

УДК 327.325 : 681.3

DOI <https://doi.org/10.32849/2663-5313.2019.7.24>**Олександр Верголяс,***аспірант Науково-дослідного інституту інформатики і права**Національної академії правових наук України,**виконавчий директор Інформаційного агентства «Петро і Мазепа медіа»*

ПЕРСПЕКТИВИ 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 унеможливується проведення СІО захисного спрямування, в тому числі контррозвідальних 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 розвідальний, так і контррозвідальний 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 ефективного 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 розвідальним 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.

Постановка проблеми. Спеціальні інформаційні операції (далі – 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 не лише під час забезпечення інформаційного, але й інших складників національної безпеки, яка є складним та багатоаспектним феноменом. Втім, незважаючи на виняткову актуальність проблематики СІО, а отже їх інформаційно-правового забезпечення, у цій сфері наразі існує значна кількість проблемних питань. Основною проблемою інформаційно-правового забезпечення СІО в умовах сьогодення

є відсутність достатнього правового унормування їх проведення. Відповідно, відсутнє й достатнє нормативне підґрунтя для розробки методологічних засад інформаційного забезпечення СІО. Це передусім зумовлює потребу у нормативно-правовому визначенні заборон під час здійснення 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 організовуватись відповідно до правових норм, які забезпечують конституційні права та свободи громадян.

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. Слосарчук, 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. Основна проблема проведення СІО сектором безпеки і оборони України полягає передусім у слабкій нормативній урегульованості, а точніше, у відсутності належних правових засад для проведення СІО іншими, окрім Збройних Сил, складниками сектору безпеки і оборони України.

Слід підкреслити, що поняття СІО тісно пов'язане із поняттям інформаційного впливу та протидії інформаційному впливу, які наразі не отримали нормативного визначення. Втім, наведені терміни вживаються у Доктрині інформаційної безпеки України, метою якої є уточнення засад формування та реалізації державної інформаційної політики насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. При цьому створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди, визначено Доктриною інформаційної безпеки України як один із національних інтересів України в інформаційній сфері [1].

Загалом Стратегія національної безпеки України та Доктрина інформаційної безпеки, виходячи з актуальних загроз національній безпеці України, передбачають необхідність протидії: веденню інформаційної війни проти України; поширенню закликів до радикальних дій, пропаганди ізоляціоністських та автономістських концепцій співіснування регіонів в Україні; здійсненню СІО, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні; проведенню державою-агресором спеціальних інформаційних операцій в інших державах з метою

створення негативного іміджу України у світі; інформаційній експансії держави-агресора та контрольованих нею структур, зокрема, шляхом розширення власної інформаційної інфраструктури на території України та в інших державах [2].

При цьому п. 6 Доктрини інформаційної безпеки України передбачає, що Служба безпеки України у межах компетенції має здійснювати моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет із метою виявлення загроз національній безпеці України в інформаційній сфері. Крім того, Служба безпеки України у межах компетенції має здійснювати протидію проведенню проти України СІО, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації. Нагадаємо також, що Доктрина інформаційної безпеки України передбачає, що Міністерство оборони України та Генеральний штаб Збройних Сил України відповідно до компетенції забезпечують протидію СІО, спрямованим проти Збройних Сил України та інших військових формувань, супроводження інформаційними засобами виконання завдань оборони України [1].

У Законі України «Про оборону України» спеціальна операція визначена 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, 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 [3]. Це визначення цілком може застосовуватись щодо СІО.

Ч. 2 ст. 4 вказаного Закону передбачає, що органи державної влади та органи військового управління, не чекаючи оголошення стану війни, вживають заходів для відсічі агресії. На підставі відповідного рішення Президента України Збройні Сили України разом з іншими військовими формуваннями розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі. Отже, виходячи зі змісту наведеного положення, спеціальні операції, в тому числі СІО, розглядаються як форма воєнних дій.

Відповідно до Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України [4], під інформа-

ційними операціями розуміють узгоджене за метою, завданнями, місцем і часом з іншими діями військ (сил) інтегроване використання можливостей з інформаційного впливу для порушення, зриву, перехоплення або іншого деструктивного впливу на процеси прийняття рішень противником при одночасному захисті власного інформаційного простору. Одночасно Концепція визначає й поняття психологічних операцій, під якими розуміють психологічні операції – сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом психологічних акцій (дій) та інших дій суб'єктів психологічних операцій, які проводяться за єдиним замислом і планом для здійснення впливу на емоційний стан, мотивацію, раціональне мислення визначених цільових аудиторій та зміни моделей їхньої поведінки у спосіб, що сприятиме досягненню політичних і військових цілей України.

