УДК 343.9:355.40:343.3

НЕТЕСА Н.В., *кандидат юридичних наук,* вчений секретар Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України.
ORCID: https://orcid.org/0000-0002-0567-4296.
МОКЛЯК В.В., *кандидат юридичних наук,* Служба безпеки України.
ORCID: https://orcid.org/0000-0003-1116-7167.

СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ПРОТИ УКРАЇНИ ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ ТА НАПРЯМИ ПРОТИДІЇ ЇМ

DOI…

***Анотація**. Розглядаються спеціальні інформаційні операції як елемент гібридної війни рф проти України. Формулюється авторське визначення спеціальних інформаційних операцій, визначаються вектори їх спрямування та види. Увага приділяється з'ясуванню можливих об'єктів інформаційного впливу, а також характеристиці засобів, методів та форм здійснення спеціальних інформаційних операцій. Констатується, що кримінальним законодавством України наразі охоплюється більшість форм розміщення та поширення інформації з деструктивним контентом, що становить зміст спеціальних інформаційних операцій, та висловлюються судження щодо деяких резервів для його подальшого вдосконалення. Робиться висновок, що оскільки спеціальні інформаційні операції є складною, багатоетапною системою заходів протидія їм має будуватися на комплексному підході, що передбачає три основні стратегічні напрями: 1) контррозвідувальні заходи спецслужб; 2) заходи із реалізації державної політики в інформаційній сфері; 3) заходи кримінально-правового характеру.*

***Ключові слова:** спеціальні інформаційні операції, інформаційна безпека, національна безпека, інформаційний простір, інформаційний вплив, гібридна війна, протидія спеціальним інформаційним операціям.*

***Summary.** The article is devoted to the consideration of special information operations as an element of Russia's hybrid war against Ukraine. The author's definition of special information operations is formulated, their vectors and types are determined. Special attention is paid to identifying possible objects of information influence, as well as characterizing the means, methods and forms of special information operations. In addition, it is stated that the criminal legislation of Ukraine currently covers most forms of posting and dissemination of information with destructive content which is the instrument of special information operations, and the author makes judgments on some reserves for its further improvement. It is concluded that since special information operations are a complex, multi-stage system of measures, counteraction to them should be based on a comprehensive approach that includes three main strategic areas: 1) counterintelligence measures of special services; 2) measures to implement the state policy in the information sphere; 3) criminal law measures.*

***Keywords:** special information operations, information security, national security, information space, information influence, hybrid warfare, countering special information operations.*

Постановка проблеми. Основним джерелом загроз інформаційній безпеці України в умовах гібридної війни є деструктивна діяльність спеціальних служб супротивника в інформаційному просторі. Останній, на відміну від зони військового збройного конфлікту, не має територіальних меж, а тому стає самостійною універсальною ареною протистояння, яка, враховуючи глобалізаційні світові процеси, відкриває фактично необмежені можливості для здійснення різнобічного впливу на внутрішню та зовнішню політику України з одночасним вирішенням державою-агресором власних геополітичних

задач, у тому числі у напрямі посилення позицій впливу на міжнародну спільноту. При цьому одним із найнебезпечніших проявів втручання в інформаційний простір, що визнається основним компонентом гібридної війни, є здійснення супротивником спеціальних інформаційних операцій, які (як зазначається в Стратегії інформаційної безпеки) спрямовані, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини [1]. Системність, багатофункціональність та комплексність як визначальні риси організації спеціальних інформаційних операцій перетворюють їх на потужну технологію інформаційного протиборства, яка дозволяє ефективно керувати суспільними процесами у різних сферах життєдіяльності – політики, економіки, психології, безпеки, оборони тощо. Виникає гостра потреба в об'єднанні зусиль науки, законотворчості, правозастосування, сил безпеки й оборони заради досягнення спільної мети – протидії агресору в інформаційному просторі, що на сьогодні є необхідною умовою здобуття переваг на полі реального бою і, врешті-решт, збереження української державності та ідентичності.

