Адміністративне право і процес; фінансове право; інформаційне право
УДК 681.3

Верголяс Олександр Олександрович
виконавчий директор
ІА «Петро і Мазепа медіа»
Верголяс Александр Александрович
исполнительный директор
ИА «Петр и Мазепа медиа»
Vergolyas Aleksander
CEO
Peter and Mazepa Media IA

СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ В СИСТЕМІ ЗАСОБІВ ПРОТИДІЇ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ
СПЕЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ В СИСТЕМЕ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ
SPECIAL INFORMATION OPERATIONS IN THE SYSTEM OF MEANS OF COUNTERACTING THREATS TO NATIONAL SECURITY OF UKRAINE

Анотація. *В цій статті проаналізовано роль та місце спеціальних інформаційних операцій в системі засобів протидії загрозам національній безпеці України, яка включає такі групи основних засобів (заходів) протидії традиційним і новим загрозам національній безпеці: політико-дипломатичні; військові; правові (законодавчі); інформаційно-психологічні; економічні; науково-технологічні; організаційні (адміністративні й процедурні); фізичні; технічні (апаратні й програмні) тощо. Визначено, що спеціальні інформаційні операції становлять самостійний засіб реалізації заходів інформаційно-психологічного*

спрямування, а також можуть розглядатися як допоміжний засіб в реалізації політичних, економічних, військових та інших заходів, які без належної інформаційної підтримки приречені на неуспіх. При цьому спеціальні інформаційні операції можуть реалізовуватись не лише при забезпечені інформаційної, але й інших складових національної безпеки, яка є складним та багатоаспектним феноменом. Як інформаційно-правове явище, спеціальні інформаційні операції класифікуються за спрямуванням, аспектами, типом та видом, а також характеризуються розгалуженим спектром методів, що можуть застосовуватись у ході їх проведення, відтак у статті досліджена система спеціальних інформаційних операцій. Зокрема, спеціальні інформаційні операції як засіб протидії загрозам національній безпеці характеризується двома аспектами - розвідувальним, що забезпечує збір розвідувальної інформації про супротивника та здійснення необхідного впливу на нього, та контррозвідувальним, який пов'язаний із захистом власної інформації, інформаційної інфраструктури й протидією спеціальним інформаційним операціям супротивника. За типом можуть бути класифіковані наступні спеціальні інформаційні операції: операції, об'єктом (ціллю) яких є конкретна особа або визначене коло осіб; операції, спрямовані на ініціювання, зміну напрямку розвитку, припинення чи «розмиття» певного процесу, явища чи події; «спін-операції». За видом можна виділити наступні спеціальні інформаційні операції: в новинарній сфері; в комунікативній сфері; в науковій та культурній сфері. Проведення спеціальних інформаційних операцій як наступального, так і оборонного спрямування характеризується розгалуженою системою методів, до якої входять зокрема, методи електронної та радіоелектронної боротьби, боротьби з комунікаційними системами, криптографічної боротьби, методи інформаційно-психологічного впливу, «війни культур», методи «хакерської боротьби», методи «кібернетичної» або «мережної

боротьби», методи економічного інформаційного протиборства тощо. Крім того, у статті також окреслені перспективи вдосконалення інформаційно-правового забезпечення спеціальних інформаційних операцій, які в сучасних умовах залежать передусім від формування належного правового підґрунтя їх проведення.

Ключові слова: *спеціальні інформаційні операції, загрози, національна безпека, контррозвідувальні, розвідувальні, оборонні, наступальні, система.*

Аннотация. *В этой статье проанализированы роль и место специальных информационных операций в системе средств противодействия угрозам национальной безопасности Украины, которая включает такие группы основных средств (мероприятий) противодействия традиционным и новым угрозам национальной безопасности: политико-дипломатические; военные; правовые (законодательные) информационно-психологические; экономические; научно-технологические; организационные (административные и процедурные) физические; технические (аппаратные и программные) и др. Определено, что специальные информационные операции составляют самостоятельное средство реализации мероприятий информационно-психологического направления, а также могут рассматриваться как вспомогательное средство в реализации политических, экономических, военных и других мероприятий, которые без надлежащей информационной поддержки обречены на неудачу. При этом специальные информационные операции могут реализовываться не только при обеспечении информационной, но и других составляющих национальной безопасности, которая является сложным и многоаспектным феноменом. Как информационно-правовое явление, специальные информационные операции классифицируются по направлению, аспектам, типам и видам, а*

