і контррозвідувальний аспект СІО проявляється на всіх етапах СІО незалежно від їх спрямування, «наступального» або «оборонного» характеру, питанням нагальної необхідності є надання на законодавчому рівні повноважень щодо проведення СІО Службі безпеки України з одночасним позбавленням її статусу військового формування, що забезпечить дотримання вимог ст.17 Конституції України, а також ефективне проведення СІО не лише в інтересах оборони, але й в інтересах антитерористичної, інформаційної та інших складових національної безпеки України. Аналогічні повноваження мають бути передбачені законом і для розвідувальних органів України, а також інших суб'єктів сектору безпеки і оборони. Не менш важливим є й нормативне закріплення визначення СІО на рівні закону, що надалі забезпечить розробку ефективної моделі та алгоритму проведення СІО. З цією метою пропонується:

– у проекті Закону України Про внесення змін до Закону України "Про Службу безпеки України" та у проекті Закону України «Про розвідку» визначити серед функцій Служби безпеки України та розвідувальних органів «участь у забезпеченні загальнодержавної системи стратегічних комунікацій», передбачити серед повноважень Служби безпеки України наступне: «проводити спеціальні інформаційні операції; протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій», а серед повноважень розвідувальних органів України – «проводити спеціальні інформаційні операції з метою сприяння реалізації національних інтересів України та протидії зовнішнім загрозам національній безпеці України у визначених законом сферах»;

– РНБО України за участю інших державних органів, що входять до складу сектору безпеки і оборони України, розробити загальнодержавну Концепцію стратегічних комунікацій, у якій закріпити наступне визначення СІО: «скоординоване і належне використання комунікативних можливостей держави з метою проведення розвідувальних або контррозвідувальних заходів, спрямованих на досягнення стратегічних (оперативних) цілей в інформаційному просторі та просування цілей держави».

Такі першочергові заходи, здійснені з дотриманням принципів інформаційного права, дозволять створити належне законодавче підґрунтя для правового забезпечення СІО, а також інформаційно-методичного забезпечення СІО.

Зокрема, важливим питанням оптимізації інформаційно-методичного забезпечення СІО є визначення моделі та формування алгоритму проведення СІО на засадах тензорної методології. Синергетична модель СІО, яка поєднуватиме

традиційні моделі, призначена для одночасного вирішення наступних завдань стосовно визначеної цільової аудиторії: зміна ставлення до певного об'єкта/дій; зміна поведінки; зміна світосприйняття та світоглядної картини (з одночасним унеможливленням досягнення аналогічних цілей іноземними державами, їх спецслужбами, окремими організаціями, спільнотами й особами, що діють на шкоду національній безпеці України тощо). Використання принципів тензорної методології дозволяє інтегрувати до синергетичної моделі проведення СІО досвід контрмережної боротьби, який передбачає використання підмереж (підмережа датчиків або ж сенсорів: підмережа комунікацій; підмережа аналізу інформації; підмережа «вузлів прийняття рішень»; підмережа «виконавчих вузлів»), а також поширити на СІО закономірності правового регулювання стратегічних комунікацій.

При цьому у проведенні СІО з урахуванням сучасних реалій гібридної війни та актуальних стандартів НАТО з питань проведення інформаційних і психологічних операцій пропонується виділити такі етапи: підготовчий етап; етап пошуку або створення інформаційного приводу (інформаційний етап); етап планування СІО; етап реалізації запланованих заходів; закріплювальний етап («етап виходу» з СІО).

