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

Кваліфікаційна наукова
праця на правах рукопису

ВЕРГОЛЯС ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ

УДК: 342+327/008:351

ДИСЕРТАЦІЯ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Спеціальність 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право
Галузь знань – 081 (Право)

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____О.О. Верголяс

Науковий керівник − **ЗОЛОТАР Ольга Олексіївна,** доктор юридичних наук, старший науковий співробітник

Київ – 2020

АНОТАЦІЯ

Верголяс О.О. Правове забезпечення спеціальних інформаційних операцій». – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук (доктора філософії) за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» (08 – право). – НДІІП НАПрН України, Київ, 2020.

Дисертацію присвячено теоретичному визначенню, обґрунтуванню й розкриттю змісту правового забезпечення та нформаційно-правових засад спеціальних інформаційних операцій (далі – СІО), а також розробленню конкретних пропозицій щодо удосконалення правового забезпечення СІО.

Емпіричну базу дослідження становлять матеріали навчальної, навчально-методичної літератури з проблематики інформаційного права та забезпечення національної безпеки, публікацій у ЗМІ, аналітичні матеріали, статистичні дані тощо. Збирання, оброблення й аналіз статистичної та соціологічної інформації здійснювалися із дотриманням вимог репрезентативності, що висуваються до подібних досліджень. Нормативно-правовою основою роботи стали як Конституція та законодавство України, зарубіжних країн, міжнародно-правові акти, що регулюють питання національної та державної безпеки, інформаційного протиборства та характеризують специфіку інформаційно-правового забезпечення СІО.

У дослідженні розглянуто історіографію та сучасний стан наукової розробки проблематики правового забезпечення СІО. З’ясовано, що не зважаючи на те, що інформаційний вплив використовувався в ході соціальних конфліктів (в тому числі збройних) з давніх давен, хвиля технічного прогресу внесла істотні зміни в методи вирішення геополітичних, військових, економічних, торговельних і інших конфліктів, тож силові методи наразі поступаються місцем методам інформаційним.

У міру накопичення досвіду практичного здійснення інформаційного впливу на цільову аудиторію у більш широкому розумінні у військових

конфліктах, економічних суперечках, політичній боротьбі тощо виникла потреба в його теоретичному осмисленні, що викликало до життя науковий інтерес до проблематики інформаційної війни та застосування інформаційної зброї, проведення СІО тощо. Втім наразі в науці інформаційного права залишаються практично недослідженими проблеми інформаційно-правового забезпечення СІО.

Визначено, що ключовими у понятійно-категоріальному апараті дослідження є наступні поняття: інформаційна безпека, інформаційна загроза, інформаційна війна, інформаційна зброя, інформаційні операції, правове забезпчечення СІО, інформаційно-правове забезпечення СІО, які належать до базових категорій інформаційного права, уточнено зміст відповідних понять.

Доведено, що концепція інформаційної війни, у становленні якої наразі вирізняють чотири покоління, передбачає використання інформаційної зброї шляхом проведення інформаційних операцій, різновидом яких є СІО. СІО у веденні інформаційної війни та забезпеченні національної безпеки можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки інформаційного протиборства. СІО обох типів, а так само комплексні СІО можуть проводитися на оперативно-тактичному, стратегічному й глобальному рівнях з метою оперативної або стратегічного маскування конфліктуючими сторонами своїх реальних військових, геополітичних, політичних, економічних задумів, завдань і намірів, а також з метою дискредитації дій імовірного супротивника, його державної політики, економічних структур тощо. Класичним прикладом використання СІО в оборонній інформаційній війні або з метою забезпечення національної безпеки, можуть вважатися антитерористичні СІО. Важливою складовою антитерористичних СІО є інформаційно-психологічний вплив не тільки на терористів, але й на цивільне населення, у тому числі на суспільну думку як у власній, так і у закордонних країнах.

Визначено, що головна ідея і основні положення концепції дослідження відображені в гіпотезі, відповідно до якої належне правове та інформаційно-правове забезпечення СІО на основі норм та принципів інформаційного права

дозволить підвищити ефективність проведення СІО, що сприятиме забезпеченню національної безпеки України та досягненню нашою державою інформаційних переваг у реальних та потенційних інформаційних конфліктах, в т.ч. в ході гібридної війни. Оскільки методологія вважається головним орієнтиром наукового пошуку, надійним засобом встановлення істини в галузях науки, окреслено методологію дослідження організаційно-правових і теоретико-методологічних засад інформаційно-правового забезпечення СІО становить систему методів (способів і прийомів), а також сукупність принципів, застосування яких уможливлює одержання нових знань щодо організації та проведення СІО.

Констатовано, що правове підґрунтя проведення СІО може бути окреслено наступними напрямками: нормативно-правові акти, що визначають обмеження і заборони при проведенні СІО (до цієї групи належать міжнародно-правові акти з питань протидії інформаційним загрозам, забезпечення інформаційної безпеки й регулювання інформаційного протиборства, а також акти національного інформаційного законодавства, присвячені регламентації інформаційних правовідносин та інформаційної сфери); нормативно-правові акти, що регламентують порядок і процес проведення СІО (до цієї групи належать внутрішньодержавні нормативно-правові акти відомчого характеру, які переважно мають закритий характер), а також здійснено дослідження відповідних нормативно-правових актів.

У дослідженні відзначається, що теоретико-методологічні засади інформаційного забезпечення СІО наразі характеризуються розгалуженим інструментарієм, який може успішно використовуватись як у військовий, так і у мирний час для різної цільової аудиторії. Так, СІО можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, тобто, охоплювати всі напрямки інформаційного протиборства, а також поводитись на стратегічному, операційному і тактичному рівнях. Сформульовані основні принципи планування та проведення СІО, а також визначені основні інструменти та методи, що мають використовуються в ході СІО за стандартами НАТО. Визначено, що взяття відповідних теоретико-методологічних

напрацювань «на озброєння» сектором безпеки і оборони України та його нормативно-правове закріплення на рівні відомчих документів значно посилить спроможності нашої держави у веденні інформаційного протиборства в умовах гібридної війни.

За результатами аналізу актуальних загроз національній безпеці України визначено та систематизовано актуальні основні засоби протидії зазначеним загрозам. Так, 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. Доведено, що СІО в системі засобів протидії загрозам національній безпеці України посідають особливе місце – як самостійний механізм реалізації заходів інформаційно-психологічного спрямування і як допоміжний захід в реалізації політичних, економічних, військових та інших заходів, які без належної інформаційної підтримки приречені на неуспіх. СІО можуть реалізовуватись не лише при забезпечені інформаційної, але й інших складових національної безпеки, яка є складним та багатоаспектним феноменом.

З’ясовано, що основною проблемою правового забезпечення СІО в умовах сьогодення є відсутність достатнього законодавчого унормування їх проведення. Відповідно, відсутнє й достатнє законодавче підґрунтя для розробки методологічних засад інформаційного забезпечення СІО. Це передусім зумовлює потребу у законодавчому визначенні заборон при здійсненні інформаційного впливу, в тому числі в ході проведення СІО, які визначатимуть межі їх проведення, адже в Україні, як у демократичній правовій державі, діяльність державних органів влади, відповідальних за забезпечення національної безпеки має ґрунтуватися на нормах закону і здійснюватись з дотриманням конституційних прав та свобод людини.

Викладено пропозиції, спрямовані на підвищення ефективності інформаційно-правового забезпечення СІО, зокрема, запропоновано внесення низки змін до чинного законодавства України в ході розробки змін до Закону

України «Про Службу безпеки України» та при розробці Закону України «Про розвідку», а також запропоновано розробити загальнодержавну Концепцію стратегічних комунікацій, у якій доцільно закріпити визначення СІО.

Зазначено, що в сучасних умовах необхідним є формування з використанням принципів тензорної методології сінергетичної 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 аудитиорії: 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 (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 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»), а також поширити на СІО закономірності правового регулювання стратегічних комунікацій.

Розроблено алгоритм проведення СІО з урахуванням сучасних реалій гібридної війни та актуальних стандартів НАТО, актуалізовано класифікацію СІО за типом та видом. Запропонована класифікація СІО, а також системний підхід до планування та підготовки СІО на базі відповідного алгоритму, слугує підґрунтям для побудови матриці інформаційно-правового забезпечення синергетичної моделі СІО, застосування якої складовими сектору безпеки і оборони України дозволить підвищити ефективність інформаційно-правового забезпечення СІО та сприятиме підвищенню їх результативності.

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

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Верголяс О.О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право.* 2018. № 4. С. 126-133
2. Верголяс О.О. Спеціальні інформаційні операції в системі засобів протидії загрозам національній безпеці України. *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки».* 2019. №4. С.7-16
3. Верголяс О.О. Міжнародно-правове регулювання інформаційного протиборства: реалії та перспективи. *Visegrad Journalon Human Rights*. 2019. №3. С. 58-63
4. Верголяс О.О. Проблемні питання проведення спеціальних інформаційних операцій сектором безпеки і оборони України. *Юридичний науковий електронний журнал.* 2019. №4. С. 102-105
5. Верголяс О.О. Перспективи вдосконалення інформаційно-правового забезпечення спеціальних інформаційних операцій. *Підприємництво, господарство і право*. 2019. №7. С. 135-139
6. Верголяс О.О. Спеціальні інформаційні операції як інструмент геополітичних змін. *Юридичний бюлетень : наук. журн. / редкол. : О. Г. Предместніков та ін. – Одеса, ОДУВС*, 2019. Вип. 9 (9). С. 16-23.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Верголяс О.О. Перспективи криміналізації статті 173-1 кодексу України про адміністративні правопорушення. *Информационные технологии и безопасность. Материалы XV Международной научно-практической конференции ИТБ-2015*. К.: ИПРИ НАН Украины, 2015. С. 42-46.
2. Верголяс О.О. Стандарти НАТО у сфері проведення спеціальних інформаційних операцій. *Матеріали Міжнародної науково-практичної конференції «Юридична наука: виклики і сьогодення»*. 2018. С. 72-76.
3. Верголяс О.О. Спеціальні інформаційні операції у веденні інформаційної війни. *International scientific and practical conference «Legal practice in EU countries and Ukraine at the modern stage» Vasile Goldis Western University of Arad, Romania. January 25–26,* 2019. С. 312-315.

ANNOTATION

Verholyas O.O. Legal support of special information operations.- Qualifying scientific work on the rights of the manuscript.

Thesis for a Candidate Degree in Law (Doctor of Philosophy) in specialty 12.00.07 "Administrative Law and Process; finance law; information law "(08 - Law). – Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine, Kyiv, 2020.

Thesis is devoted to the definition, justification and disclosure of the theoretical foundations of the information and legal provision of special information operations (hereinafter – SIO), as well as the development of concrete proposals for improving the information and legal provision of SIO.

The empirical basis of the study is the materials of educational and methodological literature on the issues of information law and national security, publications in the media, analytical materials, statistics, etc. The collection, processing and analysis of statistical and sociological information was carried out in compliance with the requirements of representativeness, put forward for such studies. The normative legal basis of the work was as the Constitution and legislation of Ukraine, foreign countries, international legal acts regulating the issues of national and state security, information confrontation and characterizing the specifics of information and legal provision of SIO.

The research considers the historiography and the current state of scientific development of the issues of informational and legal support of SIO. It has been found that despite the fact that information influence has been used during social conflicts (including armed ones) since ancient times, a wave of technological progress has made significant changes in the methods of solving geopolitical, military, economic, trade and other conflicts, so power methods are now giving way to informational methods. As the experience of practical implementation of the information influence on the target audience in the wider sense in military conflicts, economic disputes, political struggle, etc., arose the need for its theoretical

understanding, which brought to life a scientific interest in the issues of information warfare and the use of information weapons, the conduct of CIO, etc. However, the problems of information and legal provision of SIOs, which are a tool for conducting information wars and a means of ensuring national security, are still insufficiently studied.

It is determined that the key concepts in the research categorical are the following: information security, information threat, information warfare, information weapons, information operations, information and legal support, etc., most of which belong to the categories of information law. It is proved that the concept of the information war, in the formation of which is currently distinguished by four generations, involves the use of information weapons through information operations, including SIO. SIO as a tool for conducting an information warfare and a means of ensuring national security can be both informational, and informational and psychological, covering all areas of information confrontation. SIO of both types, as well as complex SIO, can be conducted at the operational-tactical, strategic and global levels for the purpose of operational or strategic masking by the conflicting parties of their real military, geopolitical, political, economic plans, tasks and intentions, as well as in order to discredit actions of probable the enemy, his state policy, economic structures, etc. A classic example of the use of SIO in a defensive information warfare, that is, as a means of ensuring national security, can be considered anti-terrorist SIO. An important component of the anti-terrorist SIO is the informational and psychological impact not only on terrorists, but also on the civilian population, including on public opinion both in its own and in foreign countries. It is determined that the main idea and the main provisions of the concept of research are reflected in the hypothesis, which is based on the assumption that the creation and implementation of an effective mechanism of information and legal provision of SIO based on the relevant rules of law will increase the effectiveness of the SIO, which will contribute to ensuring Ukraine's national security and achievement of information advantages in real and potential information conflicts, as far as hybrid war. Since the methodology is considered as the main reference point for scientific research, the methodology of the study of organizational-legal and theoretical and

methodological foundations of the information and legal support of the SIO is a system of methods (methods and techniques), as well as a set of principles whose application makes it possible to obtain new knowledge on the organization and implementation of SIO.