Результати аналізу наукових публікацій. Враховуючи дотичність тематики спеціальних інформаційних операцій до різних сфер суспільного життя, вона є предметом наукового інтересу дослідників різних галузей знань – політології, соціології, права, психології, економіки, комп'ютерних наук тощо. Більший досвід у розглядуваній царині мають зарубіжні фахівці, серед яких Дж. Л. Едгар (J.L. Edgar) [2], Дж. Арквілла (J. Arquilla), Д. Ронфельдт (D. Ronfeldt) [3], С.-Д. Бахманн (S-D Bachmann), Х. Гуннеріусон (H. Gunneriusson) [4], Ж. Най (J. Nye) [5], Б. Шнайєр (B. Schneier) [6] та ін. Щодо вітчизняних досліджень, то деякий час питання спеціальних інформаційних операцій здебільшого розглядалося у контексті реформування сектору безпеки й оборони, а переважна більшість наукових розробок стосувалися правової регламентації планування, організації та провадження заходів інформаційного протиборства. Слід відзначити внесок у розробку означених питань таких фахівців з інформаційної безпеки, як О.О. Верголяс [7], Д.В. Вєдєнєєв [8], О.Г. Заруба [9], Ю.І. Когут [10], О.М. Лебедєв [11], О.В. Литвиненко [12], В.А. Ліпкан [13], В.Я. Новицький [14], В.М. Панченко [15], О.П. Дзьобань, В.Г. Пилипчук [16], В.М. Фурашев, Д.В. Ланде [17] та ін.

Водночас слід визнати, що наукові розвідки у цьому напрямі наразі перебувають ще на початковому етапі, обмежуючись здебільшого викладенням окремих аспектів цієї проблематики. У нових воєнно-політичних реаліях, зумовлених трансформацією прихованої інформаційної агресії рф проти України у її відкриту форму, поєднану з конвенційною агресією, потужного імпульсу набуває потреба в дослідженні явища спеціальних інформаційних операцій саме як загрози інформаційній безпеці з виробленням науково обґрунтованих стратегічних напрямів протидії їм.

Метою статті є визначення характеристик спеціальних інформаційних операцій як деструктивного соціального явища в умовах гібридної війни рф проти України шляхом визначення понять, векторів спрямування, видів, можливих об'єктів інформаційного впливу, засобів та форм здійснення, а також з'ясування наявного потенціалу кримінального законодавства щодо забезпечення інформаційної безпеки та на підставі цього визначення комплексу заходів протидії їм.

Виклад основного матеріалу. З огляду на те, що національна безпека є складним, багатоаспектним феноменом, спрямовані проти неї ворожі спеціальні інформаційні операції можуть мати різне призначення. Якщо ідеться про інформаційну складову

національної безпеки, то тут вони виступають основним засобом інформаційної агресії. В умовах зростання ролі інформації у різних сферах суспільного життя спеціальні інформаційні операції нерідко виконують роль допоміжного засобу в реалізації й інших заходів – економічних, політичних, військових тощо, що зумовлює необхідність ефективної протидії, як однієї із першочергових завдань у сфері національної безпеки.

На теперішній час окремі аспекти протидії проведенню проти України спеціальних інформаційних операцій закріплені в низці документів стратегічного характеру, серед яких Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.20 р. № 392/2020 [18], Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.21 р. № 685/2021 [1], Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.21 р. № 447/2021 [19], Стратегія воєнної безпеки України, затверджена Указом Президента України від 21.03.21 р. № 121/2021 [20], Стратегія забезпечення державної безпеки, затверджена Указом Президента України від 16.02.22 р. № 56/2022 [21], а також прийняті на їх реалізацію плани заходів: План реалізації Стратегії кібербезпеки України, введений в дію Указом Президента України від 01.02.22 р. № 37/2022 [22], План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, затверджений розпорядженням Кабінету Міністрів України від 30.03.23 р. № 272-р [23], План заходів із реалізації Стратегії забезпечення державної безпеки, затверджений Розпорядженням Кабінету Міністрів України від 18.04.23 р. № 318-р [24], відомчі нормативно-правові акти органів СБУ та ін.