В сучасних умовах СІО доречно типологізувати наступним чином: СІО, об'єктом (ціллю) яких є конкретна особа або визначене коло осіб (суб'єкти прийняття рішень або інші особи, які мають певний авторитет); СІО, спрямована на ініціювання, зміну напрямку розвитку, припинення чи «розмиття» певного процесу, явища чи події; «Спін-операції», які спрямовуються на формування дискурсу та створення «вікон Овертона». Відповідно необхідно актуалізувати й видологію СІО: СІО в новинарній сфері – з використанням радіо, телебачення, періодичних друкованих ЗМІ (журнали, газети) та неперіодичних друкованих видань (листівки, плакати тощо); СІО в комунікативній сфері – використовуються електронні (on-line) соціальні мережі та фізичні (off-line) соціальні мережі; СІО в науковій та культурній сфері – впровадження «інформаційних закладок» до літературних джерел тощо.

Запропонована класифікація СІО, а також системний підхід до їх планування та підготовки на базі відповідного алгоритму слугує підґрунтям для побудови матриці інформаційно-правового забезпечення синергетичної моделі СІО, застосування якої складовими сектору безпеки і оборони України дозволить підвищити ефективність інформаційно-правового забезпечення СІО та сприятиме підвищенню їх результативності.

ВИСНОВКИ

За результатами проведеного дослідження, на підставі аналізу здобутків науки інформаційного, адміністративного, воєнного тощо права, законодавства України, зарубіжного досвіду напрацювання інформаційно-правових засад забезпечення проведення СІО, здійснено теоретичне узагальнення та запропоновано нове вирішення актуального наукового завдання щодо теоретичного визначення, обґрунтування й розкриття сутності правового

забезпечення СІО, а також напрацьовані теоретичні засади інформаційно-правового забезпечення СІО відповідно до потреб сектору безпеки і оборони України.

Відповідно до завдань дослідження, сформульовано низку важливих висновків, зокрема:

1. На основі аналізу генезису теоретико-прикладного осмислення проблематики правового забезпечення СІО, встановлено, що не зважаючи на тривалу історію теоретико-прикладного осмислення досвіду використання інформаційного впливу у військових конфліктах, економічних суперечках, політичній боротьбі, а також на неабиякий науковий інтерес до проблематики інформаційної війни, застосування інформаційної зброї, інформаційних операцій тощо, наразі в науці інформаційного права лишаються практично недослідженими проблеми правового забезпечення СІО.

2. Дослідження сутнісних характеристик дозволили визначити, що понятійно-категоріальний апарат дослідження питань правового забезпечення СІО характеризують такі категорії інформаційного права:

– інформаційна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, за якої забезпечуються формування, використання та розвиток інформаційної сфери в інтересах її суб‘єктів, сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці шляхом розвитку власного інформаційного простору, зведення до мінімуму заподіяння шкоди через неповноту, невчасність і недостовірність інформації, інформаційний вплив, негативні наслідки функціонування інформаційних технологій несанкціоновані дії з інформацією, а також постійний процес діяльності компетентних органів, спрямований на забезпечення й підтримання відповідного стану захищеності;

– інформаційні загрози – інформаційні впливи технічного або психологічного характеру, що унеможливлюють чи ускладнюють або можуть унеможливлювати чи ускладнювати збереження національних цінностей, реалізацію національних інтересів та досягнення національних цілей України;

– інформаційна війна – сукупність цілеспрямованих інформаційних впливів, що здійснюються суб‘єктом впливу на інформаційні системи або соціальні процеси з використанням засобів інформаційних технологій, інформаційних ресурсів і комунікацій шляхом створення факторів гальмування сталого розвитку або трансформації стабільності держави, суспільства, людини з метою втримання (досягнення) панування, переваги, монополії в різних сегментах людського буття;

– інформаційна зброя – інформація та інформаційні технології, включені до цілеспрямованої програми впливу на інформаційну систему, здатної призвести до досягнення запланованих суб‘єктом впливу результатів;

– СІО – алгоритм застосування інформаційної зброї/ нейтралізації загрози в інформаційній сфері, використання якого забезпечує досягнення мети інформаційної війни/ забезпечення інформаційної безпеки;

– правове забезпечення СІО – комплекс заходів, пов'язаних з розробкою та реалізацією норм права, що регламентують проведення СІО, а також із забезпеченням правового супроводу проведення СІО та профілактикою порушень вимог законодавчих та інших нормативно-правових актів в ході їх проведення;

– інформаційно-правове забезпеченням СІО – комплекс заходів організаційно-правового та теоретико-методологічного характеру щодо задоволення потреб суб'єктів СІО у правовій та іншій інформації, необхідній для проведення СІО відповідно до вимог чинного законодавства.

