УДК: 342.9
DOI https://doi.org/10.24144/2307-3322.2021.65.39

НАПРЯМИ ВДОСКОНАЛЕННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Верголяс О.О.,
к.ю.н., старший викладач кафедри права
Мелітопольський державний педагогічний університет
ім. Богдана Хмельницького
arnijazov@gmail.com
https://orcid.org/0000-0002-9780-1298

Верголяс О.О. Напрями вдосконалення правового забезпечення спеціальних інформаційних операцій

Стаття присвячена визначенню проблемних аспектів та перспектив вдосконалення інформаційно-правового забезпечення спеціальних інформаційних операцій (далі – СІО), адже наразі відсутнє достатнє нормативно-правове підґрунтя для розробки методологічних засад їх проведення. СІО в системі засобів протидії загрозам національній безпеці України посідають особливе місце як самостійний засіб реалізації заходів інформаційно-психологічного спрямування і як допоміжний засіб у реалізації політичних, економічних, військових та інших заходів. При цьому СІО можуть реалізовуватись під час забезпечення не лише інформаційного, але й інших складників національної безпеки, яка є складним та багатоаспектним феноменом. Оскільки спеціальні операції в цілому, в тому числі СІО, нині розглядаються за законодавством України як форма воєнних дій, фактично унеможливлюється проведення СІО захисного спрямування, в тому числі контррозвідувальних СІО на території України. Так, чинним законодавством не передбачено проведення СІО стосовно громадян України (крім тих, які є членами терористичних угруповань та незаконних збройних формувань), 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. Втім як розвідувальний, так і контррозвідувальний аспект СІО проявляється на всіх етапах СІО незалежно від їх спрямування, наступального або оборонного характеру. Тож питанням нагальної потреби є надання 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 в інтересах не лише оборони, але й антитерористичної, антикримінальної, інформаційної та інших складових частин національної безпеки України. Аналогічні повноваження мають також бути надані і розвідувальним органам України, а також іншим суб'єктам сектору безпеки і оборони відповідно до їхньої компетенції. Не менш важливим моментом є й власне нормативне закріплення визначення СІО на рівні закону та побудова сучасної моделі СІО та формування алгоритму проведення СІО.

Ключові слова: спеціальні інформаційні операції, інформаційний вплив, національна безпека, стратегічні комунікації, синергетична модель

Vergolyas O.O. Directions for improving the legal support of special information operations

The article is devoted to the definition of problematic aspects and prospects for improving the information and legal support of special information operations (hereinafter - SIO), because currently there is no sufficient legal basis for the development of methodological principles for their implementation. SIOs have a special place in the system of means of counteracting threats to the national security of Ukraine as an independent means of implementing information and psychological measures and as an auxiliary tool in the implementation of political, economic, military and other measures. At the same time, SIOs can be implemented while providing not only information, but also other components of national security, which is a complex and multifaceted phenomenon. As special operations in general, including SIOs, are now considered under Ukrainian law as a form of hostilities, it is virtually impossible to conduct SIOs of a protective nature, including counterintelligence SIOs on the territory of Ukraine. Thus, the current legislation does not provide for conducting SIOs against citizens of Ukraine (except for those who are members of terrorist groups and illegal armed groups), as well as conducting SIOs in Ukraine outside the territory

where martial law is imposed, outside the area of anti-terrorist operations or other places (areas) of training and use of the Armed Forces. However, both the intelligence and counterintelligence aspects of SIO are manifested at all stages of SIO, regardless of their direction, offensive or defensive nature. Therefore, the issue of urgent need is to provide the authority to conduct the SIO to the Security Service of Ukraine while depriving it of the status of a military formation, which will ensure compliance with the requirements of Art. 17 of the Constitution of Ukraine, as well as the effective conduct of SIO in the interests not only of defense but also of anti-terrorist, anti-criminal, information and other components of national security of Ukraine. Similar powers should also be given to the intelligence agencies of Ukraine, as well as to other entities of the security and defense sector in accordance with their competence. No less important is the actual normative consolidation of the definition of SIO at the level of law and the construction of a modern model of SIO and the formation of the algorithm for conducting SIO.