также характеризуются разветвленным спектром методов, которые могут применяться в ходе их проведения, поэтому в статье исследована система специальных информационных операций. В частности, специальные информационные операции как средство противодействия угрозам национальной безопасности характеризуется двумя аспектами - разведывательным, который обеспечивает сбор разведывательной информации о противнике и осуществления необходимого воздействия на него, и контрразведывательным, связанным с защитой собственной информации, информационной инфраструктуры и противодействием специальным информационным операциям противника. По типу могут быть классифицированы следующие специальные информационные операции: операции, объектом (целью) которых конкретное лицо или определенный круг лиц; операции, направленные на инициирование, изменение направления развития, прекращение или «размытие» определенного процесса, явления или события; «спин-операции». По виду можно выделить следующие специальные информационные операции: в новостной сфере; в коммуникативной сфере; в научной и культурной сфере. Проведение специальных информационных операций как наступательного, так и оборонительного характера характеризуется разветвленной системой методов, в которую входят в том числе, методы электронной и радиоэлектронной борьбы, борьбы с коммуникационными системами, криптографической борьбы, методы информационно-психологического воздействия, «войны культур», методы «хакерской борьбы», методы «кибернетической» или «сетевой борьбы», методы экономического информационного противоборства и др. Кроме того, в статье также обозначены перспективы совершенствования информационно-правового обеспечения специальных информационных операций, которые в современных условиях зависят прежде всего от формирования надлежащего правового основания их проведения.

Ключевые слова: *специальные информационные операции, угрозы, национальная безопасность, контрразведывательные, разведывательные, оборонительные, наступательные, система.*

Summary. *This article analyzes the role and place of special information operations in the system of countering threats to the national security of Ukraine, which includes such groups of fixed assets (measures) to counteract traditional and new threats to national security: political and diplomatic; military; legal (legislative) information-psychological; economic; scientific and technological; organizational (administrative and procedural) physical; technical (hardware and software), etc. It has been determined that special information operations constitute an independent means of implementing information and psychological activities, and can also be considered as an auxiliary tool in implementing political, economic, military and other activities that, without proper information support, are doomed fail. At the same time, special information operations can be realized not only in providing information, but also other components of national security, which is a complex and multidimensional phenomenon. As an informational-legal phenomenon, special information operations are classified according to direction, aspects, types and so on, and are also characterized by an extensive range of methods that can be used during their implementation; therefore, the article examines a system of special information operations. In particular, special information operations as a means of countering threats to national security are characterized by two aspects - intelligence, which collects intelligence information about the enemy and exerts the necessary influence on him, and counterintelligence, related to the protection of the own information, information infrastructure and opposition to enemy's special information operations. The following special information operations can be classified by type: operations whose object (purpose) is a specific person or a certain circle*

of persons; operations aimed at initiating, changing the direction of development, termination or "blurring" of a certain process, phenomenon or event; "spin operations". By the form of the following special information operations can be identified: in the news area; in the communicative sphere; in the scientific and cultural field. Conducting special information operations both offensive and defensive re is characterized by an extensive system of methods, including, inter alia, electronic and electronic warfare methods, communication systems, cryptographic control methods, informational and psychological impact methods, "war of cultures", "hacker fight", methods of "cybernetic" or "network struggle", methods of economic informational confrontation, etc. In addition, the article also marks the perspective willow improvement of information- legal providing special information operations, which in the present conditions depend primarily on the formation of an appropriate legal basis for their implementation.

Key words: *special information operations, threats, national security, counterintelligence, reconnaissance, defense, offensive, system.*

Постановка проблеми. Відповідно до визначення, наведеного у ст. 1 Закону України «Про національну безпеку України», загрози національній безпеці України - це явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [1]. Ст. 1 Закону України «Про національну безпеку України» також передбачає, що документом, який визначає актуальні загрози національній безпеці України та відповідні цілі, завдання, механізми захисту національних інтересів України та слугує основою для планування і реалізації державної політики у сфері національної безпеки, виступає Стратегія національної безпеки України [2]. Актуальні загрози національній безпеці України в інформаційній сфері визначені також у п. 4 Доктрини інформаційної безпеки України [3].

Відповідні переліки загроз національній безпеці не є вичерпними і включають найбільш актуальні загрози поточного періоду. Втім слід зауважити, що всі відповідні загрози обумовлюють необхідність вжиття заходів реагування у вигляді спеціальних інформаційних операцій (далі – СІО), тож далі доцільно зосередитись на місці СІО в системі засобів протидії загрозам національній безпеці України.

Стан дослідження. Дослідженням широкого спектру питань протидії загрозам національній безпеці займалися такі науковці як О. Бандурка, Я. Вішняков, В. Горбулін, Г. Горшенков, В. Дрьомін, М. Зеленков, І. Івченко, А. Качинський, М. Клейменов, О.Костенко, О. Литвак, Н. Луман, В. Лунєєв, В. Максимов, М. Мельник, Г. Новицький, В. Плєшаков, О. Фомін, С. Шабанов, А. Шаваєв, М. Шелухін та інші. При цьому проблематиці проведення СІО приділяли увагу у своїх працях Г.Почепцов, М.Стрельбицький, В.Пилипчук, М.Шилін, А.Марущак, О.Морозов, В.Ліпкан, О.Литвиненко, І.Слюсарчук, М.Чеховська, Ю.Лапутіна, Н.Іванова, В.Панченко та інші. Водночас, у науковій літературі місце СІО в системі засобів протидії загрозам національній безпеці України окреслено недостатньо чітко, що зумовлює актуальність цієї статті.

Мета статті полягає у з’ясуванні місця СІО в системі засобів протидії загрозам національній безпеці України.