It is stated that the legal basis for conducting SIO can be outlined in the following directions: in the conduct of SIO (this group includes international legal acts on issues of countering information threats, providing information security and regulation of information confrontation, as well as acts of national information legislation on the regulation of information legal relationships and information sphere); normative legal acts that regulate the procedure and process of conducting SIO (this group includes domestic state legal acts of a departmental character, which are mainly full of classified information), as well as the study of relevant regulatory acts has done.

Noted that the theoretical and methodological foundations of information provision SIO are currently characterized by ramified tools that can be successfully used both in military and in peacetime for different target audiences. Thus, SIO can be both technical or psychological, that is, cover all areas of information confrontation, as well as behave strategically, operationally and tactically. The main principles of SIO planning and implementation are formulated, as well as the main tools and methods used in the SIO for NATO standards are defined. It is determined that taking the relevant theoretical and methodological achievements "on arms" by the security and defense sector of Ukraine and its legal regulation at the level of departmental documents will considerably increase the capacity of our state in conducting information confrontation in the conditions of hybrid warfare. According to the results of the analysis of actual threats to the national security of Ukraine, the main basic means of counteracting these threats are identified and systematized. So, today the following groups of fixed assets (measures) of counteraction to traditional and new threats to national security: political-diplomatic; military; legal (legislative); information psychological; economic; scientific and technological; organizational (administrative and procedural); physical technical (hardware and software), etc. It is proved that the SIO in the system of means of

counteracting threats to national security of Ukraine occupy a special place - as an independent means of realization of events of information and psychological direction and as an auxiliary means in the realization of political, economic, military and other measures, which, without proper information support, are doomed to failure. SIO can be implemented not only with the information provided, but also other components of national security, which is a complex and multidimensional phenomenon.

It was found out that the main problem of information and legal support of SIO in the current conditions is the lack of sufficient legal norms for conducting them. Accordingly, there is no sufficient normative background for the development of the methodological foundations of the information provision of SIO. This primarily entails the need for normative legal definition of prohibitions in the implementation of information influence, including during the conduct of SIO, which will determine the limits of their implementation, since in Ukraine, as in a democratic state governed by the rule of law, the activities of state bodies responsible for ensuring national security have to be organized on the legal norms that ensure the constitutional rights and freedoms of citizens.

The proposals aimed at improving the effectiveness of the information and legal support of the SIO are presented, in particular, it is proposed to introduce a number of changes to the current legislation of Ukraine during the development of amendments to the Law of Ukraine "On the State Security Service of Ukraine" and in the development of the Law of Ukraine "On Intelligence Services", and also proposed to develop a nationwide Concept of Strategic Communications, in which it is expedient to consolidate the next definition of SIO.

It is noted that in modern conditions it is necessary to formulate using the principles of the tensor methodology of the synergetic model of SIO, which will combine models aimed at changing the attitude towards the object, changing behavior and changing the outlook. The synergistic model of the SIO is intended to address the following main tasks in relation to a specific target auditory: changes in the attitude to a particular object or action; behavioral changes; changes in perception of the world and worldview (while at the same time preventing the achievement of similar

goals by the population of Ukraine by foreign states, their special services, separate organizations and communities (including those engaged in terrorist or other criminal activity), individuals acting to the detriment of Ukraine's national security etc). Using the principles of tensor methodology will integrate into the synergistic model of the SIO experience of counter-network combat, which involves the use of subnets (subnetting sensors or sensors: subnet communication, subnet analysis of information, subnet "decision-making nodes", subnet "executive nodes")

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

Keywords: information security, information war, information weapons, special information operations, information and legal basis, legal support of SIO.

SPYSOK OPUBLIKOVANYKH PRATS ZA TEMOIU DYSERTATSII

NAUKOVI PRATSI, V YAKYKH OPUBLIKOVANI OSNOVNI NAUKOVI REZULTATY DYSERTATSII:

1. Verholias O.O. Informatsiino-pravove zabezpechennia spetsialnykh informatsiinykh operatsii. Informatsiia i pravo. 2018. № 4. S. 126-133

2. Verholias O.O. Spetsialni informatsiini operatsii v systemi zasobiv protydii zahrozam natsionalnii bezpetsi Ukrainy. Mizhnarodnyi naukovyi zhurnal «Internauka». Seriia: «Iurydychni nauky». 2019. №4. S.7-16

3. Verholias O.O. Mizhnarodno-pravove rehuliuvannia informatsiinoho protyborstva: realii ta perspektyvy. Visegrad Journalon Human Rights. 2019. №3. C. 58-63

4. 4. Verholias O.O. Problemni pytannia provedennia spetsialnykh informatsiinykh operatsii sektorom bezpeky i oborony Ukrainy. Yurydychnyi naukovyi elektronnyi zhurnal. 2019. №4. S. 102-105

5. Verholias O.O. Perspektyvy vdoskonalennia informatsiino-pravovoho zabezpechennia spetsialnykh informatsiinykh operatsii. Pidpryiemnytstvo, hospodarstvo i pravo. 2019. №7. S. 135-139

6. Verholias O.O. Spetsialni informatsiini operatsii yak instrument heopolitychnykh zmin. Yurydychnyi biuleten : nauk. zhurn. / redkol. : O. H. Predmestnikov ta in. – Odesa, ODUVS, 2019. Vyp. 9 (9). S. 16-23.

Naukovi pratsi, yaki zasvidchuiut aprobatsiiu materialiv dysertatsii:

7. Verholias O.O. Perspektyvy kryminalizatsii statti 173-1 kodeksu Ukrainy pro administratyvni pravoporushennia. Ynformatsyonnыe tekhnolohyy y bezopasnost. Materyalы XV Mezhdunarodnoi nauchno-praktycheskoi konferentsyy YTB-2015. K.: YPRY NAN Ukraynы, 2015. S. 42-46.

8. Verholias O.O. Standarty NATO u sferi provedennia spetsialnykh informatsiinykh operatsii. Materialy Mizhnarodnoi naukovo-praktychnoi konferentsii «Iurydychna nauka: vyklyky i sohodennia». 2018. S. 72-76.

9. Verholias O.O. Spetsialni informatsiini operatsii u vedenni informatsiinoi viiny. International scientific and practical conference «Legal practice in EU countries and Ukraine at the modern stage» Vasile Goldis Western University of Arad, Romania. January 25–26, 2019. S. 312-315.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АІВ – акції інформаційного впливу

ЄС, Євросоюз – Європейський Союз

ЗС України – Збройні Сили України

КК України – Кримінальний кодекс України

КПК України – Кримінальний процесуальний кодекс України

КМ України – Кабінет Міністрів України

КПК України – Кримінальний процесуальний кодекс України

МВС України – Міністерство внутрішніх справ України

МО України - Міністерство Оборони України

НАТО – Організація Північно-Атлантичного договору

ОБСЄ – Організація з безпеки та співробітництва в Європі

ООН – Організація Об’єднаних Націй

НЛП – нейролінгвістичне програмування

РФ – Російська Федерація

СБ України – Служба безпеки України

СІА – Спеціальні інформаційні акції

СІО – Спеціальні інформаційні операціїї

США – Сполучені штати Америки

ВСТУП

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

Серед науковців, що займалися дослідженням проблематики СІО з різних точок зору, можуть бути названі О. Баранов, І. Бачило, К. Бєляков, Н. Брусніцин, Т. Вронська, О. Довгань, О. Дзьобань, І. Доронін, В. Голубко,

Г. Грачов, О. Золотар, М. Ємельянов, Є. Єрофєєв, О. Копан, В. Копилов, Д. Ланде, О. Литвиненко, В. Лопатін, А. Манойло, В. Мельник, І. Мірошник, С. Онопрієнко, І. Панарин, І. Панова, В. Панченко, В. Пилипчук, Г. Почепцов, Ю. Просвирнин, М. Рассолов, Н. Савінова, О. Стрельцов, Т. Ткачук, Ю. Уфімцев, А. Фатьянов, А. Явтушенко та інші. Проблематиці інформаційних війн, інформаційних операцій, інформаційних впливів тощо буди присвячені дисертаційні дослідження К. Будиліна, В. Гарєва, О. Горбєнка, О. Губарєва, О. Денщикова, Г. Крилова, О. Потьомкіна, Д. Фролова, Д. Щербини тощо. Втім зазначені дослідження стосуються радше філософських, технічних, військових, політологічних, соціологічних тощо, аніж правових аспектів забезпечення інформаційної безпеки. Натомість актуальні підходи до визначення сутності і особливостей проведення СІО під кутом права висловлені у наукових працях О. Заруби, О. Кушнір, В. Ліпкана, В. Петрика тощо. Слід згадати також дисертаційні дослідження О. Кубишкіна, В. Разуваєва, О. Тамодліна тощо.

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

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

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

Мета і завдання дослідження. *Мета дослідження* полягає у теоретичному визначенні, обґрунтуванні й розкритті сутності правового

забезпечення СІО, а також у напрацюванні конкретних пропозицій щодо його удосконалення.

Досягнення мети здійснюється шляхом вирішення таких *завдань*:

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

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

– визначити методологію дослідження;

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

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

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

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

Предмет дослідження – правове забезпечення СІО.

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

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

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

– аналогії та компаративістики – для поглибленого дослідження теоретичних, організаційних та правових засад проведення СІО та їх

інформаційного забезпечення в Україні та зарубіжних державах, вироблення шляхів оптимізації інформаційно-правового забезпечення СІО (розділи 2, 3);

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

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

Зі спеціальних методів під час дослідження використано:

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

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

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

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

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

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

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

забезпечує єдність методів, практичної діяльності й теорії, емпіричних і наукових знань.

Емпіричну базу дослідження становлять матеріали навчальної, навчально-методичної літератури з проблематики інформаційного права та забезпечення національної безпеки, публікацій у ЗМІ, аналітичні матеріали, статистичні дані тощо. Збирання, оброблення й аналіз статистичної та соціологічної інформації здійснювалися із дотриманням вимог репрезентативності, що висуваються до подібних досліджень. Нормативно-правовою основою роботи стали Конституція та законодавство України, законодавство зарубіжних країн, міжнародно-правові акти, що регулюють питання безпеки, інформаційного протиборства тощо.

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

уперше:

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

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

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

– розроблено теоретичні засади правового забезпечення синергетичної СІО.

удосконалено:

– наукове уявлення про СІО;

– класифікацію СІО за типом і видом;

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

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

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

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

дістали подальший розвиток:

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

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

– концепція мережної боротьби в інформаційному просторі.

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

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

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

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

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

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

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

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

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, які поділяються на дев’ять підрозділів, висновків, списку використаних джерел (262 найменування на 22 сторінках), 5 додатків (на 52 сторінках). Повний обсяг дисертації становить 288 сторінок, із них основний текст – 209 сторінок.

РОЗДІЛ 1. Становлення та формування наукового знання з проблематики правового забезпечення спеціальних інформаційних операцій

1.1. Історична ретроспектива становлення та сучасний стан наукового знання з проблематики правового забезпечення спеціальних інформаційних операцій

Актуальною проблемою в сфері забезпечення міжнародної й національної безпеки сьогодні є адекватне реагування на появу нових викликів і загроз у різних сферах життєдіяльності світового співтовариства. Успішне вирішення цієї проблеми в умовах глобальних трансформацій сучасності неможливо в рамках застосування традиційних підходів до прогнозування загроз та до забезпечення належного рівня колективної й національної безпеки, тож першочергового значення набуває усвідомлення та належна оцінка значення інформації та інформаційної складової розвитку сучасної цивілізації, що є предметом уваги не лише наук безпекового циклу, але й інформаційного права.

Відзначаючи в цілому позитивну роль переходу до інформаційного суспільства (зокрема, в Окінавській Хартії глобального інформаційного суспільства [175] особливо підкреслені потенційні переваги інформаційно-комунікаційних технологій, що стимулюють конкуренцію, сприяють розширенню виробництва, створюють і підтримуючі економічне зростання та забезпечують занятість населення), що полягає передусім у переході до нових засад обробки й передачі інформації з метою підвищення ефективності функціонування багатьох сфер діяльності, необхідно також констатувати, що позитивні властивості інформації й інформаційних технологій можуть використовуватись не лише в цілях сталого розвитку суспільства, але й в корисливих і злочинних цілях. Хвиля технічного прогресу внесла істотні зміни також в методи вирішення геополітичних, військових, економічних, торговельних і інших конфліктів, тож силові методи наразі поступаються місцем методам інформаційним.

Поняття "ноосфери", запропоноване французьким ученим Е. Леруа та

розвинене його сучасниками П.Тейяр де Шарденом та В.Вернадським, наприкінці минулого століття набуло нового значення. Так, наприкінці 90-х експерти аналітичного центру RAND адміністрації США Дж.Аркілла та Д.Ронфельд запропонували об'єднати існуючі поняття кіберпростору й інформаційної сфери як сукупності кіберпростору й засобів масової інформації в єдину "ноосферу" - засновану на ідеях, духовних цінностях, етиці епістемологічну парадигму, у якій на зміну традиційній політиці "грубої" сили з її акцентом на матеріальну складову протиборства приходить нова, заснована на "м'якій силі", так звана «ноовійна», війна інформаційна [9]. Інформаційна війна становить різновид бойових дій, зброєю в яких виступають обладнання й методи обробки інформації, що дозволяють цілеспрямовано, швидко й потай впливати на військові й цивільні інформаційні системи супротивника з метою підриву його політики, економіки, боєздатності, в остаточному підсумку - національної безпеки. [85, с. 108-109, 204].