Keywords: special information operations, information impact, national security, strategic communications, synergetic model

Постановка проблеми. Якщо вести мову про напрями вдосконалення правового та інформаційно правового забезпечення СІО, слід зауважити, що їх розвиток залежить передусім від формування належного правового підґрунтя проведення СІО як на міжнародному рівні, так і на рівні національного законодавства. Зокрема, як вже зазначалося, існує потреба 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 законів, які забезпечують реалізацію конституційних прав та свобод.

Стан дослідження. Дослідженню проблематики СІО у своїх працях приділяли увагу Н. Іванова, Ю. Лапутіна, В. Ліпкан, О. Литвиненко, А. Марущак, Ю. Мороз, О. Морозов, В. Остроухов, В. Панченко В. Петрик, В. Пилипчук, Г. Почепцов, М. Присяжнюк, Є. Скулиш, І. Слюсарчук, М. Стрельбицький, Д. Фролов, М. Чеховська, М. Шилін та інші вітчизняні й зарубіжні науковці. Водночас актуальність цієї статті зумовлюється тим, що шляхи вдосконалення інформаційно-правового забезпечення СІО наразі окреслені не досить чітко.

Мета статті полягає у визначенні проблемних аспектів та перспектив удосконалення інформаційно-правового забезпечення спеціальних інформаційних операцій.