Виклад основного матеріалу. На сьогодні можуть бути виділені такі групи основних засобів (заходів) протидії традиційним і новим загрозам національній безпеці: політико-дипломатичні; військові; правові (законодавчі); інформаційно-психологічні; економічні; науково-технологічні; організаційні (адміністративні й процедурні); фізичні; технічні (апаратні й програмні) тощо.

До політико-дипломатичних заходів протидії загрозам національній безпеці можуть бути віднесені: формування державної політики

забезпечення національної безпеки; зустрічі глав держав, урядів, політичних делегацій; перемовини та консультації щодо встановлення чи активізації міждержавних відносин; проведення нарад, конференцій щодо встановлення військово-політичних союзів, керівництва ними, оцінки загроз та вироблення спільних дій; використання міжнародних інститутів (ООН, ОБСЄ тощо) для застосування санкцій до держав, що дестабілізують міжнародну обстановку; перемовини з питань, що викликають напруженість у міждержавних відносинах; заходи щодо зміцнення довіри; планування, перенесення й скасування візитів політичних лідерів, державних делегацій; передача керівництву держав, дипломатичним службам нот, вимог, меморандумів, роз'яснень у зв'язку із певними ситуаціями; розрив дипломатичних відносин тощо.

Військові заходи протидії загрозам національній безпеці включають: демонстрацію переходу регулярних збройних сил на штати воєнного часу, резерву на воєнний стан; формування нових з'єднань і частин; передислокація й розосередження збройних сил, сил і засобів військової авіації й флоту; демонстрація оперативного розгортання з'єднань і частин уздовж державного кордону; приведення стратегічних озброєнь у вищий ступінь бойової готовності; підтримка бойового потенціалу, бойової й мобілізаційної готовності військових формувань і органів військового командування на необхідному рівні; безпосередні військові дії, акції та операції тощо.

До правових заходів протидії загрозам національній безпеці належать закони, укази й інші нормативно-правові акти національного законодавства, що визначають правове поле забезпечення національної безпеки та структурують правопорядок в цілому. Це вимоги дотримання норм міжнародного права, положень міждержавних договорів і угод; підписання двосторонніх і багатосторонніх договорів і угод щодо врегулювання правових взаємин; використання юридичних засобів і між

народів правових інституцій (Міжнародний суд ООН, Європейський суд з прав людини тощо). Правові заходи також включають різноманітні заходи ліцензування, сертифікації та атестації технічних та програмних засобів, що використовуються в системі забезпечення національної безпеки.

Інформаційно-психологічні заходи протидії загрозам національній безпеці можуть знаходити прояв у формі пропаганди необхідності дотримання міжнародних договорів і угод, інформаційно-психологічного впливу на держави з метою втримати їх від надання допомоги країнам, що провокують конфлікт або беруть участь у цьому конфлікті, інформування населення й збройних сил про причини й дійсні цілі конфлікту, інформаційно-психологічні операції із запобігання розпалення міжнаціональної ворожнечі, інших деструктивних настроїв і дій тощо.

Різновидом інформаційно-психологічних заходів можуть вважатися так звані морально-етичні заходи забезпечення національної безпеки, до яких належать норми поведінки, що традиційно склалися у суспільстві. Ці норми здебільшого не є обов'язковими, на відміну від вимог нормативних актів, однак, їхнє недотримання веде звичайно до падіння авторитету або престижу людини, групи осіб або організації, а дотримання чинить профілактичний вплив на оточуючих. Морально-етичні норми можуть бути неписаними (наприклад, загальновизнані норми чесності, патріотизму тощо), або писаними, тобто оформлені у певний звід (статут, кодекс поведінки тощо) правил або приписань. Морально-етичні засоби забезпечення національної безпеки також закладають засади для подальшого юридичного оформлення відповідних норм поведінки, а відтак – можуть трансформуватися на правові засоби.

Економічні заходи протидії загрозам національній безпеці включають в себе нейтралізацію несприятливих впливів на економіку країни шляхом вжиття відповідних заходів на дискримінаційні дії іноземних держав у торгово-економічній, науково-технічній, фінансової та

інших сферах, уведення ембарго, вжиття заходів тарифного й нетарифного регулювання, підвищення стійкості банківського сектору, що виключає можливість виникнення системних криз, підвищення ефективності валютного регулювання й валютного контролю, боротьби з легалізацією (відмиванням) доходів, отриманих злочинним шляхом, нелегальним вивозом капіталу а також боротьби з фінансуванням терористичних організацій, забезпечення ефективного використання всіх видів ресурсів (трудових, природних, інтелектуальних, інформаційних, фінансових тощо), підвищення конкурентоздатності на основі технічної модернізації національної промисловості, створення умов для досягнення рівня і якості життя населення, що гарантують соціальну злагоду і політичну стабільність у країні, створення необхідного й достатнього державного матеріального резерву (потужностей і матеріалів) для забезпечення мобілізаційних потреб, а також стратегічних запасів матеріальних ресурсів для протидії різким кон'юнктурним коливанням на світових товарних і фондових ринках, створення законодавчих і економічних умов зниження криміналізації суспільства, господарсько-фінансової діяльності тощо [4].