Розгляд СІО як форми воєнних дій та фактично як монополії Збройних Сил унеможливує проведення СІО контррозвідального характеру на території України, зокрема, й щодо злочинних угруповань і перетворює їх суто на елемент нападу, який застосовується на території супротивника – іноземної держави. Так, ч. 4 ст. 17 Конституції України [5] передбачає, що Збройні Сили України та інші військові формування ніким не можуть бути використані для обмеження прав і свобод громадян. Тож на виконання відповідного конституційного положення п. 2.7 Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України [4] визначає, що у ході реалізації стратегічних комунікацій відповідно до компетенції Міністерства оборони та Збройних Сил інформаційні та психологічні операції як складники стратегічних комунікацій (тобто СІО) не проводяться стосовно громадян України (крім тих, які є членами терористичних угруповань та незаконних збройних формувань). Також вони не проводяться 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 листопаді 2017 року до Верховної Ради України було внесено проект Закону України «Про внесення змін до Закону України «Про оборону України» щодо деяких питань підготовки держави до оборони» (реєстр. № 7272). Його головна ідея – розширення правового поля держави щодо застосування Сил спеціальних операцій ЗС України. Передбачається створення правових підстав для ведення спеціальної розвідки та військових інформаційно-психологічних операцій не тільки в умовах дії правового режиму воєнного стану, але і в

мирний час в інтересах підготовки держави до оборони, тобто йдеться про проведення СІО «захисного» характеру, метою яких є забезпечення безпеки [6], а відповідно, така законодавча новація є не позбавленою сенсу умовах гібридної війни. Водночас це не вирішує проблему фактичної відсутності належного правового підґрунтя для проведення СІО силами безпеки відповідно до їхньої компетенції в тому числі й з метою протидії деструктивним СІО. Так, у масиві чинного законодавства України нині відсутні нормативно-правові акти або конкретні норми, які б регламентували порядок правової реалізації зазначеної функції. Наприклад, Закон України «Про Службу безпеки України» [7] не передбачає в числі повноважень вітчизняної спецслужби правообов'язку щодо проведення СІО. Водночас надання відповідних повноважень Службі безпеки України з одночасним позбавленням її статусу військового формування забезпечило б і дотримання згаданих вище конституційних вимог, і 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.

Усе це є, безперечно, актуальним та необхідним, адже слід враховувати той факт, що негативні інформаційні впливи можуть проводити поряд зі спецслужбами іноземних держав і терористичні організації, тож слід звернути увагу й на положення п. 3 Резолюції Організації Об'єднаних Націй 51/210 «Заходи щодо ліквідації міжнародного тероризму», якими державам пропонувалось, здійснюючи заходи з боротьби з тероризмом, у тому числі створюючи відповідне законодавство, «звернути увагу на ризик використання терористами електронних або дротових комунікацій для вчинення кримінальних дій і необхідність знайти засоби, погоджені з національним законодавством, для попередження подібної злочинності, розвитку відповідної співпраці» [8]. Виконання зазначених вимог, зауважимо, потребує передусім проведення СІО, причому йдеться про проведення СІО в рамках так званої «контрмережної боротьби», зважаючи на мережевий характер сучасного тероризму.

Отже, нині є потреба у нормативно-правовому визначенні заборон під час здійснення інформаційного впливу, в тому числі в ході проведення СІО, які визначатимуть межі їх проведення. 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 їхньої компетенції, що дозволить розширити потенційне коло об'єктів СІО та, відповідно, сферу їх застосування з метою забезпечення національної безпеки. Насамперед відповідними повноваженнями мають бути наділені Служба безпеки України та розвідувальні органи. Не менш важливим моментом є й власне нормативне закріплення визначення СІО на рівні закону, що надалі дасть можливість розробити ефективну модель та алгоритм СІО й закріпити його на рівні відомчих нормативно-правових актів.

З цією метою пропонується:

– визначити серед функцій Служби безпеки України, розвідувальних органів «участь у забезпеченні загальнодержавної системи стратегічних комунікацій»;

– при внесенні змін до Закону України «Про Службу безпеки України» (в тому числі в разі викладення його у новій редакції) передбачити серед повноважень Служби безпеки України таке:

«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»;

– під час розроблення Закону України «Про Службу безпеки України» передбачити серед повноважень розвідувальних органів України таке:

«проводити спеціальні інформаційні операції з метою сприяння реалізації національних інтересів України та протидії зовнішнім загрозам національній безпеці України у визначених законом сферах»;

– наділити спецслужби України повноваженнями щодо:

використання добровільної допомоги фізичних та юридичних осіб;

використання гласних і негласних позаштатних працівників, а також співробітників під прикриттям;

використання структур прикриття.

– розробити загальнодержавну Концепцію стратегічних комунікацій, у якій закріпити таке визначення СІО:

«Спеціальні інформаційні операції – сукупність узгоджених і взаємопов'язаних дій розвідувального та/або контррозвідувального спрямування, здійснюваних державними органами, що входять до складу сил безпеки і сил оборони 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 інши-

ми складниками сектору безпеки і оборони з метою забезпечення національної безпеки України».