Виклад основного матеріалу. Крім того, у національному законодавстві необхідно наділити повноваженнями щодо проведення СІО не лише Збройні сили, але й інші структури, що входять до сектору безпеки і оборони відповідно до їх компетенції, що дозволить розширити потенційне коло об'єктів СІО та, відповідно, сферу застосування СІО з метою забезпечення національної безпеки. У першу чергу відповідними повноваженнями мають бути наділені Служба безпеки України та розвідувальні органи, адже СІО як спеціальні операції фактивно становлять сукупність узгоджених і взаємопов'язаних дій розвідувального та/або контррозвідувального спрямування, здійснюваних державними органами, що входять до складу сектору безпеки і оборони України, з використанням можливостей інформаційного простору та/або спрямованих на досягнення стратегічних (оперативних) цілей в інформаційному просторі, які проводяться за єдиним задумом самостійно або у взаємодії з іншими складовими сектору безпеки і оборони з метою забезпечення національної безпеки України. Не менш важливим моментом є й власне нормативне закріплення визначення СІО на рівні закону, що надалі надасть можливість розробити ефективну модель та алгоритм проведення СІО й закріпити його на рівні відомчих нормативно-правових актів. Отже, 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 як складової стратегічних комунікацій: «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 дозволять створити належне законодавче для інформаційно-правового забезпечення проведення СІО. Наступним кроком у вдосконаленні інформаційно-правового забезпечення СІО має стати оптимізація власне інформаційно-методичного забезпечення, в т.ч. визначення найбільш ефективних методів їх проведення. Зокрема, припускаючи, який саме комплекс заходів буде використовувати потенційний супротивник в ході військового конфлікту, терористичної або іншої протиправної акції, необхідно застосовувати такі засоби, які дозволяють блокувати його можливості, в тому числі: навмисне введення супротивника в оману відносно передбачуваних заходів і способів протидії загрозам національній безпеці; знищення засобів зв'язку й інформаційних систем супротивника; внесення умисних викривлень у роботу інформаційних систем супротивника; виявлення точок підтримки супротивника і їх знищення; одержання конфіденційної інформації про наміри супротивника і використання цих відомостей для формування стратегій захисту; використання засобів морально-психологічного пригнічення військ супротивника або інших засобів психологічного характеру, спрямованих на зміну ціннісних орієнтирів цільової аудиторії тощо. Своєю чергою, як вже зазначалося, визначення спектру методів проведення СІО залежатиме від обраної моделі СІО. Попередньо нами було констатовано необхідність розробки синергетичної моделі СІО, яка буде спрямовуватись на вирішення наступних основних завдань стосовно визначеної цільової аудиторії: зміни ставлення до певного об'єкта або дій; зміну поведінки; зміни світосприйняття та світоглядної картини (з одночасним унеможливленням досягнення щодо населення України аналогічних цілей іноземними державами, їх спецслужбами, окремими організаціями й спільнотами (а тому числі такими, що здійснюють терористичну або іншу злочинну діяльність), окремими особами, що діють на шкоду національній безпеці України тощо). Формування синергетичної моделі СІО доцільно здійснювати з використанням принципів тензорної методології. Зокрема, діакоптика як головна складова тензорної методології дозволяє ефективно досліджувати різноманітні складні системи (від електричних до біологічних) [1]. Піддаючи аналітичному розгляду кожну з них (в нашому випадку – виокремлені Г.Почепцовим традиційні моделі СІО), надалі можемо одержати загальний висновок за допомогою операції інтегрування [2, с.4] і змоделювати СІО комплексного характеру. СІО за таких умов розглядається як тензор, що не залежить від системи координат, тобто зміна системи координат тягне за собою перетворення його проекцій відповідно до лінійних законів, тож сконструйований таким чином алгоритм СІО буде придатний до застосування у будь-якій системі координат. Зокрема, використання принципів тензорної методології дозволить інтегрувати до синергетичної моделі проведення СІО досвід контрмережної боротьби. Так, контрмережну боротьбу як напрямок у розвитку оперативного мистецтва було закладено в основу концепції будівництва американських збройних сил «Єдина перспектива (Joint Vision) 2010» та «Єдина перспектива (Joint Vision) 2020», пов'язаної з трансформацією поглядів на характер загроз у новому столітті. Інформаційна мережа, яка може успішно використовується в ході СІО, складається із наступних підмереж: підмережа датчиків або ж сенсорів (ця підмережа забезпечує збір та аналіз вхідної інформації), підмережа комунікацій, яка забезпечує передачу інформації, підмережа аналізу інформації та підмережа вузлів прийняття рішень і підмережа виконавчих вузлів. Усі підмережі включають вузли, що працюють як з реальними, так і з віртуальними об'єктами. У сенсорній підмережі власне датчики можуть бути пасивними й активними, розташовуючись як у реальній, так і у віртуальній сфері бойового простору (простору забезпечення національної безпеки). Це ж стосується й підмережі виконавчих вузлів, яка включає традиційні засоби ураження (танки, літаки, зброя тощо), так і засоби впливу на цілі у віртуальному просторі: ЗМІ, комп'ютерні віруси, соціальні мережі тощо. Зауважимо, що ми розширюємо склад традиційних для концепції «мережної боротьби» підмереж з трьох до п'яти. Важливим аспектом контрмережної стратегії (як вже зазначалося, так само при проведенні СІО може використовуватись мережна стратегія – коли виконавці СІО діють децентралізовано, переймаючи при проведенні СІО методи мережевих організацій) проведення СІО в інтернет-просторі є залучення суб'єктами СІО (структурами сектору безпеки і оборони) інтернет-користувачів до участі у боротьбі з незаконним контентом та до сприяння у проведенні СІО в цілому, в тому числі з використанням краудсорсингу, тобто, створення «груп однодумців», задіяння недержавних медійних організації, рухів, лідерів суспільної думки тощо. До основних механізмів такого задіяння можна віднести наступні:

- створення та фінансування нових неурядових структур та ЗМІ для збирання та поширення контрольованої інформації щодо діяльності потенційних супротивників, проти яких спрямовується СІО;
- проведення журналістських розслідувань, першочергово, спрямованих на підготовку та оприлюднення матеріалів щодо проблематики, яка може використовуватись як успішний фон для проведення СІО (наприклад, щодо зловживань владою та корупційних діянь з боку представників державних органів, установ і підприємств у державах, з якими відбувається конфлікт, економічне чи інформаційне протистояння, або у власній державі, якщо СІО проводиться з метою протидії корупції, корупційному підживленню організованої злочинності тощо);