Ще в давнину протиборчі сторони намагалися використовувати засоби духовного впливу, аби послабити моральний дух і бойову міць супротивника, а також підняти бойовий дух своїх військ. Разом з інформаційно-психологічним впливом на особовий склад супротивника та його командування здійснювався також інформаційно-психологічний вплив на цивільне населення. Це була історично перша форма інформаційного впливу – фактично, інформаційно-психологічне забезпечення бойових дій. Необхідно зазначити, що на той час були мало поширений звичай служби за договором (за виключенням професійних воїнів – найманців), як це поширено сьогодні, тому питання одночасного інформаційно-психологічного впливу на збройні сили та на цивільне населення стояло на першому плані.

Способи ведення інформаційного протиборства в той період були обмежені вербальними технологіями (виступи ораторів, релігійних проповідників, поширення чуток, дезінформації, театральні вистави тощо.), наочними засобами залякування (демонстрація військової переваги, страхітливі знаки, пропагандистські письмена на каменях, деревах і будівлях тощо) і фізичної протидії (арешти, вбивства ораторів тощо). Серед найважливіших

суб'єктів інформаційного протиборства того часу були священнослужителі, публічні особи, політики та інші як освічені особи, які володіли значним впливом на всі соціальні верстви населення та були лідерами суспільної думки і мали авторитет у суспільстві. При цьому поява перших писемних засобів не грала помітну роль в здійсненні інформаційного впливу, так як на той період основна маса солдатів і цивільного населення були неписьменні.

В цей період активно використовувались такий невербальні інструменти як чутки. Так, наприклад, Ксеркс I під час греко-перської війни поширював чутки про багато чисельність власного війська (легендарний епізод, коли посол персів сказав царю Леоніду про те, що один залп з усіх луків перської армії закриє Сонце), татаро-монголи поширювали чутки про свою безжальність а також підірвали довіру до власного керівництва[75]. Варто додати, що чутки, за своєю природою, здатні посилювати першозакладений зміст, мають значну швидкість поширення та видозмінення. В умовах великої соціальної напруги такий інструмент інформаційно-психологічного впливу може мати значну ефективність на цільову аудиторію [118].

Другий, "паперовий" етап розвитку інформаційного впливу почався з поширенням письменності, в умовах широкого охоплення населення новими носіями інформації: листами, книгами, газетами, журналами тощо. В цей період з'явився і спеціальний ефективний засіб інформаційного протиборства, що використовується до цих пір - листівка.

Значний поштовх на розвиток та поширення прийомів інформаційно-психологічного впливу на супротивника дало відкриття друкарського верстату. Першою війною, під час якої вперше отримало значне поширення друкованих інформаційних матеріалів, була Тридцятилітня війна (1618-1648 рр.), остання і найбільш значна релігійна війна між католиками та протестантами у Європі, під час якої власне і виник термін «пропаганда» (від лат. *Sacra Congregatio de Propaganda Fide - конгрегація пропаганди віри*), як механізм протидії поширенню протестантизму у Європі) [176].

Цікавий епізод з історії війн, який яскраво ілюструє важливість використанні інформаційного впливу як на населення, так і на збройні сили

супротивника – кампанії Наполеона Бонапарта, під час яких він активно використовував пресу. Варто зазначити, що Наполеон використовував ЗМІ не тільки під час військових походів, але й для закріплення та утримання при владі. Зокрема, військовим операціям армії Наполеона, як правило, передувало поширення чуток про значно перебільшену чисельність наполеонівських військ, після чого слідувало поширення памфлетів і листівок. Для цього в армії Наполеона була похідна друкарня з набором іноземних шрифтів. Йому належать слова: «Чотири газети зможуть заподіяти більше зла, ніж стотисячна армія». Преса, вважав Наполеон, повинна писати тільки те, що їй накажуть, і мовчати про те, що їй не слід говорити. Через свого міністра поліції Наполеон часто віддавав газетам накази збивати з пантелику ворога помилковими відомостями. Голова французької секретної служби за Наполеона Ж.Фуше був першим шефом поліції, що виділив ЗМІ як суб'єкт та об'єкт поліцейської діяльності. В організованій ним поліцейській системі він створив відділ преси та відділ театру і газет, запросивши до них кращих журналістів країни. Фуше вважав, що таємна поліція повинна правильно оцінювати інтелект супротивника і протистояти йому [158].

Значного поширення друковані засоби передачі інформації (листівки, газети, брошури) отримали у період між наполеонівськими війнами та Першою світовою війною, через здешевлення та спрощення виробництва таких матеріалів. З розвитком повітроплавання почали використовувати літаки та дирижаблі для розкидування листівок на позиції супротивника з повітря.

Перше в історії воєн використання пропагандистського тексту, який об'єднав в собі заклик аудиторії до певних практичних дій з документом, що мали юридичну силу і тому становиться особливо важливим для пропагованих, належить М.Кутузову. Таким текстом було звернення М.Кутузова до населення Польщі 8 січня 1813 року. Віддруковане значним накладом у вигляді листівки звернення мало в кінці особливу застереження: "Примірник цього оголошення всякому, хто має його, служить замість охоронного листа". Подальший розвиток об'єднання пропагандистського тексту з документом призвело до створення в роки Першої світової війни добре відомої форми пропаганди

полону у вигляді листівки-пропуску [158].

Третьому етапу розвитку інформаційного протиборства («електронному») дало початок виникнення нових носіїв інформації і нових засобів доставки інформації, що з'явилися завдяки відкриттю електрики: телеграфу, телефону, радіо, кіно, телебачення тощо.

Поступовий розвиток комунікацій закономірно призвів до значного пришвидшення поширення інформації. У першій половині XIX століття створюються перші інформаційні агентства, які дотично надають поштовх до розвитку торгових бірж. Більшої суспільної ваги набувають мас-медіа спершу у вигляді газет а з часом радіо- та телебачення, а вже наприкінці XX століття - на початку XXI століття стрімко набирає популярності, поширення та важливості мережа Інтернет, яка включає у себе не тільки окремі WEB сторінки, але й соціальні мережі, форуми, різні інформаційні сервіси тощо. З цього моменту виникає два важливих питання у інформаційній сфері: контроль інформаційного простору та інструменти збирання й поширення інформації.

З початку XIX століття систематизується робота інституту цензури у всіх розвинених на той час країнах [95] та спостерігається створення інформаційних агентств, роль яких полягає у зборі та поширенні інформації про події, явища та процесі в усьому світові. Керівництво різних держав остаточно усвідомлює важливість ЗМІ як інструменту політичної боротьби та зброї проти військового супротивника, створюються державні теле- та радіоканали.

В той же час помітно зростають масштаби збройних конфліктів та воєн, чисельність збройних сил та масовість військових операцій, у битвах беруть участь декілька сотень тисяч солдат з обох боків, відбувається еволюція військової думки від тактики генеральної битви до окопної війни, фронтів та локальних військових операцій. Відповідно до потреб, тактики і стратегії військових дій відбувається і розвиток науково-теоретичних розробок у сфері інформаційно-психологічного протиборства та інформаційного впливу.

Так, все більша увага приділялась роботі військових штабів із ЗМІ та інформаційними агентствами через які поширювалась спеціально підготовлена інформація. Так, наприклад, у Великій Британії було створено Управління з

пропаганди у ворожих країнах, який очолив медіа-магнат лорд А.Нотклiф, засновник газети «Daily Mail», який у 1914 році контролював 40% всього газетного рику Великої Британії. Як і Велика Британія, керівництво США створило аналогічну структуру – Комітет з публічної інформації (неофіційна назва - «Комітет Кріля», на честь його керівника – Дж. Кріля, журналіста за фахом).

Німеччина увійшла у Першу світову війну лише з одним прес-офіцером а впродовж війни військове керівництво перейшло до практики щотижневих брифінгів та створенні управління при Генеральному штабі [21; 24]. Німецька розвідка напередодні і в ході Першої світової війни (а пізніше - і Другої світової війни) проводила стратегічні інформаційно-психологічні та дезінформаційні операції з метою послаблення і деморалізації політичного і військового керівництва всіх держав-супротивників. Використовувалися такі методи, як компрометація найбільш активних військових і політичних діячів, дезінформація населення та здійснення на нього психологічного тиску, пропагандистське "виправдання" перед громадськістю початку німецької агресії тощо.

На початку Першої світової війни найбільш успішною була пропагандистська робота країн Троїстого союзу, яка пізніше, в силу використання великої кількості явно неправдивих відомостей, вона втратила свою ефективність. Засновані в столицях нейтральних держав, що постійно постачались з Берліна і Відня свіжі дані телеграфом, інформагентства "Вольф", "Кореспонденція-Бюро", "Оттоманської бюро" та інші, розгорнули широку діяльність з формування громадської думки в країнах, що поки що не вступили у війну. При цьому вони користувалися всебічною підтримкою посольств Німеччини та Австро-Угорщини. Зазначені інформаційні бюро не тільки співпрацювали з місцевими органами друку, але і розсилали свої бюлетені провідним політикам країни перебування, видатним державним і громадським діячам, великим промисловцям, фінансистам. Особливу активність німецькі та австро-угорські бюро розгорнули в Туреччині, Болгарії, Румунії, Греції, США, Норвегії та Швейцарії. Вони мали гарну технічну оснащеність, численний і

висококваліфікований персонал, постійно залучали до роботи відомих місцевих журналістів.

Поряд із засобами масової інформації та міністерствами закордонних справ, активну участь в пропагандистській діяльності брали генеральні штаби і спецслужби. Ряд країн, що воювали, створили спеціальні органи для ведення пропаганди на війська і населення противника і здійснення впливу на громадську думку в нейтральних країнах.

Велика Британія виявилася найбільш підготовленою до інформаційної війни, яка відбулась в ході Першої світової війни. Своїми перемогами на інформаційному полі вона зобов'язана, перш за все, такій особі, як лорд Нортклiфф, газетному магнату, який очолював під час війни англійську пропаганду проти ворожих країн. Найважливішими принципами здійснення пропаганди лорда Нортклiффа були: забезпечення правдоподібності, а не достовірності змісту пропагандистських матеріалів за рахунок вмілого поєднання брехливих і справжніх повідомлень; масований характер пропаганди; випередження пропагандою політичних дій свого уряду; пропагандистська підтримка опозиції урядів ворожих країн; ведення пропаганди від імені патріотичних сил противника. Найважливішим завданням пропаганди лорд Нортклiфф вважав розкладання армії і населення ворожих держав. Крім пропаганди, англійська сторона силами своїх спецслужб активно використовувала ЗМІ для здійснення дезінформації противника.

Ще однією потужною структурою для здійснення інформаційного впливу став створений більшовиками ще 1920 р. Агітаційно-пропагандистський відділ ЦК РКП(б) - "агітпроп", який надалі функціонував під різними назвами. Однак цей орган згодом втратив свій революційний запал, упав у догматизм і неабияк деградував, тому програв Холодну війну й безславно скінчив свої дні з розпадом СРСР. Відзначимо також інформаційну структуру Третього рейха на чолі з рейхсміністром "народної освіти й пропаганди" Йозефом Геббельсом. Слід визнати, що міністерству вдалося в початковий період мобілізувати населення Німеччини навколо ідей націонал-соціалізму.

Під час Другої світової війни всі країни-учасниці вже мали спеціалізовані

підрозділи та міністерства, на які були покладені аналогічні завдання та функції. Зокрема, варто відзначити високу ефективність пропагандистської діяльності у воєнний період фахівців з Великобританії і США. З початком Другої світової війни британський уряд за допомогою створеного при міністерстві закордонних справ відділу "політичної війни" розгорнув широку радіопропаганду проти Німеччини і здійснював закидання на її територію пропагандистської літератури. У США в червні 1942-го був створений спеціальний орган для ведення внутрішньої і зовнішньої пропаганди - Управління військової інформації. Проведенням фронтової пропаганди у взаємодії з бойовими діями військ, а також операцій "чорної пропаганди" займалося Управління стратегічних служб (УСС). При американському розвідувальному управлінні була створена "Група спеціальної служби", перейменована потім в відділення психологічної війни. Під час війни англійці та американці неодноразово створювали об'єднані пропагандистські служби, які координували свої дії з військовими операціями.

Одним з нових прийомів інформаційного впливу на цільову аудиторію, що з'явилися в арсеналі британських і американських пропагандистських органів в період Другої світової війни, стало завоювання її довіри. Іншим найважливішим прийомом здійснення інформаційного впливу британською стороною було використання неточностей офіційних повідомлень противника. Глава УСС США в період Другої світової війни Донован так охарактеризував роль пропаганди в військових діях: "Пропаганда на закордон повинна використовуватися як інструмент війни - майстерна суміш чуток і обману, правда - лише приманка, аби підірвати єдність і сіяти сум'яття ... По суті, пропаганда - вістря початкового проникнення, підготовка населення території, обраної для вторгнення. Це перший крок, потім вступає в дію п'ята колона, за ними диверсійно-десантні частини, або "командос", і, нарешті, виступають дивізії вторгнення" [159].

Згодом, під впливом Холодної війни відповідні підрозділи еволюціонували до різних агентств, які здійснювали управління радіо- та телекомпаніями, які здійснювали мовлення на територію супротивника. Також

у цьому процесі активно брали участь спеціальні служби, як країн Варшавського договору, так і країн НАТО а на час локальних бойових дій залучались спеціальні підрозділи збройних сил.