Такі першочергові заходи дозволять створити належне правове підґрунтя для проведення СІО в цілому та для інформаційно-правового забезпечення їх проведення, зокрема побудови моделі та формування алгоритму проведення СІО. Зокрема, в сучасних умовах необхідним є формування з використанням принципів тензорної методології синергетичної моделі СІО, яка поєднуватиме традиційні моделі, орієнтовані на зміну ставлення до об'єкта, зміну поведінки та зміну світоглядної картини [9]. Синергетична модель СІО призначена для вирішення таких 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, їхніми спецслужбами, окремими організаціями й спільнотами (в тому числі такими, що здійснюють терористичну або іншу злочинну діяльність), окремими особами, що діють на шкоду національній безпеці України тощо). Використання принципів тензорної методології також дозволить інтегрувати до синергетичної моделі проведення СІО досвід контрмережної боротьби, який передбачає використання у проведенні СІО низки підмереж: підмережі датчиків (сенсорів), підмережі комунікації, підмережі аналітичної обробки інформації, підмережі вузлів прийняття рішень і підмережі «виконавчих вузлів».

Висновки

Оскільки спеціальні операції в цілому, в тому числі СІО, нині розглядаються за законодавством України як форма воєнних дій, фактично унеможливується 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 анти-терористичної, 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. Такі першочергові заходи дозволять створити належне правове підґрунтя для проведення СІО в цілому та для інформаційно-правового забезпечення їх проведення зокрема. Наступним важливим питанням щодо вдосконалення інформаційно-правового забезпечення СІО є побудова сучасної моделі СІО та формування алгоритму проведення СІО. У свою чергу, побудова адекватної сучасним потребам національної безпеки України моделі СІО забезпечуватиме вибір найбільш ефективного спектру методів проведення СІО. Загалом системний підхід до планування та підготовки СІО не лише дозволить підвищити ефективність їх інформаційного забезпечення, але й сприятиме найбільш успішному виконанню алгоритму проведення СІО.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017. URL:

<http://www.president.gov.ua/documents/472017-21374> (дата звернення: 28.11.2018).

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015. URL: <https://zakon.rada.gov.ua/laws/show/287/2015> (дата звернення: 09.04.2019)

3. Про оборону України: Закон України від 06.12.1991. URL: <https://zakon.rada.gov.ua/laws/show/1932-12> (дата звернення 18.04.2019).

4. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України: Наказ Міністерства оборони України від 22.11.2017 № 612. URL: <https://zakon.rada.gov.ua/rada/show/v0612322-17> (дата звернення: 18.04.2019).

5. Конституція України. URL: <http://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80> (дата звернення: 21.11.2018)

6. Попова Т. Правове поле для спецназу. URL: <https://www.radiosvoboda.org/a/28373318.html> (дата звернення: 12.05.2019).

7. Про Службу безпеки України: Закон України від 25.03.1992. URL: <https://zakon.rada.gov.ua/laws/show/2229-12> (дата звернення: 12.05.2019).

8. Декларація, що доповнює Декларацію про заходи щодо ліквідації міжнародного тероризму 1994 року: Резолюція 51/210 Генеральної Асамблеї ООН. URL: https://zakon.rada.gov.ua/laws/show/995_370 (дата звернення: 14.05.2019).

9. Почепцов Г. Три моделі побудови інформаційних операцій. URL: https://ms.detector.media/ethics/manipulation/tri_modeli_postroeniya_informatsionnykh_operatsiy/ (дата звернення: 29.04.2019).

The article is devoted to the definition of problem aspects and prospects for improving the information and legal support of special information operations (SIO), as there is currently no sufficient legal and regulatory framework for the development of methodological principles for their implementation. SIO in the system of national security of Ukraine occupy a special place – as an independent means of realization of events of informational and psychological purpose and as an auxiliary means in the implementation of political, economic, military and other measures. SIO can be implemented not only with the information provided, but also other components of national security, which is a complex and multidimensional phenomenon. Since special operations in general, including SIOs are currently being considered under the legislation of Ukraine as a form of military action, in practice it is impossible to carry out a SIO of protection, including counter-intelligence SIO on the territory of Ukraine. Thus, the current legislation does not stipulate conducting of the SIO against Ukrainian citizens (except the members of terrorist groups and illegal armed formations), as well as conducting the SIO in the territory of Ukraine outside the area of the anti-terrorist operations or other places (areas) of the preparation and use of the Armed Forces. However, both the reconnaissance and the counter-intelligence aspect of the SIO is manifested at all stages of the SIO, regardless of their direction, offensive or defensive character. The urgent need is to empower the SIO of the Security Service of Ukraine with the simultaneous deprivation of its status of military formation, which will ensure compliance with the requirements of the Constitution of Ukraine, as well as the effective conduct of the SIO not only in the interests of defense, but in the interests of anti-terrorist, anti-criminal, informational and other components of the national security. Similar powers should be given to all intelligence agencies of Ukraine accordance with their competence. Not less important is the actual regulation of the definition of SIO I at the level of law and the construction of a modern SIO model and the formation of SIO algorithm.

Key words: special informational operations, information influence, national security, strategic communications, synergetic model.