Втім, жоден із цих документів не містить легального визначення спеціальних інформаційних операцій та не надає чіткого уявлення про їх сутність.

Зазначимо, що *спеціальні інформаційні операції* переважно розглядаються як елемент (інструмент) інформаційного протиборства [7, с. 128], яке сучасною воєнною доктриною визначається трьома основними компонентами:

1) інформаційно-психологічна війна;

2) інформаційно-технологічний вплив (проведення кібератак, втручання в діяльність електронних ресурсів органів державної влади тощо);

3) операції із захисту власного інформаційного простору від зовнішніх інформаційних операцій.

Наведене дає підстави погодитися з тезою про те, що специфікою організації спеціальних інформаційних операцій є застосування сучасних технологій та психологічних методик, які у поєднанні з можливостями сил безпеки й оборони можуть викликати значний суспільний резонанс [11, с. 155-156].

З урахуванням викладеного та спираючись на наявні доктринальні дефініції й положення відомчих нормативно-правових актів СБУ, спеціальні інформаційні операції можуть бути визначені як система взаємозалежних, багатоетапних, об’єднаних єдиним оперативним задумом гласних та негласних заходів, змістом яких є приховане керування процесами інформаційної сфери супротивника з одночасним посиленням забезпечення безпеки власної інформаційної сфери, кінцевою метою яких є маніпулювання масами на рівні суспільної та індивідуальної свідомості.

Спеціальні інформаційні операції, що проводяться спецслужбами рф проти України, мають декілька векторів спрямування таких, що:

1) здійснюються у власному інформаційному просторі рф (внутрішні спецоперації);

2) розраховані на інформаційних простір інших країн та міжнародних організацій (зовнішні спецоперації);

3) розраховані на інформаційній просторі анексованих та окупованих територій.

Розглянемо їх докладніше.

Внутрішні спеціальні інформаційні операції передбачають інформаційний вплив на власне населення рф і спрямовані на: інспірування ідей про можливий наступ США та НАТО з боку українських територій з метою посіяти паніку серед населення рф; мобілізацію бойового духу власних громадян та отримання підтримки широких верств населення шляхом демонстрації нібито досягнутих здобутків "визвільної" спецоперації в Україні та виправдовування в їх очах збройного вторгнення на територію суверенної України, зокрема, начебто боротьбою з фашизмом; укріплення духу патріотизму; придушення будь-яких опозиційних та протестних настроїв; навіювання остраху суворого покарання за ухилення від мобілізації.

Зовнішні спецоперації інформаційного впливу, що здійснюються за межами власного інформаційного простору держави-агресора, можуть бути поділені на дві підгрупи: здійснювані в інфопросторі країни, яка зазнає безпосередньої агресії (у наш час – в Україні), та здійснювані в інфопросторі третіх країн світу, які не є сторонами збройного протиборства, але які в умовах глобалізації можуть істотним чином впливати на його результат.

Спецоперації в інфопросторі України здебільшого спрямовані на: підрив обороноздатності та деморалізацію особового складу Збройних Сил України, а також представників силового блоку з правоохоронними функціями; зниження стійкості українського суспільства до деструктивних інформаційних впливів; активізацію панічних настроїв у суспільстві, зокрема, шляхом доведення до громадськості завідомо неправдивої або тенденційно оформленої інформації щодо перебігу бойових дій на різних ділянках фронту, готовності до "капітуляції" з боку окремих представників влади та військового керівництва ЗС України; загострення і дестабілізацію суспільно-політичної ситуації в Україні, в тому числі на ґрунті міжетнічних, мовних, релігійних та інших протиріч; дестабілізацію соціально-економічної ситуації в нашій державі; провокування проявів сепаратизму, екстремізму, тероризму; інші інформаційні впливи, кінцевою метою яких є підрив національної безпеки України та її національних інтересів, ліквідація української державності та знищення української ідентичності.