Наприкінці XX століття набуло поширення стільникового зв’язку та мережі Інтернет. Значно посилилися наочність і образність засобів інформаційного впливу, збільшилися можливості накопичення і тривалого зберігання інформації в будь-якому обсязі. Стало можливим надання як оперативного, так і довгострокового, як вибіркового, так і масового інформаційного впливу на свідомість, волю і почуття населення.

За допомогою використання нових комунікаційних технологій масове індустріальне суспільство стало набувати риси інформаційного (або ж – постіндустріального) суспільства. Із цього часу в словниковий обіг людства міцно входять вислів "інформаційна ера", "століття інформаційних технологій", "інформаційне століття" тощо і подальший розвиток суспільства починають пов'язувати винятково з інформатизацією як науково-технічним і соціально-економічним процесом створення оптимальних умов для задоволення інформаційних потреб. Інформаційне століття принесло новий спосіб ведення війн, що характеризується використанням сучасних інформаційних технологій і мінімальним числом людських (у фізичному сенсі) жертв. Сьогодні одним з найважливіших державних ресурсів є інформація, що циркулює в телекомунікаційних і комп'ютерних системах. Воєнні операції нового типу ведуться найбільш розвиненими в технічному плані державами й вимагають наявності потужних інтелектуальних ресурсів [107].

Порівняно з іншими засобами здійснення інформаційного впливу комп'ютерні й телекомунікаційні системи з'явилися відносно нещодавно. В 1969 р. Міністерство оборони США зв'язало свої комп'ютери, розташовані далеко одне від одного, у єдину мережу в дослідницьких цілях. Комп'ютерна військова мережа стала називатися APRANET (скорочення від англ. "Advanced Project Research Agency Network", що в перекладі означає "Мережа керування перспективних досліджень і розробок"). Саме ця система і започаткувала розвиток мережі Інтернет, що увійшла у повсякденність двадцятьма роками

пізніше, і у якій уперше почав використовувався протокол TCP/IP. Лише в 90- х роках XX століття глобальна комп'ютерна мережа стала "просочуватися" до користувачів персональних комп'ютерів. Фактично відбулася інформаційна революція, якої вдалося охопити більшу частину населення планети й втягнути до складу глобального інформаційного суспільства. Сьогодення кардинально змінило навколишній простір. Інформаційна революція сприяла також появі нових форм і способів ведення інформаційного протиборства у світовому інформаційному просторі [243].

Прикладом сучасної інформаційної війни можуть вважатися інформаційні операції, які проводило Міністерство оборони США, приміром, в Іраку. "Міноборони США заплатить приватним підрядникам в Іраку до 300 млн. доларів за виробництво політичних матеріалів, новин, розважальних програм і соціальної реклами для іракських ЗМІ, щоб залучити місцеве населення до підтримки США", - пише 3 жовтня 2008 р. газета "The Washington Post" [192]. Яскравим прикладом інформаційно-психологічної війни є конфлікт Ізраїлю й Палестини, який є глобальним, оскільки зачіпає інтереси болем десятка країн. Протиборчі сторони використовують у своїх інтересах різноманітні інформаційні ресурси: друковану пресу, телебачення, радіо, Інтернет" [248].

Сучасний інформаційний вплив пропонують розглядати в рамках теорії й практики ведення війн четвертого покоління (4th generation warfare), або «стратегії 4GW» - самостійного виду впливу, ефективної зброї, спрямованої на позбавлення супротивника волі до опору, щоб відмовитися від військової сили. Метою стратегії 4GW є злам так званого культурного коду і підкорення своїй волі морального духу супротивника. Теорія й практика ведення війн четвертого покоління, або стратегії 4 GW, була реалізована, зокрема, в операціях збройних сил США в Іраку, Афганістані, Лівії тощо [222], а також реалізується Російською Федерацією у гібридній війні проти України (Додаток Б).

У міру накопичення досвіду практичного здійснення інформаційного впливу на супротивника та цільову аудиторію у більш широкому розумінні у військових конфліктах, економічних суперечках, політичній боротьбі тощо виникла потреба в його теоретичному осмисленні.

Слід зауважити, що мистецтво стратагем була розвинене як у Греції, так і в Римській імперії (відома праця Секста Юлія Фронтина "Стратагеми"). На Сході особлива увага цій сфері приділили китайці, і найбільш систематизовані канони непрямих дій були викладені в праці китайського стратега й філософа Сунь Цзи (VI століття до н.е.) «Мистецтво війни».

У зазначеній праці докладно розглядаються інструкції з організації та підтримання морально-вольових якостей власної армії та держави, а також інструменти та прийоми зі соціально-політичної дестабілізації й «морального розкладання» армії та суспільства супротивника. Автор, окрім суто тактичних порад стосовно розміщення військ, військових маневрів та інших аспектів ведення бою, пропонував організовувати та розвивати інтриги у стані ворога, підривати авторитет командування та приковувати увагу суспільства до ганебних вчинків чи ситуацій, знецінювати традиції та ставити під сумнів вірування, засилати жінок «легкої поведінки» для «морального розкладання» війська, активно проводити шпигунську і диверсійну роботу та підтримувати зрадників. У трактаті висвітлені також основні прийоми маніпуляції противником шляхом психологічного впливу і дезінформації, в певному поєднанні складових механізму примусу обраного об'єкта до потрібних дій. Значну увагу, на думку Сунь-Цзи, необхідно приділяти отриманню знань про особистісні характеристики командуючи військами супротивника. Оскільки на той час всі аспекти військових дій повністю керувались людьми а люди наділені певними якостями, відповідно вони і визначають її хід. Звідси – введення противника в оману може принести перемогу. Але щоб обдурити ворога, його треба глибоко знати і перш за все знати його якості. Так Сунь-Цзи першим зазначив необхідність визначення характеристики цільової аудиторії інформаційного впливу [230].

Якщо спробувати узагальнити концепцію Сунь Цзи, то пріоритетними в боротьбі з ворогом є непрямі, найчастіше суто інформаційні дії, за допомогою яких потрібно добитися "руйнування всього гарного, що є у ворога, втягти його видатних представників у злочинні дійства, зробити їх посміховиськом перед суспільством, використовувати для співробітництва найбільш огидних

особистостей". Примітно, що одне з основних положень концепції Сунь Цзи - "створи в супротивника безладдя й хаос, і ти переможеш його" – було покладене в основу розробленої для Пентагона американською корпорацією RAND концепції інформаційних війн другого покоління.

Основні ідеї Сунь-Цзи активно розвивалися іншими китайськими мислителями. До їх числа належить військовий теоретик Чжуге Лян (III ст. до н.е.) [159]. Спадщина Чжуге Ляна в області інформаційно-психологічного протистояння з військом супротивника була ретельно вивчена і успішно використана партизанами В'єтконгу у Південному В'єтнамі у війні проти США. Чжуге Лян "ніколи не розмахував мечем, бо суть великої китайської військової традиції завжди зводилася до того, що мозок обдурить силу м'язів". Він, як і Сунь-Цзи, вважав, що "у військових діях атака на розуми – головне завдання, атака на зміцнення – другорядне завдання війни. Це головне, бій – це другорядна справа" [69]. У II столітті нашої ери в Китаї вперше застосували прийом пропагандистського впливу - проголошення справедливого характеру війни; обґрунтовуючи необхідність військових дій.

Варто зазначити, що праця Сунь-Цзи є єдиною працею з військового мистецтва, яка дійшла до наших часів. Іншою давньою пам’яткою, у якій містяться настанови з інформаційно-психологічного впливу на супротивника, є давньоіндійські закони Ману, у яких, серед різних інструкцій нормативно-правового характеру та відповідних норм поведінки містяться поради правителю стосовно впливу на армію ворога. Так, наприклад, у IV главі (п.п. 197-198) мова йдк про необхідність сіяння розбрату між союзниками, вивчення можливих заколотників та їх провокацію [108].

Необхідно зауважити, що стародавні мислителі не виокремлювали інформаційний вплив на супротивника як окремий, незалежний інструмент ведення бойових дій, вони лише формулювали такі інструкції як складову частину війни. Не випадково вже пізніше німецький військовий історик, один з творців теорії війни, Клаузевіц безпосередньо пов'язав війну та інформаційно-психологічний вплив на супротивника: "Війна - це акт насильства, який має на меті змусити противника виконати нашу волю" [120].

Значну увагу питанню виховання власних військ з метою забезпечення психологічної стійкості воїнів в бою, питань дезінформації та психологічного впливу на чужі армії приділяли європейські воєначальники і вчені минулого: давньогрецький письменник і історик Ксенофонт (IV ст. до н.е.), римський полководець Ю. Цезар (I ст. До н.е.) та ін. Відомий державний діяч і вчений Н. Маккіавелі (XV-XVI ст.) аналізуючи особливості інформаційно-психологічного впливу під час бою, особливу увагу у своїх працях приділяв питанням дезінформування противника.

В Європі Перша світова війна стала поворотним пунктом у розвитку теорії інформаційного впливу, на дослідженнях досвіду якого в цілому завершилося формування теоретичних засад ведення пропаганди в воєнний період. У 1920 р. в Лондоні вийшла книга К. Стюарта "Таємниці будинку Крю", в якій узагальнювався досвід англійської пропаганди з розкладання військ противника. У 1922 р. в Німеччині вийшли книги Штерн-Руберто "Пропаганда як зброя політики" та І.Пленге "Німецька пропаганда". У 1924 р. вийшла книга Ф.Шенемана "Мистецтво впливу на маси в Сполучених Штатах Америки".

Дещо раніше, у Німеччині в 1893 р. вийшли в світ книги «До питань психології великої війни» фон Біндер-Крігельштейна і «Психологічні елементи у наступі та обороні» Фрейхера фон Ліхтенштейна, а в 1904 р. в Бухаресті була видана книга доктора М. Кампанео «Досвід військової психології», присвячені питанням інформаційного впливу.

У 1927 р. в Лондоні побачила світ книга англійця Г.Ласвеля "Техніка пропаганди у світовій війні". У ній вперше була виділена інформаційно-психологічна сфера війни, а пропаганда - розглянута як особливий вид зброї, яка впливає на моральний (психічний) стан ворога, покликаний або порушити його стан або відвести ненависть ворожої сторони від воюючою з ним країни. В якості основних стратегічних цілей пропаганди в книзі були названі: створення у власному населенні, а також в населенні країн-союзників і нейтральних країн ненависті до ворога; підтримання дружніх відносин з союзниками; збереження добрих відносин з нейтральними країнами і утримання їх підтримки; деморалізація противника. Найважливішими факторами успіху пропаганди

визнані майстерність застосовуваних засобів і вірний облік умов ведення пропаганди [21].

На початку XX століття активного поштовху теорія інформаційного впливу зазнала і у США, причому розробляли питання інформаційно-психологічного впливу та інформаційних війн у США, в першу чергу, через призму реклами й піару. Ринкова економіка, всеохоплююче виборче право та міжпартійна боротьба сприяла розвитку науково-теоретичній думці у сфері маніпуляції масовою свідомістю. Найбільш відомими постатями у цій сфері стали Е.Бернейс (фахівець, який впровадив жіноче паління як символ емансипації на замовлення просунути на ринку торгову марку «Lucky Strike» тютюнової корпорації American Tobacco Company, а також впровадив у щоденний сніданок американців смажений бекон як обов'язковий), який першим почав використовувати психологічний вплив на цільову аудиторію, та А.Лі (амерканський журналіст, що організував та керував інформаційною компанією зі створення позитивного образу Дж.Рокфеллера після «бійні у Людлоу» 1914 р. та автор «декларації принципів», основоположних ідей PR) [41, 57].

Надалі, напередодні Другої світової війни та під час неї у Німеччині вийшли такі книги як «Ведення війни духу» майора А. Блау (Потсдам, 1937), «Готовність до ведення війни духу» К.-Х. Рюдигера (Берлін, 1944) і «Військовий обов'язок духу» В. Блея (Мюнхен, 1935).

В подальшому, після закінчення Другої світової війни відбувається розвиток маркетингу, виборчих технологій, рекламний інструментів та інших галузей суспільних наук, які мають на меті вплив на суспільство з метою отримання того чи іншого результату для ініціаторів чи замовників інформаційно-психологічного впливу поза межами бойових дій.

Зауважимо, що тривалий час не було офіційно прийнято жодних нормативних актів, які б регламентували порядок здійснення інформаційного впливу і тільки після Другої світової війни, у 1949 році Міністерство оборони США розробило так звану «Настанову FM-33-5», які регламентували ведення інформаційних війн, спеціальних інформаційних операцій. Ця настанова, яка

отримала назву «Психологічна війна в бойових операціях», стала першою кодифікованою та змістовною інструкцією з інформаційно-психологічного впливу для Збройних сил. Надалі Міністерство оборони США випустить ще декілька таких документів, такі як FM-33-5 («Операції з психологічної війни») 1955 р., FM-33-5 («Психологічні операції») 1962 р., FM-33-1 («Психологічні операції») 1979 р. Остання розсекречена настанова відома як FM 33-1-1 («Техніка і процедури психологічних операцій»).

У книзі відомих дослідників Элвина й Хейди Тоффлер "Війна й антивійна" виділяються три типи суспільств, які еволюційно змінюють одне одного в розвитку цивілізації - аграрне, промислове й інформаційне суспільства. Кожному з них відповідає свій тип виробництва й, відповідно, свої способи ведення війни [38]. Така класифікація впритул підштовхнула науковий світ до відокремлення проблематики інформаційної війни.