3. На сонові системного аналізу, з'ясовано, що методологія дослідження правового забезпечення СІО, як головний орієнтир наукового пошуку, становить систему методів (способів і прийомів), а також сукупність принципів, застосування яких уможливлює одержання нових знань щодо організації та проведення СІО. Особливу роль у дослідженні відіграє тензорна методологія, яка дозволяє обґрунтовано пов'язувати процес і структуру, що набуває особливого значення для організації та проведення СІО як складової системи стратегічних комунікацій. Застосування тензорної методології дозволяє поширити на СІО закономірності здійснення стратегічних комунікацій.

4. Встановлено, що СІО можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки інформаційного протиборства. СІО обох типів, а так само комплексні СІО можуть проводитися на оперативно-тактичному, стратегічному й глобальному рівнях.

5. На основі ґрунтовного аналізу правової бази, визначено, що організаційно-правові засади проведення СІО ґрунтуються на нормативно-правових актах, що визначають обмеження і заборони при проведенні СІО (міжнародно-правові акти з питань протидії інформаційним загрозам, забезпечення інформаційної безпеки й регулювання інформаційного протиборства, а також акти національного інформаційного законодавства, присвячені регламентації інформаційних правовідносин та інформаційної сфери) та нормативно-правових актах, що регламентують порядок і процес проведення СІО (національні акти відомчого характеру). У сучасному міжнародному праві статус СІО лишається невизначеним, що зумовлює необхідність створення універсального режиму міжнародної інформаційної безпеки відповідно до підходів, окреслених в Резолюції 60/45 Генеральної Асамблеї ООН. За законодавством України СІО розглядається як різновид стратегічних комунікацій та форма воєнних дій. Останнє унеможливлює проведення СІО щодо громадян України (крім тих, які є членами терористичних угруповань та незаконних збройних формувань), а також на території України поза межами території, на якій введено правовий режим воєнного стану, району проведення антитерористичної операції або інших місць (районів) підготовки та застосування Збройних Сил.

6. На основі узагальнення вітчизняного досвіду проведення СІО, розкрито, що теоретико-методологічні засади інформаційного забезпечення СІО характеризуються розгалуженим інструментарієм, який може використовуватись як у військовий, так і у мирний час для різної цільової аудиторії. Взяття сектором безпеки і оборони України «на озброєння» методологічного інструментарію,

передбаченого стандартами НАТО, посилить спроможності нашої держави у веденні інформаційного протиборства в умовах гібридної війни.

7. Аналіз загроз інформаційній безпеці держави дозволив довести, що СІО в системі протидії загрозам національній безпеці України посідають особливе місце – як самостійний механізм реалізації заходів інформаційно-психологічного спрямування і як допоміжний напрям діяльності в реалізації політичних, економічних, військових та інших заходів, які без належної інформаційної підтримки приречені на неуспіх. СІО можуть реалізовуватись не лише при забезпечені інформаційної, але й інших складових національної безпеки, яка є складним та багатоаспектним феноменом.