Дещо інше призначення мають зовнішні спеціальні інформаційні операції проти України, що здійснюються в інформаційному просторі зарубіжних країн (та міжнародних організацій). Ці інформаційні впливи здійснюються представниками російських спецслужб переважно за такими напрямами: виправдовування перед світовою спільнотою військової агресії проти України; намагання всіляко дискредитувати політичне та військове керівництво нашої держави в очах міжнародних партнерів, які задіяні у наданні Україні військової та гуманітарної допомоги, шляхом поширення недостовірної інформації у російських та підконтрольних іноземних ЗМІ щодо "нецільового використання" наданої допомоги; активне звинувачення ЗС України у вчиненні воєнних злочинів проти "мирного" населення на тимчасово окупованих територіях (обстріли житлових будинків, об'єктів критичної інфраструктури, замовні вбивства "законно обраних" представників влади псевдоадміністрацій тощо); формування серед населення країн-партнерів України антиукраїнського світогляду, нав'язування їм нових цінностей "руського миру", кінцевим завданням яких є зміна вектору стосунків з нашою державою; створення інформаційних передумов для ускладнення реалізації реформ та програм розвитку України у контексті євроінтеграції (насамперед, блокування вступу до ЄС та НАТО); посилення адвокаційної кампанії за зняття санкцій, запроваджених щодо рф санкцій у зв'язку з порушенням нею суверенітету й територіальної цілісності України. У науковій літературі такі спеціальні інформаційні операції стосуються як дружніх супротивнику країн, так і тих, які налаштовані нейтрально чи навіть вороже [9, с. 82].

Наприклад, щодо країн-партнерів України, які надають їй військову допомогу, застосовуються інформаційні спецоперації, змістом яких є дискредитація українського військово-політичного керівництва та ЗС України, які начебто не здатні опанувати надану військову зброю і швидко її втрачають на полі бою чи взагалі перепродають, з одночасним демонструванням власної "могутності" та можливості завдання удару у відповідь у разі, наприклад, втручання в конфлікт, або ж шантажування застосуванням ядерної зброї (тактичної чи стратегічної).

Отже, головне призначення цього виду зовнішніх спеціальних інформаційних операцій – це "інформаційне виснаження" світової та міжнародної спільноти з тим, щоб вони припинили підтримувати Україну та почали чинити тиск на український уряд, підштовхуючи його до перемовин на вигідних кремлю умовах.

І, нарешті, третій вид спеціальних інформаційних операцій, який заслуговує на окремий розгляд, – це *спецоперації на анексованих та окупованих українських територіях,* де поєднуються засоби й методи зовнішнього та внутрішнього інформаційного впливу. Їх головним призначенням є поширення серед населення таких територій сепаратистських, автономістських, екстремістських та терористичних настроїв, навіювання думки про їх звільнення від "українських фашистів", загострення соціальних та ідеологічних протиріч між населенням цих територій та територій, підконтрольних Україні, та, врешті-решт, їх залучення до збройного протистояння на боці рф заради утвердження нібито соціальної та історичної справедливості.

Спеціальні інформаційні операції можуть бути класифіковані й за іншими критеріями.

Так, за характером здійснення вони можуть поділятися на *інформаційно-технологічні*, що передбачають вплив на функціонування інформаційно середовища суспільства (інформаційно-комунікаційні, електронно-комунікаційні щодо засобів та систем електронні комунікаційних мереж) та *інформаційно-психологічні,* що передбачають вплив на функціонування й розвиток інформаційно-психологічного середовища суспільства, психіку й поведінку окремих осіб та їх груп [7, с. 129].

Прикладом першого виду спеціальних інформаційних операцій є вчинення кібератак на інформаційну інфраструктуру.