Науково-технологічні заходи протидії загрозам національній безпеці – це, зокрема, забезпечення на основі державної інноваційної політики реалізації стратегічних національних пріоритетів, що включають підвищення якості життя населення, досягнення економічного росту, розвиток фундаментальної науки, освіти, культури, забезпечення оборони й безпеки країни. Це також різнопланові технологічні рішення й прийоми, засновані на використанні структурної, функціональної, інформаційної, часової надмірності тощо, які спрямовані на зменшення можливості здійснення суб’єктами забезпечення національної безпеки помилок і порушень у рамках наданих їм прав і повноважень.

Організаційні заходи протидії загрозам національній безпеці необхідні для забезпечення ефективного застосування інших заходів і

засобів захисту в частині, що стосується регламентації дій виконавців. Зокрема, в інформаційному аспекті - це заходи адміністративного й процедурного характеру, що регламентують процеси функціонування систем обробки даних, використання їх ресурсів, діяльність обслуговуючого персоналу, а також порядок взаємодії користувачів і обслуговуючого персоналу із системою таким чином, аби найбільшою мірою ускладнити або виключити можливість реалізації загроз безпеці або знизити розмір втрат у випадку їх реалізації.

Фізичні заходи протидії загрозам національній безпеці засновані на застосуванні різного роду механічного, електро- або електронно-механічного обладнання і споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення й доступу потенційних порушників до компонентів об’єктів або систем, що й захищаються (зокрема – об’єктів критичної інфраструктури), а також засобів візуального спостереження, зв'язку й охоронної сигналізації.

Технічні заходи протидії загрозам національній безпеці пов’язані із використанням різного електронного обладнань і спеціальних програм, що входять до складу комплексів засобів захисту або виконують функції захисту. Зокрема, військово-технічні заходи передбачають створення й підтримку цілісної системи озброєння держави, що становить взаємопов'язану сукупність озброєння Збройних сил, інших військових формувань, органів, що забезпечує вирішення завдань оборонної безпеки країни на необхідному рівні. Цей рівень досягається в тому числі реалізацією військово-технічної політики – системи поглядів і практичних дій, реалізованих органами державної влади з метою військово-технічного забезпечення національної безпеки.

Організаційні й технічні заходи протидії загрозам національній безпеці можуть утворювати групу організаційно-технічних засобів забезпечення національної безпеки, яка включає:

- комплекс організаційних заходів (внутрішні правила, режими, регламенти тощо) і технічних засобів (використання програм і приладів для протидії загрозам національній безпеці);
- розробку (створення нових), експлуатацію й удосконалення вже наявних засобів протидії загрозам національній безпеці;
- перманентний контроль над дієвістю заходів протидії загрозам національній безпеці, який передбачає застосування відповідних методик оцінювання.

Кожна з груп заходів протидії загрозам національній безпеці залежно від характеру джерел загроз має зовнішній і внутрішній аспекти. Залежно від об'єкту національної безпеки, життєво важливі інтереси якого захищаються від внутрішніх і зовнішніх загроз, відповідні заходи реалізуються у площині забезпечення безпеки особистості, суспільства, держави тощо.

В цілому система заходів протидії загрозам національній безпеці вибудовується і функціонує відповідно до наступних основних принципів: законності; системності; комплексності; наступності і безперервності; своєчасності; постійного удосконалювання; розумної достатності заходів; персональної відповідальності; поділу функцій; мінімізації дискреційних повноважень; взаємодії та співробітництва складових сектору безпеки і оборони та інших суб'єктів; гнучкості системи захисту; відкритості алгоритмів і механізмів захисту; простоти застосування засобів захисту; наукової обґрунтованості і технічної придатності до реалізації; спеціалізації й професіоналізму; взаємодії й координації; обов'язковості контролю.

При цьому взаємодія відповідних заходів «в середині» системи відбувається наступним чином:

- нормативні й організаційно-розпорядчі документи розробляються та приймаються з урахуванням та на основі існуючих норм моралі й

етики;

- організаційні заходи забезпечують виконання існуючих нормативних актів і будуються з урахуванням існуючих правил поведінки, прийнятих у державі, органі, організації, установі тощо;
- втілення організаційних заходів вимагає розробки відповідних нормативних і організаційно-розпорядчих документів;
- для ефективного застосування організаційні заходи повинні бути підтримані фізичними й технічними засобами;
- застосування й використання технічних засобів захисту вимагає відповідної організаційної підтримки.

При цьому слід враховувати, що правові заходи мають подвійну природу, і можуть розглядатися як з точки зору форми (тоді мова йде про логічний взаємозв'язок: «правові-організаційні-технічні й фізичні заходи», за якого презюміюється, що правове підґрунтя повинні мати політичні, військові, економічні та інші заходи), так і з точки зору змісту (як самостійна за змістовним наповненням група заходів). Це ж стосується також і заходів інформаційного характеру, які не лише становлять самостійну групу заходів протидії загрозам національній безпеці, але й забезпечують та супроводжують реалізацію інших заходів, а також забезпечують обмін інформацією між різними елементами системи відповідних заходів. Тож СІО в системі засобів протидії загрозам національній безпеці України посідають особливе місце – як самостійний засіб реалізації заходів інформаційно-психологічного спрямування і як допоміжний засіб в реалізації політичних, економічних, військових та інших заходів, які без належної інформаційної підтримки приречені на неуспіх. Слід також зауважити, що СІО можуть реалізовуватись не лише при забезпечені інформаційної, але й інших складових національної безпеки, яка є складним та багатоаспектним феноменом.