– залучення журналістів до реалізації масових акцій протесту, з метою дискредитації діяльності влади та власників ЗМІ у державах, з якими відбувається конфлікт, економічне чи інформаційне протистояння;
– здійснення за допомогою міжнародних та закордонних неурядових організацій дискредитації вищих органів влади у державах, з якими відбувається конфлікт, економічне чи інформаційне протистояння шляхом поширення публічних заяв і звернень щодо погіршення стану свободи слова, знищення «незалежних» ЗМІ, переслідування журналістів тощо;
– надання українськими журналістами організаційної підтримки знімальним групам іноземних ЗМІ для підготовки сюжетів, спрямованих на дискредитацію діяльності влади у державах, з якими відбувається конфлікт, економічне чи інформаційне протистояння, з подальшим їх оприлюдненням за кордоном;
– досягнення домовленостей з іноземними медійними структурами щодо взаємодії та підтримки, у разі перешкоджань законній журналістській діяльності; - використання вітчизняних журналістів для підготовки негативних матеріалів щодо суспільно-політичної, соціальної та інших ситуацій у державах, з якими відбувається конфлікт, економічне чи інформаційне протистояння з їх подальшим поширенням в іноземних ЗМІ;
– дискредитація діяльності загальнонаціональних телеканалів у державах, з якими відбувається конфлікт, економічне чи інформаційне протистояння, в контексті контрольованості їх інформаційної політики з боку влади та власників;
– просування «підконтрольних» журналістів до керівництва окремих політичних сил тощо.

Зауважимо, що здійсненню СІО наступального характеру сприятиме передусім наявність значної кількості інформаційних приводів для ефективного проведення цільових кампаній деструктивного впливу, що може бути зумовлено невирішеністю низки проблемних питань у соціальній, економічній та політичній сферах життєдіяльності у державах, з якими відбувається конфлікт, економічне чи інформаційне протистояння. Одночасно в ході проведення оборонних СІО зусилля мають спрямовуватись на протидію та блокування намірів представників іноземних урядових та не урядових структур, окремих радикальних громадсько-політичних організацій і об'єднань використати вітчизняні ЗМІ для дестабілізації і загострення суспільнополітичної обстановки в державі, зокрема, шляхом здійснення: - заходів, спрямованих на мінімізацію та нівелювання деструктивного інформаційного впливу закордонних та вітчизняних структур на розвиток політичної та соціально-економічної ситуації в країні, а також негативного інформаційного впливу на формування суспільної думки населення; -заходів з недопущення втручання проросійських та інших іноземних структур та їх місцевих сателітів у редакційну політику вітчизняних ЗМІ, створення механізмів деструктивного впливу для пропаганди сепаратизму, тероризму, посягання на державний суверенітет і територіальну цілісність України; - профілактично-роз'яснювальної роботи серед вітчизняних журналістів, які виїжджають у зону ООС або за кордон, зокрема в РФ, з метою виявлення спроб та намірів представників іноземних спецслужб або «спецслужб» самопроголошених республік залучити їх до протиправної діяльності (пропаганди сепаратизму, державної зради) тощо. Ефективність заходів, що застосовуються в ході проведення СІО, безпосередньо залежатиме в тому числі від їх відповідності наступним критеріям: - динамічність і гнучкість, постійне пристосування до умов безпекового середовища; - здатність змінювати власну інтерпретацію конкретного явища, аби більш ефективно його використати за мінливих обставин; - теми для «інформаційних спекуляцій» не повинні бути вигаданими, а виходити з питань і проблем, які існують в реальному житті; - базування на якісній розвідувальній інформації, на знанні політичних, соціальних, військових, економічних, побутових, духовних особливостей регіонів, соціальних груп (країни, народу) для яких вони призначені; - прихований характер заходів проведення СІО; - мережева стратегія реалізації; - використання «лавинного» ефекту (наприклад, перетворення споживачів пропагандистської інформації на її мимовільних поширювачів). В умовах сучасної гібридної (інформаційної) війни особливої ваги набуває також координація діяльності всіх складових сектору безпеки і оборони щодо проведення СІО, адже така координація дає можливість оперативно реагувати на інформаційні диверсії, передбачати майбутні інформаційні загрози для національного інформаційного простору, знаходити шляхи їх нейтралізації, забезпечувати достовірною інформацією громадян власної країни, у тому числі тих, які сьогодні перебувають під іноземним інформаційним впливом, забезпечуючи таким чином належне протистояння деструктивним СІО проти України. Вибір та реалізація конкретних заходів, необхідних для проведення СІО, має здійснюватись в рамках виконання алгоритму її проведення, який може буди розроблений на даному етапі нашого дослідження. Отже, з урахуванням сучасних реалій гібридної війни та актуальних стандартів НАТО пропонуємо виділяти наступні етапи проведення СІО (зміст окремих з ним різнитиметься залежно від того, чи мова йде про наступальну чи оборонну СІО, а також від того, який аспект притаманний СІО – розвідувальний чи контррозвідувальний):