Щодо другого їх виду – інформаційно-психологічних операцій, то вони передбачають різноманітний вплив на свідомість і навіть підсвідомість (в тому числі емоційно-вольову сферу) невизначеного кола осіб та встановлення контролю над ними, а відповідно, є достатньо складними за своєю структурою. Вони спрямовані на реалізацію геноцидних планів рф щодо України, що полягають в ураженні національної свідомості українців шляхом формування викривленої оцінки реальних подій (починаючи ще з 2014 року) та виправдовування збройної агресії з кінцевою метою знищення української ідентичності та державності.

Нерідко спеціальні інформаційно-технічні операції виступають засобом вчинення інформаційно-психологічних спецоперацій, що дає нам підстави говорити про існування так званих кібер-інформаційних впливів. Можна навести широке застосування російськими спецслужбами напередодні та в перші тижні повномасштабного вторгнення в Україну такого прийому, як злам медійних веб-сайтів для подальшого розміщення на них інформації впливу та її поширення через численні Інтернет-платформи (у тому числі російськомовні веб-сайти, Інтернет-форуми, блоги тощо).

Об'єктами впливу при здійсненні спеціальних інформаційних операцій найчастіше виступають: вище військово-політичне керівництво (Президент України, Прем'єр-Міністр України та члени Кабінету Міністрів України, Головнокомандувач ЗС України та інші

високопосадовці); військовослужбовці (від вищого офіцерського до рядового складу ЗС України); представники силового блоку з правоохоронними функціями (співробітники СБУ, МВС, Національної поліції, Державної прикордонної служби України та ін.); представники добровольчих військових формувань (зокрема, батальйонів територіальної оборони ЗС України, добровольчих батальйонів Нацгвардії України та патрульної служби поліції особливого призначення та ін.); цивільне населення; окремі цільові групи (етнічні, релігійні меншини, опозиційні групи, бізнесмени тощо).

Залежно від характеристик цільової аудиторії (вік, рівень освіти та медіаграмотності, рід занять, доступність сучасних інформаційно-комунікаційних технологій, тип місцевості та сфера, де здійснюється деструктивна інформаційна діяльність, тощо) [25, с. 208] обираються способи (деморалізація, дискредитація, маніпуляція та ін.), інструментарій (дезінформація, пропаганда, залякування) та засоби впливу на відповідну аудиторію. Останні передбачають використання достатньо широкого арсеналу: від традиційних, давно усталених та перевірених часом і практикою застосування друкованих засобів (листівки, газети, брошури), радіомовлення, телебачення (в тому числі аналогове, цифрове, супутникове), використання можливостей публічної дипломатії, залучення експертів та лідерів громадської думки до новітніх технологій та можливостей мережі Інтернет (проведення кібератак, використання соціальних мереж та мессенджер-каналів, створення спеціальних блог-платформ та інформаційних майданчиків, користування послугами SMM/SEO-маркетингу для просування інформації з деструктивним контентом у пошукових системах та соціальних мережах з метою нарощування їх рейтинговості та значимості в інформаційному просторі та ін.).

Що стосується найпоширеніших форм здійснення спеціальних інформаційних операцій проти України, то можна виокремити такі їх прояви:

- збір та передавання ворогу даних про військові об’єкти, об’єкти критичної інфраструктури (зокрема в частині проведення та подальшого підтвердження результатів ракетних атак на них), розташування логістичних вузлів, обсягів та видів наданої Україні партнерами військової допомоги та ін.;
- розміщення та поширення матеріалів деструктивного та антидержавницького характеру, проросійського контенту, в тому числі шляхом підміни понять та вживання “токсичних” слів (як-от: замість “українська влада” – “режим Зеленського”, “український режим”, “київський режим”, “фашистський режим”; замість “війна” – “військова спецоперація”, “український конфлікт”, “українська криза” тощо);
- поширення закликів до повалення конституційного ладу або посягань на територіальну цілісність України;
- DDoS-атаки, злам спеціалізованих баз даних, веб-сайтів та інформаційних ресурсів;
- організація або провокування публічного обговорення питань, які викликають панічні настрої, загострюють соціальні протиріччя, викривляють погляди на перебіг бойових дій на окремих територіях України.