СІО як засіб протидії загрозам національній безпеці характеризується

двома аспектами - розвідувальним, що забезпечує збір розвідувальної інформації про супротивника та здійснення необхідного впливу на нього, та контррозвідувальним, який пов'язаний із захистом власної інформації, інформаційної інфраструктури й протидією СІО супротивника.

Розвідувальні СІО. Швидкий розвиток інформаційних технологій, зростання їх можливостей за одночасного зниження їх відносної вартості, передусім у галузі систем передачі й розподілу інформації, диктує усе більш гостру необхідність створення нової архітектури систем, призначених для збору й обробки інформації, у тому числі розвідувальної. Така архітектура повинна забезпечити об'єднання сенсорних систем, розподільників інформації й систем зброї, причому кожний з її елементів має бути здатен діяти автономно, маючи доступ до узагальнених інформаційних ресурсів. За таких умов перевага розвідувальних СІО над традиційною розвідкою полягає в тому, що вони забезпечують отримання й використання інформації в реальному або близькому до реального масштабі часу, використовуючи адаптовані алгоритми доведення ненадлишкової інформації до безпосередніх споживачів і осіб, що ухвалюють рішення. Для забезпечення проведення розвідувальних СІО потрібні наступні основні компоненти (під мережі [5]):

- розгалужена структура так званих «сенсорів» або «датчиків», які забезпечують збір актуальної інформації, необхідної для вирішення завдань сектору безпеки і оборони, в режимі реального часу;
- система інформаційних комунікацій, що забезпечує передачу інформації споживачам у реальному масштабі часу;
- автоматична або автоматизована система попереднього аналізу й розподілу інформації;
- система обробки, аналізу й підтримки прийняття рішень на всіх ієрархічних рівнях, аж до самих нижніх.

Контррозвідувальні СІО. Якщо метою розвідувальних СІО є

оперативний збір, обробка й доведення до кінцевого користувача максимально повної інформації про супротивника, то головна мета контррозвідувальних СІО, відповідно, полягає в недопущенні одержання супротивником аналогічної інформації про власні сили й засоби або ж у її викривленні на кожному з рівнів системи збору розвідданих супротивника, у тому числі при передачі, проходженні й обробці інформації. Використання таких методів дозволяє підвищити керованість силами сектору безпеки і оборони, а також мінімізувати потенційні втрати у результаті протистояння. Іншим аспектом контррозвідувальних СІО є захист власних засобів одержання інформації від засобів ураження й заходів протидії супротивника. Одним з найбільш ефективних способів при цьому є спрощення й, відповідно, здешевлення систем до такого рівня, коли спроби їх фізичного знищення стають невиправдано витратними. Методи захисту інформації, що передбачають її викривлення, можуть виявитися найбільш ефективними в тому випадку, якщо відповідні дані виходять із розподілених систем інформації, що вимагають порівняння й доповнення даних різних джерел [6].

Зауважимо, що розвідувальний і контррозвідувальний аспект СІО проявляється на всіх етапах СІО незалежно від їх типу, виду та спрямування.

Так, О. Литвиненко у своїх наукових працях виділив наступні типи СІО:

- СІО, спрямовані проти суб'єктів прийняття рішень (наприклад, надання недостовірної інформації військовому командуванню чи державному керівництву (дезінформація), що може здійснюватись контактно або безконтактно (введення інформації через підставних осіб, поширення недостовірних чуток тощо);
- СІО, що мають на меті компрометацію об'єкта (проводяться шляхом поширення дискредитуючих даних про ціль СІО; наприклад, можуть

використовуються теми нетрадиційної орієнтації, наркоманії, етнічного походження тощо;

- СІО, спрямовані на дестабілізацію (економічну, політичну) ситуації (наприклад, дискредитація керівництва країни, посилення опозиційних настроїв, «ідеологічна диверсія» тощо) [7-10].