– підготовчий етап;
– пошук/створення інформаційного приводу (інформаційний етап); - планування СІО;
– реалізація запланованих заходів; - закріплювальний етап («етап виходу» з СІО).

Підготовчий етап справедливо може вважатися найбільш значущим у контексті інформаційно-правового забезпечення проведення СІО. На даному етапі передусім необхідно вивчити правове підґрунтя та законодавчі заборони щодо проведення СІО, попередньо визначити суб'єктний склад, потенційних об'єктів (в т.ч. мова йде й про об'єкти інформаційного впливу) та мету проведення СІО (деталізація цих напрацювань далі відбуватиметься на стадії планування СІО). Також необхідно дослідити безпекове середовище з урахуванням внутрішніх та зовнішніх загроз національній безпеці. Задля аналізу безпекового середовища може бути використана, зокрема, методика SWOT-аналізу, яка передбачає здійснення огляду безпекового середовища через його сильні сторони, слабкі сторони, можливості та загрози.

Огляд безпекового середовища проведення СІО з використанням SWOT-аналізу Аналіз внутрішніх факторів Аналіз зовнішніх факторів Сильні сторони Strengths S Слабкі сторони Weaknesses W Можливості Opportunities O Загрози Threats T Для забезпечення якісного аналізу безпекового середовища шляхом виявлення його сильних і слабих сторін, загроз та можливостей, які матимуть значення при проведенні СІО доцільно:

– провести аналіз розвідувальних матеріалів, матеріалів контррозвідувальних та оперативно-розшукових справ тощо (залежно від спрямування СІО та органів, що входять до складу сектору безпеки і оборони, які ініціюють або безпосередньо залучаються до проведення СІО;
– здійснити моніторинг ЗМІ та інтернет-ресурсів з питань проблематики, яка визначає спрямування та інформаційний фон СІО;
– вивчити напрацювання та думки неурядових інформаційноаналітичних центрів щодо пріоритетів зовнішньої політики іноземних держав стосовно України та соціально-політичної ситуації в нашій державі;
– оцінити громадську думку щодо суспільно-політичних подій в Україні, наявні в українському суспільстві протестні настрої, у тому числі її врахування в діяльності державних і громадських структур;
– здійснювати постійний моніторинг подій в світі, реакцію ЗМІ на найбільш гострі питання, що стосуються України;
– виокремити фейкові повідомлення із загального інформаційного потоку;
– з'ясувати офіційні й так звані «оперативні можливості» потенційних супротивників («агентура впливу» з-поміж журналістів, громадських діячів, політиків, державних службовців, представників правоохоронних органів та фінансово-промислових груп; підконтрольні іноземним державам або кримінальним структурам медіахолдинг, інші телерадіоорганізації, друковані ЗМІ, інформаційні агентства та інтернет-видання; отримані дані про наміри представників іноземних держав започаткувати в Україні нові інформаційні ресурси з антиконституційною метою чи встановити фінансовий контроль над провідними українськими виданнями) тощо. Це дозволить передусім з'ясувати спрямування іноземних держав, їх спецслужб, терористичних або злочинних організацій, інших утворень, суспільних груп та окремих осіб, котрі розглядаються як потенційні об'єкти СІО в інформаційному просторі України, з'ясувати так звані «оперативні можливості» цих держав, спецслужб, організацій, утворень тощо, а також можливі передумови для проведення СІО тощо. Відповідно, якісне інформаційне забезпечення СІО на підготовчому етапі дозволить визначити ймовірні ризики проведення СІО та зменшити їх. За результатами дослідження цільової аудиторії і визначення ризиків в ході підготовчого етапу необхідно також здійснити прогноз розвитку ситуації у випадку проведення СІО, в тому числі с прогнозувати можливі заходи потенційного супротивника з метою попередження і нейтралізації СІО. Якісний прогноз розвитку ситуації надасть можливість суб'єктам проведення СІО ефективно реалізувати наступні етапи нашого алгоритму, а саме заходи з виявлення, попередження та припинення. Отже, під час пошуку або створення інформаційного приводу для проведення СІО необхідно з'ясувати передумови для проведення інформаційних впливів, зокрема, визначити вразливі місця у безпековому середовищі супротивника: проблемні аспекти морально-психологічної обстановки в державі або угрупованні; місця розташування стратегічно важливих об'єктів; події у районах бойових дій, дислокації військ; ступінь потенційного впливу на цільову аудиторію - населення, правоохоронців, військовослужбовців, членів певних релігійних, терористичних, кримінальних спільнот, субкультур них груп тощо, - пропаганди та інших форм інформаційного впливу. Інформаційний етап СІО передбачає створення чи вибір інформаційного приводу як тригеру (автоматичні поведінкові реакції людини, що виникають у відповідь на яку-небудь подію) для СІО. Саме від правильного вибору інформаційного тригера за-