Викладене дає підстави зазначити, що спеціальні інформаційні операції завжди плануються й організовуються спецслужбами іноземної держави, але з опорою на наявні оперативні позиції й можливості в країні, де ці спецоперації проводяться [14, с. 115], що свідчить про те, що безпосередні виконавці більшості вище вказаних форм суспільно небезпечних діянь перебувають на території України, а отже, до них можуть бути застосовані відповідні заходи протидії, в тому числі кримінально-правові.

Оцінюючи наявний потенціал кримінального законодавства України в частині протидії спеціальним інформаційним операціям, можна констатувати, що в цілому він є

прийнятним. Так, за збір та передавання "чутливої" інформації передбачено кримінальну відповідальність у низці статей КК України, зокрема, ст. 111 ("Державна зрада"), ст. 114 ("Шпигунство"), ст. 114^2 ("Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану") та ін. Так само вже охоплено приписами КК України поширення закликів до повалення конституційного ладу або посягань на територіальну цілісність України (ч. 2 та ч. 3 ст. 109, ст. 110 КК України), а також більшість форм розміщення та поширення інформації деструктивного й антидержавницького характеру (зокрема, окремі форми колабораційної діяльності, передбачені частинами 1, 3, 6 ст. 111^1 КК України; пропаганда війни (ст. 436 КК України), діяння, передбачені статтями 436^1, 436^2 КК України, ч. 2 ст. 442 КК України та ін.).

КК України України містить окремий Розділ XVI "Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку", а також передбачає засоби реагування на діяння, що спрямовані на загострення соціальних протиріч (зокрема, розпалювання національної, регіональної, расової чи релігійної ворожнечі та ненависті, приниження національної честі, гідності (ст. 161 КК України), тощо.

Незважаючи на це є певний резерв для подальшого вдосконалення вітчизняного кримінального законодавства в частині протидії проведенню проти України спеціальних інформаційних операцій. Вже давно обговорюється питання щодо доцільності запровадження кримінальної відповідальності за умисне систематичне поширення дезінформації, принаймні з питань національної безпеки, територіальної цілісності, суверенітету й обороноздатності нашої країни, права українського народу на самовизначення та ін. [26, с. 11; 27, с. 235]. Крім того, як убачається, одним з ефективних заходів протидії інформаційній агресії, з технологічної точки зору, є обмеження можливості потрапляння в інфопростір України ворожої дезінформації та деструктивної пропаганди шляхом блокування в Україні доступу до інформаційних ресурсів, на яких розміщується інформація з деструктивним контентом. І хоча правова підстава для цього нібито є (низка рішень РНБО "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", уведених у дію Указами Президента України починаючи з Указу від 15.05.17 р. № 133/2017, якими в межах реалізації обмежувальних заходів щодо фізичних та юридичних осіб передбачається, серед іншого, заборона користування радіочастотним ресурсом України, обмеження або припинення надання телекомунікаційних послуг і використання телекомунікаційних мереж загального користування, інші санкції, що відповідають встановленим законом принципам їх застосування, зокрема і блокування Інтернет-провайдерами доступу до веб-ресурсів), проте є провайдери, які всупереч покладеним на них обов'язкам продовжують безкарно надавати доступ до підсанкційних інформаційних ресурсів. Певною мірою така ситуація пояснюється правовою невизначеністю порядку обмеження доступу до інформації з деструктивним контентом, а також підстав і механізму притягнення до відповідальності суб'єктів, які залучаються до забезпечення виконання обмежувальних заходів.

Убачається, що в умовах війни такі форми пособництва ворогу в інформаційній, економічній та інших сферах потребують передбачення адекватного реагування, яким, на наш погляд, є встановлення кримінальної відповідальності за умисне невиконання спеціальних економічних та/або інших обмежувальних заходів (санкцій), що дозволить притягати до відповідальності в тому числі Інтернет-провайдерів. До речі, відповідний

законопроєкт “Про внесення змін до Кримінального та Кримінального процесуального кодексів України та інших законів щодо встановлення кримінальної відповідальності за порушення законодавства про санкції” вже зареєстрований на сайті Верховної Ради України (реєстр. № 8384 від 25.01.2023 р.) [28]. І хоча досі виникає чимало запитань про можливий обсяг криміналізації форм порушення вимог законодавства про санкції, які пропонується закріпити у проєктованій ст. 111^3 КК України, потребу в зазначенні в законі спеціальної мети, доцільність передбачення спеціальних видів звільнення від кримінальної відповідальності за такі діяння тощо, запровадження такої норми є вкрай необхідним у світлі забезпечення захисту інформаційного простору України.