8. Критичний аналіз національного законодавства, а також узагальнення пріоритетних напрямів розвитку системи інформаційної безпеки України, дозволили встановити, що основною проблемою правового забезпечення СІО є відсутність достатнього законодавчого унормування їх проведення, а відтак – і підґрунтя для розробки методологічних засад СІО. Це зумовлює потребу у законодавчому визначенні заборон при здійсненні інформаційного впливу, які визначатимуть межі проведення СІО з метою забезпечення дотримання конституційних прав і свобод громадян. Ефективне проведення СІО не лише в інтересах оборони, але в інтересах антитерористичної, антикримінальної, інформаційної та інших складових національної безпеки України зумовлює необхідність надання повноважень щодо проведення СІО Службі безпеки України з одночасним позбавленням її статусу військового формування. Аналогічні повноваження мають також бути надані і іншим суб’єктам сектору безпеки і оборони відповідно до їхньої компетенції. Необхідним є також нормативне закріплення визначення СІО на рівні закону, що надалі надасть можливість регламентувати на рівні підзаконних нормативно-правових актів порядок проведення СІО. З цією метою пропонується:

– у проекті Закону України Про внесення змін до Закону України “Про Службу безпеки України” та у проекті Закону України «Про розвідку» визначити серед функцій Служби безпеки України та розвідувальних органів «участь у забезпеченні загальнодержавної системи стратегічних комунікацій», передбачити серед повноважень Служби безпеки України наступне: «проводити спеціальні інформаційні операції; протидіяти проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій», а серед повноважень розвідувальних органів України – «проводити спеціальні інформаційні операції з метою сприяння реалізації національних інтересів України та протидії зовнішнім загрозам національній безпеці України у визначених законом сферах»;

– РНБО України за участю інших державних органів, що входять до складу сектору безпеки і оборони України, розробити загальнодержавну Концепцію стратегічних комунікацій, у якій закріпити наступне визначення СІО: «скоординоване і належне використання комунікативних можливостей держави з метою проведення розвідувальних або контррозвідувальних заходів, спрямованих

на досягнення стратегічних (оперативних) цілей в інформаційному просторі та просування цілей держави».

9. Виявлено, що сучасних умовах необхідним є формування синергетичної моделі СІО, призначеної для одночасного вирішення наступних завдань щодо цільової аудиторії: зміна ставлення до об'єкта/ дій; зміна поведінки; зміна світосприйняття та світоглядної картини (з одночасним унеможливленням досягнення аналогічних цілей іноземними державами, їх спецслужбами, окремими організаціями, спільнотами й особами, що діють на шкоду національній безпеці України тощо). Ця модель передбачає: використання підмереж (сенсорів; комунікацій; аналізу інформації; прийняття рішень; виконавчих вузлів); побудову матриці інформаційно-правового забезпечення (з урахуванням актуалізованої класифікації СІО за видом і типом); алгоритм реалізації (підготовчий етап; інформаційний етап; етап планування; етап реалізації запланованих заходів; етап виходу з СІО). Зазначена модель включає проведення СІО наступального, так і оборонного спрямування з використанням розгалуженої системи методів, а її застосування сектором безпеки і оборони України дозволить підвищити ефективність інформаційно-правового забезпечення СІО та їх результативність.

Також результати проведеного дисертаційного дослідження дозволяють дійти висновку про те, що до перспективних напрямів подальших наукових пошуків належить передусім подальший розвиток міжнародного інформаційного права, розробка загальнодержавної Концепції стратегічних комунікацій, а також методології проведення СІО, котра деталізуватиме розроблену в ході дослідження матрицю інформаційно-правового забезпечення синергетичної моделі СІО.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Верголяс О.О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право.* 2018. № 4. С. 126–133.

2. Верголяс О.О. Спеціальні інформаційні операції в системі засобів протидії загрозам національній безпеці України. *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки».* 2019. № 4. С. 7–16.

3. Верголяс О.О. Міжнародно-правове регулювання інформаційного протиборства: реалії та перспективи. *Visegrad Journal on Human Rights*. 2019. № 3. С. 58–63.

4. Верголяс О.О. Проблемні питання проведення спеціальних інформаційних операцій сектором безпеки і оборони України. *Юридичний науковий електронний журнал.* 2019. № 4. С. 102–105.