В сучасних умовах видається доцільним ввести наступну типологію СІО:

- СІО, об'єктом (ціллю) яких є конкретна особа або визначене коло осіб. У таких операціях цільовою аудиторією можуть виступати конкретні суб'єкти або коло осіб, причому як власне суб'єкти прийняття рішень, так і особи, які мають певний авторитет, наприклад, лідери суспільної думки;
- СІО, спрямовані на ініціювання, зміну напрямку розвитку, припинення чи «розмиття» певного процесу, явища чи події. Наприклад, метою таких СІО може бути ініціювання протестних рухів у державі. У такому випадку здійснюється штучне підвищення соціальної напруги шляхом фінансування, організації та висвітлення у вигідному для організаторів СІО світлі у мас-медіа протестних рухів, акцентування уваги суспільства на соціально-економічних проблемах, інспірація або навіть вигадування чи зміщення акцентів у описанні подій що призводить до поширення негативних настроїв у суспільстві, дискредитації державних керівників тощо;
- «Спін-операції» (від spin (англ.) – обертання). Такі СІО спрямовуються на формування дискурсу та формування «вікон Овертона» [11]. Фактично, організатор СІО - спін-доктор, інспірує дискусію навколо питання, явища, події тощо (предмету дискусії), в результаті чого виникають дві сторони дискусії - прихильники та противники, які в тій чи іншій мірі та різними способами демонструють своє відношення (наукові дослідження, публічні дискусії, інформаційні матеріали у ЗМІ, вуличні

акції тощо). В залежності від завдань, що стоять перед організаторами СІО, в процесі дискусії розширюється коридор можливого сприйняття суспільством предмету та зміщується відношення суспільства до предмету (класичним прикладом може слугувати питання легалізації наркотиків. Такі СІО можуть проводитись проти влади іншої країни то зазначені СІО можуть мати на меті базовий підрив авторитету влади через поширення сумнівів у правильності дій, відкриття альтернативи, порівняння із іншими країнами тощо.

Запропонована типологія передбачає збільшення цільової аудиторії СІО та варіативність впливу на цільову аудиторію. В результаті, на наш погляд, матеріально-технічні та людські ресурси сектору безпеки і оборони мають бути використані більш ефективно, оскільки передбачають застосування інструментів, прийомів та методів СІО не лише щодо безпосередніх об'єктів СІО, але й для впливу на суміжні аудиторії, досягаючи таким чином мультиплікації ефекту впливу СІО.

Відповідно необхідно актуалізувати і видологію СІО за такими ознаками:

- СІО в новинарній сфері – з використанням радіо, телебачення, періодичних друкованих ЗМІ (журнали, газети) та неперіодичних друкованих видань (листівки, плакати тощо);
- СІО в комунікативній сфері – використовуються електронні (on-line) соціальні мережі та фізичні (off-line) соціальні мережі;
- СІО в науковій та культурній сфері – впровадження «інформаційних закладок» до наукової та культурної літератури тощо.

СІО в новинарній сфері передбачають реалізацію комплексу заходів з використанням класичних ЗМІ (друковані, радіо та телебачення) через публікацію підготовлених матеріалів у відповідних медіа. До новинарної сфери також можуть бути віднесені неперіодичні видання або такі видання, що мають незначну кількість ітерацій друку. Ключова риса

зазначеного виду СІО – використання класичних та масових інструментів впливу на людську свідомість – телебачення, радіо, журнали та газети. Такі ЗМІ традиційно мають значне охоплення споживачів інформації хоча в той же час вимагають значних витрат матеріально-технічних ресурсів. Дещо окремо в цьому ряду стоять листівки, плакати, відкритки та інші неперіодичні друковані видання. Такі інструменти можуть мати значно менше охоплення аудиторії (в порівнянні із телебаченням та радіо), однак через значно нижчу ціну у виробництві та поширенні, існує можливість у масовому, швидкому та широкому використанні. Особливість таких інструментів інформаційно-психологічного впливу полягає у тому, що інформацію вони подають максимально стисло із використанням сугестивних прийомів впливу через текст та малюнок. Характерна риса листівок, плакатів та інших неперіодичних видань (в т.ч. і тих, що мають формат газет) – відвертий агітаційний, пропагандистський характер інформаційних матеріалів.

СІО в комунікативній сфері можуть бути як пов’язані з першим видом так і здійснюватися окремо. Необхідно розділити електронні (on-line) соціальні мережі (далі on-line мережі) та фізичні (off-line) соціальні мережі (далі off-line мережі) оскільки незважаючи на схожість родових ознак (соціальні мережа це соціальна структура, що утворена індивідуумами та (або) організаціями й демонструє різноманітні зв’язки між її членами) on-line соціальна мережа, з точки зору інформаційних та комунікативних технологій, створює умови для використання значно більшої кількості інструментів інформаційно-психологічного впливу а ніж off-line в силу технологічних можливостей з розміщення та доставки аудіо- та відеоінформації до адресата. On-line мережі, як було зазначено вище, мають значно більший спектр можливостей з розміщення та доставки інформації до адресата найрізноманітнішого характеру (відео, картинки, світлини, текст, аудіо). Швидкість поширення інформації в on-line мережі