Не применшуючи значення кримінально-правового забезпечення протидії спеціальним інформаційним операціям проти України, слід констатувати, що ключова роль у цій справі має відводитися ефективній контррозвідувальній діяльності вітчизняних спецслужб, спрямованій на ідентифікацію спеціальних інформаційних операцій супротивника та викриття його спроб впливати на громадську думку, а отже, й на суспільні процеси в Україні, а також заходам із реалізації державної політики у сфері інформаційної безпеки, спрямованим на підвищення інформаційної стійкості суспільства й держави та посилення національно-державницької ідеології (створення та розвиток ефективної системи стратегічних комунікацій, підвищення рівня інформаційної гігієни та соціальної відповідальності за поширення інформації з деструктивним контентом, розвиток української громадянської ідентичності, забезпечення інформаційної реінтеграції населення тимчасово окупованих територій до загальноукраїнського інформаційного простору та ін.).

Висновки.

Спеціальні інформаційні операції є основною формою реалізації компонентів інформаційного протиборства, що належать до виключної компетенції сил безпеки й оборони. Маючи різні вектори спрямування (внутрішні, зовнішні, здійснювані на окупованих та анексованих територіях), відрізняючись за характером здійснення, об’єктами впливу, засобами, способами, методами та формами проведення, спеціальні інформаційні операції характеризуються комплексністю та системністю їх здійснення, що забезпечується за рахунок їх планування та реалізації у межах єдиного оперативного задуму та спільного стратегічного наративу з кінцевою метою керування суспільними процесами у різних сферах життєдіяльності. Така специфіка організації спеціальних інформаційних операцій та їх багатозадачність зумовлює потребу у застосуванні комплексного підходу до протидії їм. Останній, як убачається, має передбачати три основні блоки заходів, що відбивають стратегічні напрями такої протидії:

1) контррозвідувальні заходи, спрямовані на захист інтересів держави в інформаційній сфері (діяльність спецслужб);

2) заходи із реалізації державної політики у сфері інформаційної безпеки, насамперед із забезпечення інформаційної стійкості українського суспільства та держави;

3) заходи кримінально-правового характеру у вигляді встановлення кримінальної відповідальності за різні прояви суспільно небезпечних діянь проти національної безпеки в інформаційному просторі.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року “Про Стратегію інформаційної безпеки”: Указ Президента України від 28.12.21 р. № 85/2021. URL: https://www.president.gov.ua/documents/6852021-41069

2. Edgar Jeffry L. The Role of Special Operations Forces in Information Warfare: Enablers, Not Cyber Warriors. Newport: Naval War College, 2000. 27 p. URL: https://efaidnbmnnnibpcajpcglclefindmkaj/ https://apps.dtic.mil/sti/pdfs/ADA381914.pdf

3. Arquilla J., Ronfeldt D. The Emergence of Noopolitik: Towards an American Information Strategy. RAND/MA-103305D. 1999. 102 p.

4. Bachmann S-D, Gunneriusson H. Hybrid Wars: The 21st Century's New Threats to Global Peace and Security. *Scientia Militaria. South African Journal of Military Studies.* Vol 43. No. 1. 2015. Pp. 77-98. URL: https://ung.edu/institute-leadership-strategic-studies/_uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientia-militaria.pdf

5. Nye J. Soft Power: The Means to Success in World Politics. New York: Public Affairs Group, 2004. 192 p.

6. Schneier B. Secrets and Lies: Digital Security in a Networked World. Wiley; 15th Anniversary edition. 2015. 450 p.

7. Верголяс О.О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право*. № 4(27)/2018. С. 126-133.