лежить інформаційний розвиток ситуації навколо явища, процесу чи події, які є базою СІО. За своєю суттю інформаційний привід покликаний мотивувати чи демотивувати цільову аудиторію СІО до зміни ставлення до певних дій, подій, об'єктів чи суб'єктів, вчинення певних дій чи до бездіяльності, або ж зміни свого світосприйняття чи світоглядної картини відповідно до намірів, цілей та оперативного задуму організаторів операції. Так, кожен інформаційний привід здатен викликати окрему, специфічну реакцію в аудиторії, що і є головною метою інформаційного етапу СІО у процесі підбору чи створення інформаційного приводу. Саме заплановане емоційне забарвлення інформаційного приводу визначає наміри щодо подальшого розвитку самої СІО та ситуації навколо об'єкту СІО. Своєю чергою, результати інформаційного етапу та обраний інформаційний привід визначатимуть зміст наступного етапу, тобто, етапу планування СІО. При цьому принципами планування СІО мають бути наступні: - застосування «ефект-орієнтованого» підходу з акцентуванням уваги в інформаційній сфері на причинах та наслідках; - поєднання мережевого (децентралізованого) виконання і централізованого планування й координації дій суб'єктів проведення СІО; -забезпечення оптимальної послідовності, синхронізації та безперервності дій, а також уникнення внутрішніх суперечностей між виконавцями СІО; - належне інформаційно-аналітичне забезпечення процесу проведення СІО та налагодження «зворотного зв'язку» за результатами проведення запланованих заходів.

На етапі планування також уточнюється склад команди виконавців СІО, безпосередні об'єкти впливу у складі цільової аудиторії, а також суб'єкти інформаційного простору, які можуть бути використані в ході СІО з метою здійснення маніпулятивного інформаційного впливу. Проведення СІО наступального (розвідувального), так і оборонного (контррозвідувального) спрямування, характеризується розгалуженою системою методів, до якої входять зокрема, методи електронної та радіоелектронної боротьби, боротьби з комунікаційними системами, криптографічної боротьби, методи інформаційно-психологічного впливу, «культуркампф», методи «хакерської боротьби», методи «кібернетичної» або «мережної боротьби», методи економічного інформаційного протиборства тощо. СІО всіх наведених видів, передусім здійснювані в рамках синергетичної моделі СІО, можуть супроводжуватись різноплановими заходами технічного характеру. При цьому за будь-якого «набору» запланованих заходів, в ході етапу реалізації відбувається «розкрутка» інформаційного приводу задля впливу на цільову аудиторії відповідно до задуму організаторів СІО.