На сьогоднішній момент більшість дослідників погоджується з думкою, що інформаційні війни можуть активно проводитися тільки в умовах сформованого інформаційного суспільства. Разом з тим, відзначимо, що до самого поняття "інформаційне суспільство" науковці і практики ставляться по-різному й розуміють під ним різні явища. Показовим у даному контексті є дослідження Ф.Уебстера, присвячене аналізу більш-менш відомих теорій другої половини XX століття [237].

Вагомий внесок у розвиток до теорії інформаційного права в аспекті наукової думки про інформаційні війни свого часу був внесений С.Расторгуєвим [212-216], який широко й багатогранно підходить до дослідження цієї проблеми. Зокрема, С.Расторгуев висунув теорію інформаційної війни, під якою розуміється наука про закони зародження, зміни й загибелі інформаційних процесів, властивих інформаційним системам, і, звичайно, про "життя" інформаційних моделей, суб'єктів інформаційного простору. У рамках цієї теорії під інформаційною війною розуміється цілеспрямоване широкомасштабне оперування суб'єктів «змістами»: створення, знищення, модифікація, нав'язування й блокування носіїв змістів інформаційними методами для досягнення поставлених цілей.

Концепція інформаційної війни передбачає проведення інформаційних операцій - комплексу взаємозалежних за метою, місцем і часом заходів і акцій, спрямованих на ініціалізацію й управління процесами маніпулювання інформацією, з метою досягнення й утримання інформаційної переваги шляхом впливу на інформаційні процеси в інформаційних системах супротивника [249, с.191-193].

Сучасний зміст і термінологія інформаційних операцій почали формуватися в ще 1991 р. У 1998р. уже була розроблена "Об'єднана доктрина інформаційних операцій" Міністерства оборони США. У цьому документі, в основу якого були покладені розробки вже відомої нам корпорації RAND, представлені, зокрема визначення понять "інформаційна операція" і "інформаційна війна":

- інформаційна операція – дії з метою ускладнити збір, обробку, передачу й зберігання інформації інформаційними системами супротивника при захисті власної інформації й інформаційних систем;

- інформаційна війна - комплексний вплив на систему державного управління конфронтуючої сторони і її військово-політичне управління, яке вже в мирний час може привести до прийняття рішень, сприятливих для країни, що веде інформаційну війну, а в ході збройного конфлікту здатний повністю паралізувати функціонування управлінської інфраструктури супротивника.

З наведеного формулювання випливає, що інформаційна війна - це реалізація інформаційних загроз технічного й духовно-психологічного типу. Інформаційними операціями, фактично, є акції з реалізації зазначених загроз або відвернення чи нейтралізації таких загроз з боку супротивника.

Розробки в банному наразі напрямку тривають, і в цей час у практичну площину перемістилася концепція інформаційних війн наступних поколінь. І якщо війна першого покоління розглядається як певний важливий компонент поряд із традиційними засобами, то вже в другому поколінні вона здобуває повністю самостійне значення, яке кристалізується у наступних поколіннях (третьому й четвертому).

Серед завдань, які вирішуються в ході сучасної інформаційної війни,

Г.Арутюнян пропонує вирізняти наступні:

- формування атмосфери бездуховності й аморальності, негативного відношення до культурної спадщини супротивника;

- маніпулювання суспільною свідомістю й політичною орієнтацією соціальних груп населення країни з метою створення політичної напруженості й хаосу;

- поширення недовіри й підозрілості, загострення політичної боротьби між партіями, провокація взаємознищення;

- завдання збитків життєво важливим інтересам нації й держави в політичній, економічній, оборонної й інших сферах[51].

Неважко помітити, що деякі положення інформаційних війн цього покоління нагадують "Стратагеми" Сунь Цзи. Відомо також, що методологія інформаційних широко застосовується в "кольорових" революція, коли, не вдаючись до бойових дій сторона, що здійснює вплив, вирішує політичні або ідеологічні завдання, що стоять перед нею. Слід підкреслити, що за наявності потужних і неконтрольованих інформаційних потоків (які також створюють віртуальний "хаос" у свідомості суспільства [64]), практично неможливо заборонними (або тільки заборонними) методами протистояти загрозам інформаційного характеру. Ефективна протидія можлива винятково за наявності критичної маси інтелектуально-духовних ресурсів у даного суспільства й уміння оптимально використовувати ці ресурси також у контексті інформаційної безпеки.

Водночас, у XXI столітті теорія й практика стратегам розбудовуються доволі стрімко й сьогодні, як вже зазначалося, мова йде вже про інформаційні операції, проведені в рамках інформаційних війн третього й четвертого покоління [51]. Інформаційними операціями в найбільш загальному виді прийнято вважати використання й управління інформаційними й комунікаційними технологіями для досягнення переваги над супротивником. Зокрема, американські військові включають до структури інформаційних операцій п'ять компонентів:

- радіоелектронну боротьбу;

- дезінформацію супротивника різними методами;

- ведення "психологічної війни": пропаганду й контрпропаганду в інформаційному просторі (у тому числі в Інтернеті, зокрема, у соціальних мережах);

- забезпечення комп'ютерної безпеки, захист інфраструктури й режиму таємності;

- проведення кібернетичних атак, збір і обробку військових тактичних даних тощо.

У військовій науці формування концепцій інформаційних операцій почалося в 1970-х років, уперше цей термін було вжито у звіті Томаса Рона "Системи зброї й інформаційна війна" («Weapon systems and information war»), підготовленому в 1976 р. для компанії Boeing.

Розуміння шкідливості й руйнівної сили інформаційної війни вимагає більш глибокого дослідження цього феномена із правової точки зору, оскільки це явище перешкоджає не тільки розвитку інформаційного суспільства, але й торкається буквально всіх сторін соціального життя в масштабі планети. Особливої уваги в цьому контексті заслуговують так звані спеціальні інформаційні операції (далі – СІО), які складають змістовне наповнення інформаційної війни.

Серед науковців, що займалися дослідженням зазначеної проблематики з різних точок зору, можуть бути названі О.Баранов, І. Бачило, К.Бєляков, Н.Брусніцин, О.Довгань, І.Доронін, В.Голубко, Г.Грачов, М.Ємельянов, Є.Єрофєєв, О.Заруба, В.Копилов, Г.Красноступ, В.Крисько, Д.Ланде, О.Литвиненко, В.Лопатін, А.Манойло, І.Мірошник, В.Наумов, І.Панарин, В.Петрик, В.Пилипчук, Г.Почепцов, Ю.Просвирнин, М.Рассолов, І.Рассолов, Н.Савінова, О.Стрельцов, Н.Ткачук, Т.Ткачук, Ю.Уфімцев, А.Фатьянов, М.Федотов, Д.Фролов, В.Ченцов,А.Явтушенко, М.Якушев та інші.

Зокрема, предметно питанням СІО присвячене дослідження О.Литвиненка [148]. Автор вважає, що основою сучасних СІО є синергетичні принципи. Синергетичними підходами можна скористатися, розглядаючи суспільство як надзвичайно складну систему, кожний з елементів якої має дуже багато

ступенів свободи. При цьому СІО О.Литвиненко розглядає в контексті пропагандистських технологій і пропонує загальний алгоритм їх проведення.

Заслуговує на увагу й монографія С.Расторгуєва й М.Литвиненка "Інформаційні операції в мережі Інтернет" [215], у якій запропонований і обґрунтований підхід до побудови систем виявлення інформаційних загроз, надані базові визначення й проведене дослідження спеціальних дій, що притаманні інформаційним операціям у мережі Інтернет. У цьому дослідженні увагою науковців охоплені не лише інформаційно-психологічні операції, але й СІО технічного характеру. Зокрема, авторами продемонстроване, що виробництво практично всіх компонентів інформаційної операції вже поставлене на промислову основу: від вірусів, націлених на автоматизовані об'єкти військового й промислового призначення, до генераторів повідомлень у вигляді текстів, голосових повідомлень по заданій голосовій характеристиці або відеосюжетів по заданій вихідній "картинці". У книзі описаний механізм, що дозволяє частково автоматизувати планування СІО за рахунок використання типових схем їх проведення, й визначено, яким чином можлива організація ігрового тренінгу з моделювання проведення СІО.

Не менш цікава колективна наукова праця "Розпізнавання інформаційних операцій" [99], присвячена розгляду питань розпізнавання СІО на основі аналізу інформаційного простору, насамперед вебресурсів мережі Інтернет, соціальних мереж, блогів тощо.

Проблематиці інформаційних війн, інформаційних операцій, інформаційних впливів тощо буди присвячені й дисертаційні дослідження К.Будиліна [61], В.Гарєва [74], О.Губарєва [87], О.Горбєнка [77], О.Денщикова [94], Г.Крилова [140], О.Потьомкіна [189], Є.Соловйової [225], Д.Фролова [242], Л.Шишкіної [254], Д.Щербини [257] тощо. Втім зазначені дослідження стосуються радше філософських, технічних, військових, політологічних, соціологічних тощо, аніж правових аспектів забезпечення інформаційної безпеки. Натомість актуальні підходи до визначення сутності і особливостей проведення СІО під кутом права висловлені у наукових працях В.Ліпкана [152, 155], В.Петрика [179], О.Заруби [109], О.Кушнір [145] тощо. Слід згадати також

дисертаційні дослідження В.Разуваєва [211], О.Тамодліна [233], О.Кубишкіна [142] тощо.

Методологічну основу сучасного розуміння суті інформаційного протиборства заклали публікації М.Попова, А.Лук'янця, В.Фоміна, А.Рося, К.Данилішина, С.Сосніна, В.Толубко, В.Гурковського тощо.

Історичні аспекти інформаційного протиборства та використання інформаційної зброї системно проаналізовані в дисертаційному дослідженні українського вченого Я.Жаркова «Інформаційно-психологічний вплив на війська та населення противника (1939 – 2000 рр.)», в якому досліджені особливості інформаційно-психологічного впливу провідних країн світу на війська та населення противника за тривалий період [104].

6 червня 2014 року Науково-дослідним інститутом інформатики і права та Науково-дослідним інститутом правового забезпечення інноваційного розвитку Національної академії правових наук України спільно з Навчально-науковим центром інформаційного права та правових питань інформаційних технологій ФСП Національного технічного університету України "Київський політехнічний інститут" було проведено науково-практичну конференцію на тему: "Проблеми протидії правопорушенням в інформаційній сфері: інформаційні війни ". У ході конференції було розглянуто низку актуальних проблем забезпечення інформаційної безпеки та протидії правопорушенням в інформаційній сфері в умовах інформаційної війни. Учасники конференції охопили широке коло питань щодо вказаної проблематики, починаючи від дефініцій термінології, теоретико-правового аналізу, визначення форм та методів проведення інформаційного протиборства до аналізу інформаційної війни як фактора сучасної глобальної політики, а також концептуальні підходи протидії правопорушенням у національному та міжнародному праві. Особливе місце в ході обговорення було відведено соціологічним аспектам дослідження феномену інформаційної війни та правовим гарантіям захищеності людини в процесі інформаційного протиборства. Були запропоновані методики виявлення та аналізу СІО і правового моделювання як універсальних засобів попередження та протидії інформаційним війнам. У конференції взяли участь

фахівці з інформаційної безпеки центральних органів виконавчої, правоохоронних органів і військових формувань України, вчені Національної академії наук України і Національної академії правових наук України, представники Національного технічного університету України “Київський політехнічний інститут” та інших вищих навчальних закладів, зокрема, Д.Ланде, О.Баранов, Г.Красноступ, К.Бєляков, Н.Савінова тощо. Протягом останніх років, зважаючи на втягнення України у гібридну війну, проблеми забезпечення інформаційної безпеки, протидії інформаційній війні та проведення СІО набувають все більшої актуальності, тож відповідні наукові заходи з цієї проблематики саме правового спрямування проводяться все частіше, зокрема, наприкінці листопада 2018 року відбувся круглий стіл на тему «Забезпечення Службою безпеки України інформаційної та кібернетичної безпеки в контексті імплементації Закону України «Про національну безпеку України», організований Службою безпеки України, Науково-дослідним інститутом інформатики і права Національної академії правових наук та Національною бібліотекою України імені В.І.Вернадського [171].

Втім слід констатувати, що питання інформаційно-правових засад СІО у наукових працях розкрито ще не повною мірою. Розпочати розгляд цього питання видається за доцільне з уточнення понятійно-категорійного апарату дослідження з точки зору інформаційного права, у площині якого це дослідження проводиться.

1.2. Понятійно-категоріальний апарат дослідження проблематики правового забезпечення спеціальних інформаційних операцій

Уточнення понятійно-категоріального апарату є принципово важливим етапом дослідження будь-якої наукової проблеми. Для дослідження проблематики інформаційно-правових засад СІО цей етап має особливе значення, адже понятійно-категоріальний апарат відповідної проблеми досі остаточно не розроблений.

Поняття та категорії, що використовуються у дослідження питань

інформаційно-правових засад СІО є доволі різноманітними, однак ключовими поняттями в даному випадку слід визнати наступні: національна безпека, інформаційна безпека, інформаційна загроза, інформація, інформаційна війна, інформаційна зброя, інформаційні операції тощо, більшість яких належать до базових категорій інформаційного права. Інші поняття й категорії, що мають відношення до предмету дослідження, тією чи іншою мірою пов'язані з наведеними та визначаються ними відповідно до мети та завдань дослідження.

Почнемо окреслення понятгєво-категоріального апарату дослідження проблематики інформаційно-правових засад СІО з уточнення сутності та змісту поняття «національна безпека» як основоположного.