8. Вєдєнєєв Д., Левченко С., Сегеда С. Організаційно-правове структурування системи протидії загрозам в інформаційно-психологічній сфері України: тези Всеукр. наук.-практ. конф. *Актуальні проблеми правоохоронної діяльності в умовах воєнного стану,* м. Хмельницький, 16 бер. 2023 р. Хмельницький: Вид-во НАДПСУ, 2023. С. 334-337.

9. Заруба О.Г. Планування спеціальних інформаційних операцій. *Інформаційна безпека людини, суспільства, держави*. 2017. № 1(21). С. 140-154.

10. Когут Ю.І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології): практ. посіб. Київ: Консалт. компанія "СІДКОН"; ВД "Дакор", 2022. 284 с.

11. Лебедєв О. Деструктивний інформаційний вплив як елемент інформаційної війни проти України: тези Всеукр. наук.-практ. конф. *Актуальні проблеми правоохоронної діяльності в умовах воєнного стану,* м. Хмельницький, 16 бер. 2023 р. Хмельницький: Вид-во НАДПСУ, 2023. С. 155-157.

12. Литвиненко О.В. Спеціальні інформаційні операції та пропагандистські кампанії: монографія. Київ: Сатсанга, 2000. 222 с.

13. Ліпкан В.А. Сучасний зміст інформаційних операцій проти України. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102(1). С. 34-43.

14. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. № 1(40)/2022. С. 111-118.

15. Панченко В.М. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. *Інформація і право*. № 3(12)/2014. С. 13-16.

16. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти: монографія / за заг. ред. проф. В.Г. Пилипчука. Харків: Майдан, 2011. 244 с.

17. Фурашев В.М., Ланде Д.В. Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів. *Правова інформатика*. № 2(22)/2009. С. 49-57.

18. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.20 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

19. Про рішення Ради безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

20. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 21.03.21 р. № 121/2021. URL: https://www.president.gov.ua/documents/1212021-37661

21. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки": Указ Президента України від 16.02.22 р. № 56/2022. URL: https://www.president.gov.ua/documents/562022-41377

22. План реалізації Стратегії кібербезпеки України: Указ Президента України від 01.02.22 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

23. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30.03.23 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text

24. Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: Розпорядження Кабінету Міністрів України від 18.04.23 р. № 328-р. URL: https://zakon.rada.gov.ua/laws/show/328-2023-%D1%80#Text

25. Нетеса Н.В. Пропаганда як форма інформаційного впливу в умовах гібридної війни: тези Всеукр. наук.-практ. конф. *Актуальні проблеми правоохоронної діяльності в умовах воєнного стану,* м. Хмельницький, 16 бер. 2023 р. Хмельницький: Вид-во НАДПСУ, 2023. С. 207-210.

26. Батиргареєва В.С. Модернізація кримінально-правової охорони інформаційного простору України. *Питання боротьби зі злочинністю*: зб. наук. пр. / редкол.: В.С. Батиргареєва та ін. Харків: Право, 2022. Вип. 43. С. 11-23.

27. Павленко Т.А. Інформаційна безпека та протидія дезінформації в умовах збройної агресії рф проти України: матеріали VI міжнар. наук.-практ. конференції *Кримінально-правова охорона інформаційної безпеки,* м. Харків, 12 трав. 2022 р. / редкол.: Л.М. Демидова (голов. ред.) та ін. – (НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України; Нац. юрид. ун-т ім. Ярослава Мудрого; громад. організація “Всеукраїнська асоціація кримінального права”). Харків: Право, 2022. С. 233-235.

28. Про внесення змін до Кримінального та Кримінального процесуального кодексів України та інших законів щодо встановлення кримінальної відповідальності за порушення законодавства про санкції: проєкт Закону України (реєстр. № 8384 від 25.01.23 р.). URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41227

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~