5. Верголяс О.О. Перспективи вдосконалення інформаційно-правового забезпечення спеціальних інформаційних операцій. *Підприємництво, господарство і право*. 2019. № 7. С. 135–139.

6. Верголяс О.О. Спеціальні інформаційні операції як інструмент геополітичних змін. *Юридичний бюлетень: наук. журн.* / редкол.: О. Г. Предместніков та ін. Одеса: ОДУВС, 2019. Вип. 9 (9). С. 16–23.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Верголяс О.О. Перспективи криміналізації статті 173-1 кодексу України про адміністративні правопорушення. *Информационные технологии и безопасность. ИТБ-2015:* материалы XV Международной научно-практической конференции. Киев, 21.10.2015 г. / ИПРИ НАН Украины. Киев, 2015. С. 42–46.

8. Верголяс О.О. Стандарти НАТО у сфері проведення спеціальних інформаційних операцій. *Юридична наука: виклики і сьогодення:* матеріали Міжнародної науково-практичної конференції. Одеса, 7–8 червня 2019 р. Одеса, 2019. С. 72–76.

9. Верголяс О.О. Спеціальні інформаційні операції у веденні інформаційної війни. *Legal practice in EU countries and Ukraine at the modern stage:* International scientific and practical conference / Vasile Goldis Western University of Arad, Romania. January 25–26, 2019. Arad, 2019. С. 312–315.

АНОТАЦІЇ

Верголяс О.О. Правове забезпечення спеціальних інформаційних операцій. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Науково-дослідний інститут інформатики і права Національної академії правових наук України, Київ, 2020.

У дисертації проведено комплексне наукове дослідження з проблематики правового забезпечення спеціальних інформаційних операцій, а також розробленні рекомендації щодо їх вдосконалення. Проаналізовано ґенезу та сучасний стан наукових поглядів на проблеми інформаційного протиборства, проведення спеціальних інформаційних операцій та інформаційно-правового забезпечення їх проведення. Виявлено специфіку спеціальних інформаційних операцій у веденні інформаційної війни та забезпечені національної безпеки, визначено місце спеціальних інформаційних операцій в системі заходів протидії загрозам національній безпеці України. Окреслено методологічні засади дослідження проблематики правового забезпечення спеціальних інформаційних операцій, а також організаційно-правові засади проведення спеціальних інформаційних операцій та теоретико-методологічні засади інформаційного забезпечення їх проведення. В роботі також аналізуються актуальні проблеми правового та інформаційно-правового забезпечення спеціальних інформаційних операцій в Україні на сучасному етапі та визначаються шляхи їх подолання. Зокрема, розроблено алгоритм проведення спеціальних інформаційних операцій з урахуванням сучасних реалій гібридної війни та актуальних стандартів НАТО, актуалізовано класифікацію спеціальних інформаційних операцій за типом та видом. Запропонована класифікація спеціальних інформаційних операцій, а також системний підхід до їх планування та підготовки на базі відповідного алгоритму, слугують підґрунтям для побудови матриці інформаційно-правового забезпечення синергетичної моделі спеціальних інформаційних операцій, застосування якої складовими сектору безпеки і оборони України дозволить підвищити ефективність

правового та інформаційно-правового забезпечення спеціальних інформаційних операцій та сприятиме підвищенню їх результативності.

Ключові слова: інформаційна безпека, інформаційна війна, інформаційна зброя, спеціальні інформаційні операції, інформаційно-правові засади, правове забезпечення спеціальних інформаційних операцій.

Верголяс А.А. Правовое обеспечение специальных информационных операций. – Рукопись.

Диссертация на соискание ученой степени кандидата юридических наук по специальности 12.00.07 - административное право и процесс; финансовое право; информационное право. – Научно-исследовательский институт информатики и права Национальной академии правовых наук Украины, Киев, 2020.