На думку О.Фоміна, поняття «національна безпека» є базовим поняттям у системі соціальної безпеки і означає стан країни, за якого забезпечується життєздатність держави, цільовий розвиток і збереження її фундаментальних цінностей і традицій, неконфліктні відносини особистості й держави, захист національних інтересів і досягнення національних цілей, здатність ефективно долати будь-які внутрішні й зовнішні загрози [240].

Вперше термін "національна безпека" був використаний президентом США Т.Рузвельтом в 1904 р. як синонім поняття «оборона». Втім системне використання відповідного поняття розпочалося в США відразу після Другої світової війни при розробці концепції національної безпеки та доктрини державної безпеки країни. Дещо пізніше був прийнятий закон про національну безпеку, а також була запроваджена нова державна посада - спеціальний помічник Президента США з питань національної безпеки [221]. Якщо спочатку поняття "національна безпека" застосовувалося до питань забезпечення військової безпеки, то згодом його почали розуміти як здатність держави забезпечити національні інтереси у зовнішніх та внутрішніх умовах, а також збереження основних ідеалів людського суспільства, недоторканості, свободи та своєрідності.

Як зазначає Г. Новицький, в СРСР термін «національна безпека» не набув поширення насамперед через розуміння терміна «національна» як такого, що пов'язаний з певним етносом. Тому введення в політичний та науковий обіг в

Україні запозиченого з західної політології поняття «національна безпека» спиралося на американську і французьку політологічні школи, які розглядають націю як співгромадянство, тобто, «політичну націю» [173]. У такому розумінні безпека будь-якого соціального суб'єкта входить до національної безпеки.

Перший офіційний підхід до проблем національної безпеки в Україні був представлений у Концепції (основах державної політики) національної безпеки України у 1997 році [134]. Наступним важливим кроком в цьому напрямку було прийняття у 2003 році Закону України "Про основи національної безпеки України", який містив визначення національної безпеки, започаткувало становлення в Україні загальної теорії безпеки. Відповідно до цього Закону України, національна безпека визначалася як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у різних сферах державного управління (у статті наведено невичерпний перелік) при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам [200].

Відповідно до Закону України «Про національну безпеку України», прийнятому 21.06.2018 р. [198], національна безпека України - це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. При цьому національні інтереси України визначені як життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян. Водночас, зміст національної безпеки охоплює не лише національні інтереси , але й національні цінності і національні цілі [210] – зазначені елементи визначають зміст, характер, конфігурацію та спрямованість системи. Найбільш статичним елементом у цій тріаді є національні цінності, під якими в загальному вигляді розуміють ідеальні, матеріальні, соціальні й духовні блага, що задовольняють потреби й інтереси людей і сприяють прогресивному

розвитку особи й соціальних утворень [79-81, 208]. Інтереси зазвичай визначаються як усвідомлені потреби, відтак під національними інтересами традиційно розумілася сукупність життєво важливих інтересів особи, суспільства та держави, що виражаються у спрямуванні нації на збереження та сталий розвиток, а також становлять першопричину політичних дій та звершень, переломлюючись у вигляді економічних, політичних та інших доктрин, концепцій та програм [63]. У свою чергу, під національними цілями слід розуміти не стільки «конкретні цілі, які держава ставить перед собою заради захисту національних інтересів», скільки пріоритети суб'єктивної діяльності, спрямованої на реалізацію національних інтересів за допомогою інструментальних державних механізмів [81, с.123-127]. Так само, як і інтереси, цілі можуть бути орієнтовані на стабільність або зростання.

У контексті національної безпеки як поняття більш загального рівня традиційно досліджується зміст поняття «інформаційна безпека». Зокрема, як зазначає В.Ліпкан, «національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу» [153], тож конструктивним шляхом визначення поняття «інформаційна безпека» науковець вважає виокремлення його сутнісних ознак, які є похідними від поняття «національна безпека» [155].

Так, відповідно до ст. 17 Конституції України, «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [133]. Законодавче визначення інформаційної безпеки наведене у Законі України «Про основні засади розвитку інформаційного суспільства на 2007-2015 роки» [201] (інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та

доступності інформації), і в цілому відповідає доктринальним підходам до розуміння її сутності. Погляди багатьох дослідників – А.Марущака [164], Г.Почепцова [190-193], С.Расторгуєва [214], Р. Хаби [244], Р.Калюжного [117], В.Шульги [255], І.Бондар [59] та інших фахівців у сфері інформаційного права, - збігаються в тому, що вони розглядають інформаційну безпеку як стан, що характеризується відсутністю небезпеки, тобто чинників та умов, які загрожують безпосередньо індивіду, державі, спільноті з боку інформаційно-комунікаційного середовища. Т.Ткачук розширює відповідне поняття, трактуючи інформаційну безпеку не лише як стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема, захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їхніх суб'єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері, але й як постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час [234].

У будь-якому випадку слід враховувати, що інформаційний чинник може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації. Враховуючи той факт, що під дією інформаційних впливів може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав'язуватися чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки,

вироблення механізмів протидії їм у всіх напрямах. Таким чином, інформацію сьогодні слід розглядати як найважливіший елемент системи виживання, а відповідно – національної безпеки країни в цілому. Основа функціонування управлінського механізму забезпечення національної безпеки та його ефективність передусім залежить від ефективності функціонування підсистеми інформаційного забезпечення. Отже, інформаційна складова національної безпеки включає, зокрема: вжиття комплексних заходів щодо захисту свого інформаційного простору та входження України в світовий інформаційний простір; виявлення та усунення причин інформаційної дискримінації України; усунення негативних чинників порушення інформаційного простору, інформаційної експансії з боку інших держав; розробку і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно-значущої інформації, створення розвиненої інфраструктури в інформаційній сфері. Важливо усвідомлювати, що активніше розвивається інформаційна сфера, яка стала системоутворюючим фактором життєдіяльності суспільства, тим більше політична, економічна, оборонна та інші складові національної безпеки будь-якої держави залежатимуть від інформаційної безпеки, причому в ході розвитку технічного прогресу ця залежність все більше зростатиме. Тож інформаційна безпека є не лише самостійною складовою національної безпеки, але й невід‘ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Майже всі взаємовідносини між суб‘єктами інформаційного суспільства ґрунтуватимуться на споживанні й обміні інформацією, тому питання інформаційної безпеки є таким, що превалює порівняно з іншими. Тому у соціальних системах залежність має інформаційну природу, яка слугує підставою для визначення завдання моделювання й оцінки стану інформаційної безпеки. Так, можна очікувати одержання об‘єктивних оцінок впливу різних компонентів інформаційної впливової дії на внутрішню структуру інтересів (життєвих цінностей, соціальних пріоритетів, внутрішніх настанов) на соціальні об‘єкти (держава, суспільство, соціальні групи, окрема особистість) і на еволюцію їх зовнішньої соціальної поведінки. По-перше, інформаційні

відносини і процеси пронизують всі інші, які мають місце в суспільстві, тому як елемент інформаційна безпека має входити в усі підсистеми національної безпеки. По-друге, в сучасних умовах, коли різноманітні інформаційні технології та процеси, засоби обчислювальної техніки інтенсивно та в масовому порядку впроваджуються в більшість галузей людської діяльності, питання інформаційної безпеки набуває самостійного суспільного значення. По-третє, система зовнішніх та внутрішніх загроз інформаційній безпеці має комплексний характер. Реалізація загроз інформаційній безпеці може завдати цілком конкретної шкоди як державі, так і окремому індивіду [55]. Таким чином, інформаційна безпека як одна з основних складових національної безпеки реалізується в двох вимірах: суспільному та державному, та поділяється на внутрішню та зовнішню в залежності від джерел загроз, небезпек та ризиків для життєво важливих інтересів.

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

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері Доктрина інформаційної безпеки України [205] визначає:

- здійснення спеціальних інформаційних операцій, 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;

- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;
- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;
- інформаційне домінування держави-агресора на тимчасово окупованих територіях;
- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;
- неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, - недостатній рівень медіа-культури суспільства;
- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

В цілому, зважаючи на те, як Закон України «Про національну безпеку України» [198] визначає загрози національній безпеці України (явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України), під загрозами інформаційній безпеці можемо розуміти явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України, а також досягнення національних цілей України в інформаційній сфері. Таке загальне визначення дозволяє припустити, що загрози інформаційній безпеці можуть мати досить різну

природу, причому не завжди інформаційну. Тож варто виокремити власне інформаційні загрози із загального спектру загроз інформаційній безпеці - під інформаційними загрозами пропонується розуміти інформаційні впливи технічного або психологічного характеру, що унеможливлюють чи ускладнюють або можуть унеможливлювати чи ускладнювати збереження національних цінностей, реалізацію національних інтересів та досягнення національних цілей України. Особливістю інформаційних загроз є те, що впливаючи безпосередньо на інформаційну безпеку, вони можуть нести негативні наслідки для будь-яких складових національної безпеки.

Дослідження сутності інформаційних загроз вимагає передусім розуміння природи феномену інформації. Отже, Закон України «Про інформацію» визначає інформацію як - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [197].

Інформація утворює співвідношення буття до людської істоти. Визначення інформації як всюдисущої субстанції дискретного характеру, що слугує взаємозв‘язком об‘єктивного та суб‘єктивного, корініться ще у філософських поглядах Геракліта, Платона, номіналістів та їх послідовників, знаходить відображення при розгляді філософської категорії “колективного несвідомого” [224, с. 23; 259, с. 141]. Фактично, інформація становить семантичну сутність матерії, здатну діставати прояв в певній матеріально-енергетичній формі, відбиваючись в свідомості людини та об‘єктивуючись шляхом закріплення на матеріальних носіях, становлячи при цьому сукупність відомостей незалежно від форми їх фізичного та логічного представлення, під якими розуміються ідеальні (суб‘єктивні) образи об‘єктів, процесів та явищ навколишнього світу, сформовані в свідомості людини, а також множина ознак, що притаманні матерії та формують ідеальні відображення [123] в процесі взаємодії між двома або більше альтернативними відокремленими або узгодженими між собою елементами. Зауважимо, що, наприклад, Д.Іванов під інформацією розуміє не сукупність відомостей про що-небудь, а комунікацію, операцію трансляції символів, що спонукує до дії. "Якщо ми визначимо інформацію подібним

чином, - пише автор, - стане зрозумілим, чому головним феноменом комп'ютерної революції став Internet, а не гігантські електронні банки даних або штучний інтелект. У глобальній мережі Internet не створюється ніякого знання, але зате багаторазово збільшуються можливості здійснення комунікацій" [111]. Така точка зору, заснована на більш ранніх працях М.Маклюена, Д.Белла, Е.Тоффлера тощо, підводить нас до змісту категорій «інформаційна війна» та «інформаційна зброя».

Термін "інформаційна війна" уперше виявився у фокусі уваги у зв'язку з війною в Перській затоці в 1991 р. Необхідно зауважити, що він дотепер залишається переважно публіцистичним і не одержав широкого наукового визначення, тим більше - правового. Наслідком цього є неминучість виникнення значної кількості визначень цього терміна, що приводять до плутанини. В цілому існуючі визначення інформаційної війни можна розділити на три основні групи.

У визначеннях, які можуть бути віднесені до першої групи, автори зводять поняття інформаційної війни до окремих інформаційних заходів та операцій, інформаційних способів і засобів корпоративної конкуренції або ведення міждержавного протиборства або збройної боротьби [60]. Найбільш відомим фахівцем, що відносить інформаційну війну до інформаційних способів і засобів ведення протиборства, є український вчений Г.Почепцов. Так, він пише: "Інформаційна війна - це комунікативна технологія впливу на масову свідомість з короткочасними і довготривалими цілями" [191, с.10]. При цьому до комунікативних технологій Г.Почепцов відносить пропаганду, рекламу, виборчі технології, PR тощо.

Класичним прикладом визначень другої групи є визначення С.Расторгуєва, котрий визначає зміст інформаційної війни як "відкритих і прихованих цілеспрямованих інформаційних впливів інформаційних систем одне на одного з метою отримання певного виграшу в матеріальній сфері" [213]. При цьому він вважає, що, поки противник усуває отриманий збиток, супротивник має перевагу. На думку С.Расторгуєва, інформаційна війна не відрізняється від війни традиційної в частині ознак ураження. Агресор

домагається перемоги виключно підпорядкувавши собі структури управління противника, які є інформаційною мішенню. Звідси слідують і основні рекомендації щодо напрямків організації захисту: зменшення розміру мішені, захист мішені; регулярне знищення "інформаційного бур'яну", установка власного жорсткого контролю за власною системою управління.

В.Пірумов, визначення якого може репрезентувати третю групу, визначає інформаційну війну як нову форму боротьби двох і більше сторін, яка полягає в цілеспрямованому використанні спеціальних засобів і методів впливу на інформаційні ресурси противника, а також захисту власного інформаційного ресурсу для досягнення призначених цілей. На його думку, в мирний час інформаційна війна носить переважно прихований характер. Її основним змістом є ведення розвідувальних і інформаційно-психологічних дій щодо супротивника, а також здійснення заходів щодо забезпечення власної інформаційної безпеки. У період наявності загрози, як вважає В.Пірумов, з'являються додаткові завдання, які вирішуються в інтересах забезпечення необхідної ефективності запланованих бойових дій [182]. До особливостей ведення інформаційної війни в цей період можна віднести граничну обмеженість у використанні її сил і засобів; дотримання існуючих норм міжнародного права (наприклад, заборона радіоелектронного придушення певних частот і систем, передбачених Статутом Міжнародного союзу електрозв'язку та Регламентом радіозв'язку) тощо. З початком військових дій сили і засоби інформаційної війни вирішують такі завдання, як масований вплив на інформаційний ресурс супротивника і запобігання зниження бойових можливостей власних сил; проведення заходів щодо зниження рівня морально-психологічної стійкості військ супротивника і забезпечення нейтралізації інформації, що впливає на морально-психологічний стан свого особового складу; ведення розвідувальної діяльності та забезпечення конспірації найважливіших заходів власних військ тощо.