значно більша ніж в off-line мережі в силу простоти передачі та мовлення. Окрім цього, варто зазначити такий важливий момент, що виробництво, поширення та доставка до адресата інформаційної продукції (контенту) для поширення в on-line мережі вимагає значно меншої витрати людських та матеріально-технічних ресурсів ніж в on-line мережі, у першу чергу за рахунок швидкості поширення та надзвичайно низьких витрат на мультиплікацію інформаційних матеріалів. Наприклад, для поширення усної інформації off-line мережею необхідно здійснити фізичний контакт з однією чи колом осіб і, відповідно, витратити на це час та певні зусилля. У випадку поширення друкованих матеріалів необхідно витратити час та ресурси на друк та поширення фізичних копій матеріалу. У випадку поширення інформації on-line мережею витрати на мультиплікацію інформації зводиться до натискання кнопки «поділитись», що значно зменшує витрати у порівнянні з off-line мережею. Необхідно зазначити, що бурхливий розвиток on-line мереж завдяки розвитку та поширенню інформаційних технологій фактично започаткував нову інформаційну епоху та загалом новий інформаційний простір як такий, оскільки зазначені мережі майже повністю дублюють off-line мережі у плані можливостей використання телебачення, радіомовлення, в певній мірі аналогів друкованих видань [12]. Серед недоліків on-line мереж можна зазначити високу інформаційну інфляцію, значний обсяг інформації, що може надходити до людини та, перш за все, необхідність наявності певної телекомунікаційної інфраструктури, відсутність якої зводить нанівець всі переваги on-line мереж. Тоді як off-line мережі існують з моменту виникнення життя на планеті і для свого існування не вимагають ніяких складних технічних засобів і взагалі, можуть існувати без якихось допоміжних засобів передачі, поширення та отримання інформації.

СІО в науковій і культурній сфері мають на меті закладення певних «інформаційних мін» в науковій та культурній літературі, що в

майбутньому обумовлює можливість використання таких технологій як «термінологічне мінування», що полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загально світоглядного та оперативно-прикладного характеру [13, с.110-116]. Такі СІО мають достатньо сильний вплив у інформаційному просторі та завдають значної шкоди у психологічній сфері через те, що «заміновані» терміни можуть закладатись в інформаційний базис інформаційних, пропагандистських, ідеологічних та інших кампаній при спрацьовуванні яких весь інформаційний базис буде зруйновано та направлено проти організаторів вищезазначених кампаній. СІО такого виду можуть бути як наступального характеру так і оборонного характеру. На нашу думку, під час наступальних СІО проводяться заходи із «термінологічного мінування» в інформаційний політиці опонента, через створення подвійного тлумачення подій, процесів, явищ, хибних висновків та їхнє поширення та укорінення із використанням прийомів сугестії. Такі «міни» спрацьовують у певний, задуманий організаторами, момент та наносить інформаційно-психологічну шкоду як організаторам інформаційних, пропагандистських, ідеологічних та інших кампаній так і підопічним особам (збройні сили у зоні конфлікту, підрозділи правоохоронців під час масових заворушень та загалом суспільство тощо). СІО оборонного спрямування мають на меті формування системи термінологічного мінування інформаційних, пропагандистських, ідеологічних та інших кампаній опонентів з метою нівелювання негативного інформаційно-психологічного впливу на підопічних осіб (збройні сили у зоні конфлікту, підрозділи правоохоронців під час масових заворушень та загалом суспільство тощо).

Проведення СІО як наступального, так і оборонного спрямування, характеризується розгалуженою системою методів, до якої входять зокрема, методи електронної та радіоелектронної боротьби, боротьби з

комунікаційними системами, криптографічної боротьби, методи інформаційно-психологічного впливу, «війни культур», методи «хакерської боротьби», методи «кібернетичної» або «мережної боротьби», методи економічного інформаційного протиборства тощо [14]. Перелік наведених груп методів не є вичерпним, так само, як і спектр методів у їх складі, оскільки динамічний розвиток суспільства та невпинна інформатизація всіх сфер його життєдіяльності зумовлює постійну появу нових. Слід також зауважити, що СІО будь-якого типу, виду та спрямування можуть супроводжуватись різноплановими заходами технічного характеру, що забезпечує синергетичний ефект у протидії загрозам національній безпеці України.

Висновки. СІО в системі засобів протидії загрозам національній безпеці України посідають особливе місце – як самостійний засіб реалізації заходів інформаційно-психологічного спрямування і як допоміжний засіб в реалізації політичних, економічних, військових та інших заходів, які без належної інформаційної підтримки приречені на неуспіх. Слід також зауважити, що СІО можуть реалізовуватись не лише при забезпечені інформаційної, але й інших складових національної безпеки, яка є складним та багатоаспектним феноменом. У свою чергу СІО, як інформаційно-правовий феномен класифікуються за спрямуванням, аспектами, типом та видом, а також характеризуються розгалуженим спектром методів, що можуть застосовуватись у ході їх проведення. перспективи вдосконалення інформаційно-правового забезпечення СІО в сучасних умовах залежать передусім від формування належного правового підґрунтя проведення СІО як на міжнародному рівні, так і на рівні національного законодавства.