Етап закріплення результатів СІО має своїм завданням забезпечення плавного завершення СІО після досягнення поставлених цілей та фіксації отриманих результатів. Змістовне наповнення цього етапу зумовлюється наступним: аби цільова аудиторія «засвоїла» інформацію необхідно її зробити достатньо значущою та/або такою, що добре запам'ятовується. В результаті запропонованого системного й комплексного підходу до планування та підготовки СІО, який слугує підґрунтям для побудови матриці інформаційно-правового забезпечення синергетичної моделі СІО прогнозується більша ефективність та результативність відповідних заходів у порівнянні з інформаційними акціями, які несуть одноразовий характер, мають вузьку тематичну направленість та реалізуються в ході обмеженого часового проміжку. [4]

Важливим питанням оптимізації інформаційно-методичного забезпечення СІО як складової їх інформаційно-правового забезпечення є визначення моделі та формування алгоритму проведення СІО. В сучасних умовах необхідним є формування з використанням тензорної методології синергетичної моделі СІО, яка поєднуватиме моделі, орієнтовані на зміну ставлення до об'єкта, зміну поведінки та зміну світоглядної картини. Синергетична модель СІО призначена для вирішення наступних основних завдань стосовно визначеної цільової аудиторії: зміни ставлення до певного об'єкта або дій; зміни поведінки; зміни світосприйняття та світоглядної картини (з одночасним унеможливленням досягнення щодо населення України аналогічних цілей іноземними державами, їх спецслужбами, окремими організаціями й спільнотами (а тому числі такими, що здійснюють терористичну або іншу злочинну діяльність), окремими особами, що діють на шкоду національній безпеці України тощо). Використання принципів тензорної методології дозволить 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»). При цьому у проведенні СІО з урахуванням сучасних реалій гібридної війни та актуальних стандартів НАТО з питань проведення інформаційних і психологічних операцій пропонуємо 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). Проведення СІО наступального (розвідувального), так і оборонного (контррозвідувального) спрямування, характеризується розгалуженою системою методів, до якої входять зокрема, методи електронної та радіоелектронної боротьби, боротьби з комунікаційними системами, криптографічної боротьби, методи інформаційно-психологічного впливу, «культуркампф», методи

«хакерської боротьби», методи «кібернетичної» або «мережної боротьби», методи економічного інформаційного протиборства тощо.

Висновки. Важливим питанням оптимізації інформаційно-методичного забезпечення СІО як складової їх інформаційно-правового забезпечення є визначення моделі та формування алгоритму проведення СІО. В сучасних умовах необхідним є формування з використанням тензорної методології синергетичної моделі СІО, яка поєднуватиме моделі, орієнтовані на зміну ставлення до об'єкта, зміну поведінки та зміну світоглядної картини. Синергетична модель СІО призначена для вирішення наступних основних завдань стосовно визначеної цільової аудиторії: зміни ставлення до певного об'єкта або дій; зміни поведінки; зміни світосприйняття та світоглядної картини (з одночасним унеможливленням досягнення щодо населення України аналогічних цілей іноземними державами, їх спецслужбами, окремими організаціями й спільнотами (а тому числі такими, що здійснюють терористичну або іншу злочинну діяльність), окремими особами, що діють на шкоду національній безпеці України тощо). Використання принципів тензорної методології дозволить 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»). При цьому у проведенні СІО з урахуванням сучасних реалій гібридної війни та актуальних стандартів НАТО з питань проведення інформаційних і психологічних операцій пропонуємо 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). Проведення СІО наступального (розвідувального), так і оборонного (контррозвідувального) спрямування, характеризується розгалуженою системою методів, до якої входять зокрема, методи електронної та радіоелектронної боротьби, боротьби з комунікаційними системами, криптографічної боротьби, методи інформаційно-психологічного впливу, «культуркампф» [3], методи «хакерської боротьби», методи «кібернетичної» або «мережної боротьби», методи економічного інформаційного протиборства тощо.

Список використаних джерел:

1. Крон Г. Исследование сложных систем по частям - диакоптика. М.: Наука, 1972. 544с.
2. Петров А.Е. Тензорная методология в теории систем. М., 1985. 152 с.
3. Фролов Д.Б. Информационная война: эволюция форм, средств и методов. URL: cyberleninka.ru/article/n/informatsionnaya-voyna-evolyutsia-formsredstv-i-metodov (дата звернення 12.12.2018)
4. Ковтун Н.А., Мухин В.И., Набока Ю.И., Чумаров И.С. Основные категории информационной борьбы. Вопросы защиты информации. 2001. №2. С. 2-7