С.Комов вважає, що поняття інформаційної війни (у контексті військових конфліктів) характеризується чотирма основними аспектами: визначення заходів для одержання інформації про супротивника й умови бою, а також для

збору інформації про свої війська й війська союзників; визначення заходів щодо блокування процесу збору супротивником інформації про війська, планування заходів щодо дезінформації на всіх етапах бойових дій; здійснення заходів щодо організації взаємодії з іншими військовими контингентами, що беруть участь у конфлікті тощо [125].

В.Маркоменко виділяє наступні прояви інформаційної війни: фізичне придушення елементів інфраструктури державного й військового управління (поразка центрів командування й управління); електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (радіоелектронна боротьба); одержання розвідувальної інформації шляхом перехоплення й аналізу більших обсягів інформації (радіоелектронна розвідка); здійснення несанкціонованого доступу до інформаційних ресурсів шляхом використання програмно-апаратних засобів прориву систем захисту інформаційних і телекомунікаційних систем супротивника з наступним викривленням, знищенням або розкраданням інформації або порушенням нормального функціонування цих систем (кібернетична війна); формування й масове поширення інформаційними каналами супротивника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри й орієнтацію населення й осіб, що ухвалюють рішення (психологічна війна) [163].

Серед ознак інформаційної війни в умовах інформатизації можна відзначити, зокрема, більш глибоке врахування стану «мішені» (об'єкта нападу), впливу на сфери відносин, регіон, психології людей, особливостей масової свідомості; адресність різних форм інформаційних війн. Загальною ознакою інформаційних війн є масовість впливу на обране середовище впливу.

Результати й наслідки ведення інформаційної війни можуть виражатися у впливі на перспективу розвитку суспільства, на організаційне значення діяльності держави, руйнування цілісності особистості тощо. Ф.Уебстер у цьому зв'язку відзначає: «Після того як ми твердо встановили роль інформації в розвитку капіталістичного суспільства й визнали місце рефлексивної модернізації й теоретичного знання, нагромадженням якого супроводжується

розвиток капіталізму, ми створили виняткові умови для управління власним майбутнім»[239, с. 292-298].

Інформаційна війна, з урахуванням існуючих точок зору на її природу, може бути визначена як сукупність цілеспрямованих інформаційних впливів, що здійснюються суб‘єктом впливу на інформаційні системи або соціальні процеси з використанням засобів інформаційних технологій, інформаційних ресурсів і комунікацій шляхом створення факторів гальмування сталого розвитку або трансформації стабільності держави, суспільства, людини з метою втримання (досягнення) панування, переваги, монополії в різних сегментах людського буття [62, 78, 82-83, 107, 123,125, 135-138, 141, 143, 207].

Деякі дослідники вказують на те, що термін "інформаційна війна" щодо сучасних інформаційних способів ведення війни не зовсім адекватний і було б більш правильно називати цей вид воєнних дій інформаційною боротьбою, розглядаючи його як інформаційну складову збройної боротьби [86]. Втім вважаємо, що в умовах сьогодення інформаційна війна не лише супроводжує збройні акції, але й може їх замінювати. Це можна побачити на прикладі моделі так званої «мережоцентричної» війни як системи, що складається з трьох підсистем: інформаційної, сенсорної (розвідувальної) і бойової. Інформаційна підсистема пронизує собою всю систему в повному обсязі, забезпечуючи взаємодію інших її складових. У сучасних умовах, як показує досвід останніх військових конфліктів, агресія гіпотетичного супротивника реалізується у два етапи. На першому етапі цілями враження обираються критично важливі об'єкти держави-жертви виходячи з концепції так званих "п'яти кілець полковника Уордена": політичне керівництво, система життєзабезпечення; інфраструктура; збройні сили й населення. При цьому одночасно з бойовими діями здійснюються скоординовані операції інформаційної війни: інформаційно-психологічні операції; електронне придушення й знищення системи державного, економічного, фінансового й військового управління, зв'язку, розвідки тощо; наступальні комп'ютерні операції. Другий етап агресії - наземне вторгнення - може й не початися, оскільки власне вже перший етап може забезпечити досягнення мети [186-187].

Крім того, не виключено ведення інформаційної війни або використання окремих прийомів інформаційної війни для досягнення інших цілей, ніж геостратегічні.

Вирізняльними ознаками інформаційної війні А.Манойло вважає застосування інформаційної зброї й особливу організаційну форму ведення підривних дій - інформаційно-психологічні операції [161-162], тож варто зупинитися на змісті цих понять детальніше.

Існують різні визначення інформаційної зброї (Information weapon): у вузькому сенсі - це сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виведення з ладу функцій або служб інформаційної інфраструктури загалом або окремих її елементів. У широкому сенсі під інформаційною зброєю розуміються способи цілеспрямованого інформаційного впливу на супротивника, рефлексивного управління ним з метою зміни його задуму на проведення стратегічних або тактичних дій у потрібному напрямку [162].

Як зазначають Ж.Мина, А.Яновська та О.Матвійчук, інформаційна зброя – це засоби, які спрямовані на активізацію або гальмування в інформаційній системі процесів, в яких зацікавлений суб'єкт, що застосовує зброю. Сюди відносять різноманітні засоби знищення, перекручування або розкрадання інформаційних масивів, обмеження або заборони доступу до них законних користувачів, виведення з ладу інформаційно-комп’ютерних технологій, комп'ютерних систем, та й загалом усього високотехнологічного функціонування держави [168].

Інформаційну зброю характеризує передусім її цільове призначення і адресний контекст, адже фіксованих форм та змісту вона не має. Так, інформація «стає» інформаційною зброєю в разі включення до цілеспрямованої програми впливу на інформаційну систему, здатної призвести до досягнення запланованих суб‘єктом впливу результатів. Як інформаційна зброя можуть використовуватися й інформаційні технології - не лише як потенційно призначені для обробки, передачі та виконання інших запланованих дій з

інформацією, а й у поєднанні з передачею адресатові інформації певного характеру, зокрема, задля впливу на інформацію, що циркулює в інформаційних системах, або її одержання. Застосування інформаційної зброї та настання в результаті запланованих наслідків опосередковуються належним сприйняттям змісту інформаційного впливу тією мішенню, проти якої інформаційну зброю було застосовано.

Нищівна здатність інформаційної зброї та її цільове призначення є контекстно залежними від якостей мішені, а також визначаються потенційною спроможністю ефективно викликати в стані, структурі або поведінці мішені інформаційного впливу наслідки, бажані для суб‘єкта впливу. Інформація, за допомогою якої здійснюється інформаційний вплив, має бути індивідуально призначена для його мішені: зокрема, комп‘ютерний вірус може ефективно впливати на інформацію, що циркулює в автоматизованих системах (якщо планується її знищити, блокувати чи модифікувати), а компрометуюча інформація так само ефективно впливатиме на суспільне ставлення до певної особи, однак взаємна зміна мішеней впливу для цих різновидів інформаційної зброї не призведе до очікуваного результату. Інформаційна зброя також може виступати як призначена для впливу на обмежену або ж необмежену кількість мішеней. За межами певного контексту застосування інформація або інформаційні технології не лише втрачають нищівну здатність, але й припиняють існування в якості інформаційної зброї, тобто втрачають якості алгоритму, за допомогою якого може бути здійснений ефективний вплив на конкретну мішень. Це викликано можливістю різнобічного застосування однієї й тієї ж інформації [212, с. 99, 142, 160, 398].

Небезпека, реальність та ефективність проявів інформаційної війни забезпечується сугестивним характером впливів, таємним або завуальованим характером несанкціонованого одержання інформації чи її застосування, інших шкідливо-результативних дій в інформаційній сфері, які, в свою чергу, безпосередньо створюють умови для утиску інтересів або порушення процесів функціонування інформаційних систем [78; 245, с. 290; 83, с. 21-38; 107, 125, 135-138, 141, 143, 207].

Вперше спроба надати таким явищам, як інформаційна війна та інформаційна зброя нормативне визначення та перевести їх з розряду політичних проблем до проблем правових була здійснена в проекті Закону Республіки Білорусь «Про інформаційну безпеку» [206]. В Україні термін «інформаційна війна» також застосовувався в положеннях чинних нормативно-правових актів з початку 2000х років [196], хоча визначення та правової оцінки це явище досі не отримало.

Інформаційна зброя є засобом здійснення інформаційних операцій. При цьому під інформаційними операціями традиційно розуміють дії, що застосовуються для досягнення інформаційних переваг у забезпеченні воєнної стратегії шляхом впливу на інформацію, інформаційні системи та інформаційну інфраструктуру супротивника з одночасним посиленням забезпечення безпеки власної інформації, інформаційних систем та інформаційної інфраструктури [157] (як вже зазначалося, мова йде не лише про інформаційне супроводження традиційних війн або інформаційну війну як інструмент геополітичних змін, але й про будь-які прояви інформаційної війни). Більш універсальним визначенням інформаційних операцій є наступне – «акції, спрямовані на інформацію та інформаційні системи супротивника,і захист власної інформації та інформаційних систем» [99, с.5]. Деякі визначення зосереджуються лише на окремих аспектах досліджуваного явища.

Зокрема, а психологічному аспекті СІО зосереджується у своєму визначенні і К.Будилін, який пропонує розуміти під інформаційною операцією "сукупність погоджених і взаємозалежних за метою, завданнями, місцем і часом інформаційних ударів і атак, заходів щодо оперативного маскування, дій щодо знищення (виведення з ладу) об'єктів інформаційної інфраструктури, радіоелектронної боротьби, психологічних і пропагандистських акцій, проведених одночасно й послідовно за єдиним задумом і планом для вирішення завдань військово-політичної діяльності". Автор також відзначає, що в ході проведення інформаційних операцій використовуються спеціальні методи (політичні, економічні, дипломатичні, військові й інші), а також способи й засоби для впливу на інформаційно-психологічне середовище конфронтуючої

сторони в інтересах досягнення поставлених цілей [61].

Як зазначає О.Деньщиков, військово-політичне керівництво США розрізняє інформаційні операції в широкому й вузькому (військовому) сенсі. Так, інформаційні операції, що розуміються в широкому сенсі, - це форма боротьби, що становить використання спеціальних (політичних, економічних, дипломатичних, військових і інших) методів, способів і засобів для впливу на інформаційне середовище конфронтуючої сторони й захисту власної в інтересах досягнення поставлених цілей. У цьому сенсі трактування поняття "інформаційні операції" найбільш близьке до поняття "інформаційне протиборство", яке передбачає використання сил і засобів інформаційної боротьби у всіх аспектах міждержавних відносин.

На думку американського військового керівництва, інформаційні операції в ході ведення воєнних дій становлять сукупність методів впливу на інформаційні ресурси й системи супротивника при захисті власних інформаційних ресурсів і систем з метою захоплення інформаційної переваги, домінування в інформаційному просторі тощо. Таким чином, поняття "інформаційна боротьба" ("Information warfare") передбачає комплексне застосування сил і засобів інформаційних операцій і збройної боротьби у період актуалізації загрози і при веденні бойових дій.

На відміну від інформаційної боротьби, інформаційні операції ведуться як у мирний, так і у воєнний час. Основні цілі інформаційних операцій полягають у створенні в супротивника неадекватного сприйняття реальної обстановки й порушенні його можливостей з управління військами [94]. Фахівці також визначають інформаційні операції як сукупність заходів гласного та негласного характеру, спрямованих на приховане управління процесами інформаційної сфери. На відміну від пропагандистських заходів, вони мають обмежену у часі тривалість, підпорядковані конкретній меті та координуються єдиним центром – спеціальними службами [150]. Фактично, за наявності у інформаційних операцій такого координуючого центру, мова має йти про СІО. Так, на думку О.Заруби, СІО – це інформаційні операції, які проводяться в інтересах забезпечення національної безпеки з використанням сил безпеки і оборони

[109]. Як правило, СІО складається з спеціальних інформаційних акцій (далі – СІА), або акцій інформаційного впливу (далі – АІВ), які мають простий склад, відносно короткий термін дії, одноразовий непродовжуваний характер.

О.Литвиненко визначає СІО як «інтегроване використання можливостей електронної зброї, комп'ютерних мережевих операцій (CNO), психологічних операцій (PSYOP), операцій з військової дезінформації і дезорганізації та операцій безпеки (OPSEC) для використання можливостей впливу на людську свідомість з метою руйнування, розкладання, або й взагалі перехоплення впливу на прийняття рішень противника, при цьому захищаючи своє власне (рішення)» [150]. Цієї ж точки зору дотримуються також О.Додонов та Д.Ланде [99]. Як бачимо, таке визначення робить наголос саме на деструктивному харатері СІО, що є виправданим з урахуванням загального контексту проведення СІО, який завжди передбачає наявлість суб'єкта (уповноваженого державного органу, збройного формування тощо) та об'єкта (потенційного супротивника або «транзитної мішені», вплив на яку дозволяє опосередковано чинити вплив на супротивника).