В диссертации проведено комплексное научное исследование по проблематике правового обеспечения специальных информационных операций, а также разработка на основании результатов такого исследования рекомендаций по усовершенствованию правового и информационно-правового обеспечения специальных информационных операций. Проанализированы генезис и современное состояние научных взглядов на проблемы информационной безопасности, информационного противоборства, специальных информационных операций и информационно-правового обеспечения специальных информационных операций. На основе выявления специфических признаков специальных информационных операций и информационно-правового обеспечения специальных информационных операций даны определения этих явлений, а также предложены оптимизированные определения информационной безопасности, информационной войны, информационных угроз. Рассмотрены сущностные особенности информационного оружия, которое представляет собой целенаправленное использование информации. Выявлена специфика специальных информационных операций при ведении информационной войны и обеспечении национальной безопасности, определено место специальных информационных операций в системе мер противодействия угрозам национальной безопасности. Так, в системе мер противодействия угрозам национальной безопасности специальные информационные операции занимают особое место – как самостоятельный механизм реализации мер информационно-психологической направленности и как вспомогательное мероприятие в реализации политических, экономических, военных и других мер, которые без надлежащей информационной поддержки обречены на провал. Специальные информационные операции могут реализовываться не только при обеспечении информационной безопасности, но и при обеспечении других составляющих национальной безопасности, которая является сложным и многоаспектным феноменом. Обозначены методологические основы исследования проблематики информационно-правового обеспечения специальных информационных операций, а также организационно-правовые основы проведения специальных информационных операций и теоретико-методологические основы информационного обеспечения их проведения.

В работе также анализируются актуальные проблемы правового обеспечения специальных информационных операций в Украине на современном этапе и предлагаются пути их преодоления, в т.ч. вносятся конкретные рекомендации по усовершенствованию действующего законодательства и оптимизации алгоритма проведения специальных информационных операций.

Ключевые слова: информационная безопасность, информационная война, информационное оружие, специальные информационные операции, правовое обеспечение специальных информационных операций.

Vergolas O.O. Legal support of special information operations. – Manuscript.

Dissertation for the degree of a Candidate of Law in specialty 12.00.07 Administrative Law and Process; Finance Law; Information Law. – Scientific and Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine, Kyiv, 2020.

In the dissertation the complex scientific research on the issues of legal support of special information operations is carried out, as well as the development of recommendations for its improvement. The genesis and current state of scientific views on the problems of information confrontation, carrying out of special informational operations and information and legal support of their conduct are analyzed. The specifics of special information operationsas a tool for conducting information warfare and means of ensuring national security were revealed, the place of special information operations in the system of means of counteracting threats to national security of Ukraine was determined. The methodological principles of the study of the information and legal support of special information operations, as well as the organizational and legal principles of carrying out special information operations and the theoretical and methodological principles of information provision of their conduct are out lined. The dissertation also analyzes the actual problems of informational and legal support of special information operations in Ukraine at the present stage and identifies ways of overcoming them.

The algorithm of special information operations implementation taking into account the current realities of the hybrid war and the actual NATO standards is elaborated, also the classification of the special information operations has been apdated. The proposed classification of special information operations, as well as a systematic approach to the planning and preparation of special information operations based on the corresponding algorithm, serves as the basis for constructing the information and legal support matrix of a synergistic model of special information operations, the application of which components of the security and defense sector of Ukraine will increase the effectiveness of information and legal provision of special information operations and will increase their effectiveness.

Keywords: information security, information warfare, information weapon, special information operations, legal support of special information operations.

Гарнітура Таймс. Формат 60х84/16.
Наклад 100. Папір офсетний. Ум.-др. арк. 0,9.
Підписано до друку 21.01.2020. Замовлення 108.

Надруковано в «МП Леся».
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи серія ДК № 892 від 08.04.2002.
«МП Леся»
03148, Київ, а/с 115.
Тел./факс: (066) 60-50-199, (098) 455-41-17
E-mail: lesya3000@ukr.net