Література

1. Про національну безпеку України: Закон України від 21.06.2018. URL: https://zakon.rada.gov.ua/laws/ show/2469-19 (дата звернення 09.04.2019)
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 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).
4. Силові та ненасильницькі методи забезпечення національної безпеки. URL: http://vabb.com.ua/assets/files/Tema_9_ONB.pdf
5. Ведение информационной войны США и их союзниками в ходе операции в Афганистане. URL: scef.ru/ru/oborona-i-bezopasnost/265/vedenie-informaczionnoj-vojni-ssha-i-ih-soyuznikami-v-hode-operaczii-v-afganistane/(дата звернення 13.04.2019)
6. Информационные вызовы национальной и международной безопасности. URL: www/pricentr.org|media/content/files/9/13464042510/pdf
7. Литвиненко О. В. Інформаційні впливи та операції: теорет.-аналіт. нариси. К.: Нац. ін-т стратегічних досліджень, 2003. 239 с.
8. Литвиненко О. Інформаційні впливи та інформаційні операції: механізми самоорганізації. Людина і політика. 1999. № 6.С. 32–36
9. Литвиненко О. В. Інформаційна безпека Європи: Конспект лекцій до курсу лекцій для студ. спец. «Між-нар. інформація» спеціалізації «Європ. комунікації». К. : Київ. ун-т ім. Т. Шевченка. Ін-т міжнар.

відносин, Центр європ. студій. Каф. міжнар. комунікацій та зв'язків з громадськістю, 1999. 61 с.

10. Литвиненко О.В. Спеціальні інформаційні операції: монографія. К.: НІСД, 1999. 163 с.
11. Nathan J. Russell An Introduction to the Overton Window of Political Possibilities. URL: https://www.mackinac.org/7504 (дата звернення 12.05.2019)
12. Мелещенко О.К. Взаємодія ЗМІ: нові форми як відповідь на виклики часу. URL: http://web.znu.edu.ua/herald/issues/archive/articles/2780.pdf (дата звернення 10.05.2019)
13. Присяжнюк М.М., Пампуха І. В., Петрик В. М. Основні поняття та особливості проведення спеціальних інформаційних операцій. Зб. наук. праць Військового інституту Київського нац. ун-ту ім. Т. Шевченка. 2014. № 46. С. 112–120.
14. Фролов Д.Б. Информационная война: эволюция форм, средств и методов. URL: cyberleninka.ru/article/n/informatsionnaya-voyna-evolyutsia-form-sredstv-i-metodov

References

1. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018. URL: https://zakon.rada.gov.ua/laws/ show/2469-19 (data zvernennia 09.04.2019)
2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 26.05.2015. URL: https://zakon.rada. gov.ua/laws/show/287/2015 (data zvernennia 09.04.2019)
3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 25.02.2017. URL: http://www.president.gov.ua /documents/ 472017-21374 (data zvernennia 28.11.2018).

4. Sylovi ta nenasylnytski metody zabezpechennia natsionalnoi bezpeky. URL: http://vabb.com.ua/assets/files/Tema_9_ONB.pdf
5. Vedenye ynformatsyonnoi voinы SShA y ykh soiuznykamy v khode operatsyy v Afhanystane. URL: scef.ru/ru/oborona-i-bezopasnost/265/vedenie-informaczionnoj-vojni-ssha-i-ih-soyuznikami-v-hode-operaczii-v-afganistane/(data zvernennia 13.04.2019)
6. Informatsyonnye vyzovy natsyonalnoi i mezhdunarodnoi bezopasnosti. URL: www/pricentr.org|media/content/files/9/13464042510/pdf
7. Lytvynenko O. V. Informatsiini vplyvy ta operatsii: teoret.-analit. narysy. K.: Nats. in-t stratehichnykh doslidzhen, 2003. 239 s.
8. Lytvynenko O. Informatsiini vplyvy ta informatsiini operatsii: mekhanizmy samoorhanizatsii. Liudyna i polityka. 1999. № 6.S. 32–36
9. Lytvynenko O. V. Informatsiina bezpeka Yevropy: Konspekt lektsii do kursu lektsii dlia stud. spets. «Mizh-nar. informatsiia» spetsializatsii «Ievrop. komunikatsii». K. : Kyiv. un-t im. T. Shevchenka. In-t mizhnar. vidnosyn, Tsentr yevrop. studii. Kaf. mizhnar. komunikatsii ta zv'iazkiv z hromadskistiu, 1999. 61 s.
10. Lytvynenko O.V. Spetsialni informatsiini operatsii: monohrafiia. K.: NISD, 1999. 163 s.
11. Nathan J. Russell An Introduction to the Overton Window of Political Possibilities. URL: https://www.mackinac.org/7504 (data zvernennia 12.05.2019)
12. Meleshchenko O.K. Vzaiemodiia ZMI: novi formy yak vidpovid na vyklyky chasu. URL: http://web.znu.edu.ua/herald/issues/archive/articles/2780.pdf (data zvernennia 10.05.2019)
13. Prysiazhniuk M.M., Pampukha I. V., Petryk V. M. Osnovni poniattia ta osoblyvosti provedennia spetsialnykh informatsiinykh operatsii. Zb. nauk.

prats Viiskovoho instytutu Kyivskoho nats. un-tu im. T. Shevchenka. 2014. № 46. S. 112–120.

14. Frolov D.B. Ynformatsyonnaia voina: эvoliutsyia form, sredstv y metodov. URL: cyberleninka.ru/article/n/informatsionnaya-voyna-evolyutsia-form-sredstv-i-metodov