Про те, що СІО чинить негативний вплив на об'єкт, зазначає і В.Петрик, досліджуючи рівні проведення СІО та АЗА (акти зовнішньої інформаційної агресії), що є справедливим, адже йдеться про інспіровану ззовні зміну стану інформаційної системи (водночас, важко стверджувати, що СІО не призводитимуть до позитивних наслідків для суб'єктів їх проведення.

Так, на думку В.Петрика, АЗА(акти зовнішньої інформаційної агресії) та СІО вміщують у себе психологічні дії зі стратегічними цілями, психологічні консолідуючі дії та психологічні дії з безпосередньої підтримки бойових дій. Дослідник також зазначає, що СІО та АЗА відбуваються на макро- й мікрорівнях. На макрорівні це будь-яка агітаційно-пропагандистська і розвідувально-організаційна діяльність, орієнтована на конкретні соціальні групи людей і здійснювана здебільшого через засоби масової інформації та каналами зв'язку. СІО та АЗА мікрорівня, зісвого боку, уособлюють будь-яку агітаційно-пропагандистську й розвідувально-організаційну діяльність ідеологічного характеру, прицільно персоналізовану і здійснювану переважно

через міжособистісне спілкування. Для цього практикується поширення чуток чи інші методи негативного інформаційного впливу.

Відповідно, СІО розглядається як «проведення спецслужбами, передусім іноземних держав, таємних операцій та акцій негативного чи навіть деструктивного ідеологічного, ідейно-політичного та соціального впливу на особу, групу осіб або суспільство в цілому зметою їх переорієнтації на інші цінності та ідеали, підштовхування до вчинення протиправних дій із підриву й послаблення державного та суспільно-політичного утрою». Втім В.Петрик одночасно пропонує і наступне визначення СІО – «це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, з метою схилення до прийняття управлінських рішень або (та) вчинення дій, вигідних для суб'єкта інформаційного впливу. СІО можуть містити також вплив на інформаційно-технічну інфраструктуру, але для більш ефективного впливу на свідомість і поведінку людей» [179]. Так визначення, як бачимо, має певний психологічний ухил, однак висвітлює універсальний характер застосування інформаційної зброї, а також передбачає доволі широкий спектр напрямків використання СІО, в т.ч. не лише деструктивних. Також необхідно звернути увагу на підкреслення спеціального характеру відповідних операцій – з інформаційних операцій в цілому їх вирізняє саме проведення спецслужбами. В своє чергу, ця обставина зумовлює прихований характер проведення СІО, які для об'єктів впливу не анонсуються і проводяться з використанням негласних форм і методів діяльності спецслужб.

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, а Служба безпеки України протидіє проведенню проти України СІО, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій [205]. Виходячи з такого розуміння СІО, вони можуть носити як інформаційно-

технічний, так і інформаційно-психологічний характер, тобто, охоплювати всі напрямки інформаційного протиборства.

Оскільки СІО можуть проводитись не лише в ході наступальної інформаційної війни, але й з метою забезпечення національної безпеки, в узагальненому вигляді під СІО у функціональному спекті пропонується розуміти алгоритм застосування інформаційної зброї/ нейтралізації загрози в інформаційній сфері, використання якого забезпечує досягнення мети інформаційної війни/ забезпечення інформаційної безпеки (принагідно зауважимо, що наразі таке визначення не становитиме правової дефініції СІО, формулювання якої маємо здійснити за результатами дослідження). Як і для будь-яких акцій застосування інформаційної зброї, для СІО характерний цільовий контекст, причому ми можемо виокремити об'єкт впливу (цільову аудиторію, а також інформаційні ресурси й інформаційні системи, вплив на які у низці випадків опосередковує вплив на цільову аудиторію)) й об'єкт спрямування («мішень») СІО, які можуть не співпадати, а також власне об'єкт СІО (людина, суспільство, держава – ті об'єкти національної безпеки, на захист яких або проти яких спрямовується СІО за основним задумом. Навіть, якщо СІО спрямовується, наприклад, на заволодіння секретною інформацією, зафіксованою на певному матеріальному носієві – кінцевою метою таких дій є послаблення державної безпеки, порушення роботи державних органів, дискредитація певних осіб).

Фактично, досліджуючи інформаційно-правові засади СІО ми ведемо мову про організаційно-правові засади їх проведення, а також про теоретико-методологічні засади інформаційного забезпечення СІО. Тож квінтесенція змісту цієї складної та взаємообумовленої категорії (проведення СІО вимагає передусім інформації правового характеру, яка визначає підстави й межі проведення СІО, і за своїм змістом є переважно інформаційною діяльністю, тож передбачає ґрунтовну інформаційну підготовку, збір та використання різнопланової – залежно від мети, об'єкта, суб'єктів СІО тощо - інформації) може бути закумульована у поняттях правового та інформаційно-правового забезпечення [144] СІО, які далі будуть використовуватись у цій роботі. Ці

поняття можуть бути віднесені до інтуїтивно-зрозумілих і є дотичними до основних категорій інформаційного права.

Так, правове забезпечення СІО доцільно визначити як комплекс заходів, пов'язаних з розробкою та реалізацією норм права, що регламентують проведення СІО, а також із забезпеченням правового супроводу проведення СІО та профілактикою порушень вимог законодавчих та інших нормативно-правових актів в ході їх проведення. При цьому, оскільки прийняття відповідальних управлінських рішень щодо планування та проведення СІО передбачає використання як правової, так і іншої інформації, під інформаційно-правовим забезпеченням СІО в контексті цього дослідження будемо розуміти комплекс заходів організаційно-правового та теоретико-методологічного характеру щодо задоволення потреб суб'єктів СІО у правовій та іншій інформації, необхідній для проведення СІО відповідно до вимог чинного законодавства.

1.3. Методологія дослідження проблематики правового забезпечення спеціальних інформаційних операцій

Головна ідея і основні положення концепції дослідження відображені в гіпотезі, що ґрунтується на припущенні, за яким належне інформаційно-правове забезпечення СІО на основі норм та принципів інформаційного права дозволить підвищити ефективність проведення СІО, що сприятиме забезпеченню національної безпеки України та досягненню нашою державою інформаційних переваг у реальних та потенційних інформаційних конфліктах, в т.ч. в ході гібридної війни. При цьому беззаперечним є те, що саме методологія вважається головним орієнтиром наукового пошуку, надійним засобом встановлення істини в галузях науки.

Чималу увагу методологічним проблемам приділено в наукових працях О.Бандурки, А.Васильєва, Г.Гальперіна, В.Гоймана, В.Ісакова, Д.Керімова, Н.Нижник, І.Рассохи, С.Мосова, О.Скакун та багатьох інших учених. Водночас особливості вирішення будь-якої наукової проблеми, зокрема проблематики

інформаційно-правових засад СІО, вимагають певної методики та методів дослідження.

Поняття “методологія” та поняття “метод” у деяких наукових школах вважають тотожними, хоча вітчизняна наука чітко розмежовує ці поняття.

Так, у науковій літературі зустрічаються різні поняття терміну “методологія”. Серед них найбільш розповсюджені філософські поняття, де методологія розглядається як філософське вчення про методи пізнання та практику, або перетворення дійсності. На думку О. Скакун, методологія – це система визначених теоретичних принципів, логічних прийомів, конкретних способів дослідження предмета науки. Теоретичні принципи – історія, єдність логічного й історичного. Логічні прийоми – дедуктивний та індуктивний умовивід, аналіз і синтез, порівняння, узагальнення. Конкретні способи дослідження – інструменти пізнання, застосовувані для встановлення знання про досліджуваний предмет [223, с. 2]. В.Шейко та Н.Кушнаренко вважають, що у предмет загальної методології науки входять такі питання, як специфіка наукового пізнання в порівнянні з повсякденним мисленням, основні особливості і закономірності науково-пізнавальної діяльності, відношення емпіричного і теоретичного рівнів наукового дослідження, гіпотеза як форма розвитку науки, пояснення і передбачення як вихідні функції наукового мислення, загальні прийоми наукового дослідження – абстрагування, ідеалізація, моделювання, закон як форма наукового пізнання, природа, структура й функції наукової теорії закономірності її формування і розвитку, взаємовідношення теорії і її емпіричного базису [252, с. 35].

У цілому доробки, відображені у працях низки вчених, дають змогу дійти висновків, що поняття методології тлумачать у двох аспектах: 1) система певних способів і прийомів, які застосовують у певній сфері діяльності (наприклад, науці, політиці, мистецтві тощо); 2) вчення про цю систему, загальна теорія методу, теорія в дії.

Переходячи від узагальненого уявлення методології як науки про метод до більш конкретного розуміння її сутності, зазначимо, що науковцями виділяється кілька аспектів інтерпретації цього поняття. Зокрема, методологія

розглядається як наука про метод або ж теорія методу, що розкриває його сутність, концептуально пояснюючи його пізнавальні, оцінні або практичні можливості, разом з тим розглядає структуру, механізм, алгоритм, межі, переваги й недоліки методу. Однак, наукою дотепер не вироблена єдина теорія методу, а існує безліч різних теорій і концепцій. При цьому сутність методології зводиться до сукупності принципів, що є орієнтирами при побудові й здійсненні людської діяльності. Слід зауважити також, що до методології відносять усе, що можна розглядати як метод діяльності. До методології практичної діяльності поряд із принципами практики відносять теорії матеріальної цілеспрямованої людської діяльності, а також методи і конкретні прийоми їхнього здійснення. У методологію пізнавальної діяльності поряд із принципами пізнання входять теорії методів, власне методи пізнання, а також прийоми і правила пізнавальної діяльності, тобто усе, що можна використовувати для одержання знань як метод.

При цьому у дослідженні проблематики інформаційно-правових засад СІО методологічність наукового підходу є усвідомленим ставленням до засобів і передумов діяльності щодо формування, функціонування й удосконалення діяльності сектору безпеки і оборони країни [198] в аспекті проведення СІО на основі організаційних та правових засад. То ж в цілому методологія покликана виконувати дві основні функції: 1) отримання нового знання та подання цього знання у вигляді понять, критеріїв, законів, теорій, гіпотез; 2) організація використання нових знань у практичній діяльності. Тож завдяки правильно обраній методологічній системі способів і прийомів нам вдасться одержати нові знання щодо проблематики інформаційно-правових засад СІО.

У свою чергу, метод (грец. – шлях дослідження чи пізнання) – це спосіб організації практичного й теоретичного освоєння дійсності, зумовлений закономірностями розвитку об’єкта [167]. Це також сукупність прийомів чи операцій практичного або теоретичного освоєння дійсності, підпорядкованих вирішенню конкретного завдання. Відмінність між методом і теорією має функціональний характер: формуючись як теоретичний результат попереднього дослідження, метод виступає вихідним пунктом та умовою майбутніх

досліджень [107, с. 23]. Отже, під методом у нашому випадку слід розуміти сукупність конкретних прийомів і способів пізнання, перетворення чи оцінки дійсності. Якщо під методологією зазвичай розуміють сукупність знань про методи, то під методом – певну сукупність прийомів, способів та засобів досягнення визначеного результату чи досягнення мети, тобто вирішення поставлених завдань. Відтак метод є складовою методології.

У роботі використовувалася сукупність теоретичних та емпіричних методів дослідження, що властиві науковим розробкам у сфері інформаційного права та забезпечення національної безпеки. Так, застосування діалектичного методу надало можливість визначити зміст та встановити специфіку інформаційно-правового забезпечення СІО в сучасних умовах, вивчити зарубіжний досвід у цій сфері. За допомогою системно-структурного методу було досліджено недоліки нормативно-правового регулювання та прикладні проблеми інформаційно-правового забезпечення СІО в діяльності українських спецслужб. Метод правового аналізу дав змогу охарактеризувати правові норми відповідних галузей права, що стосуються питань інформаційної безпеки та проведення СІО, а також визначити шляхи удосконалення нормативної бази у відповідній сфері. Використання формально-логічного методу сприяло формуванню понятійного апарату дослідження, дозволило сформулювати відповідні пропозиції з внесення змін до актів чинного законодавства, якими регламентовано питання проведення СІО, а також сформулювати висновки дисертації. Порівняльно-правовий та історичний методи дозволили дослідити історичну ретроспективу становлення інформаційно-правового забезпечення СІО та провести узагальнення досвіду інших країн з питань проведення СІО. За допомогою методу моделювання визначено та оптимізовано модель СІО. На підставі використання соціологічного та статистичного методів визначено актуальні підходи до сутності інформаційної безпеки, досліджені стан та властивості інформаційно-правового забезпечення СІО в сучасних умовах. Зокрема, застосування соціологічного і соціотехнічного підходу до інформаційної безпеки в умовах глобалізації на основі тензорної методології складних систем полягає в тому, що інформаційне протиборство розглядається

на основі концепції специфічної інформаційної реальності, що обумовлена не лише розвитком технологій, але й глобальною фінансово-економічною кризою, та характеризується загостренням протиріч між динамічними турбулентними процесами глобалізації й зростанням значущості національної держави та її безпеки в інформаційному протиборстві. Крім того, тензорна методологія дозволяє обґрунтовано пов'язувати процес і структуру, що набуває особливого значення для організації та проведення СІО (складової системи стратегічних комунікацій) при розуміння інформації як комунікації. Застосування тензорної методології також дозволяє представляти будь-яку систему з низки аналогічних систем як проекцію узагальненої системи. «Якщо розглядати узагальнену систему як тензор, а конкретні системи цього класу – як її проекції в окремих системах координат, то можна використовувати головне для тензорного методу», а саме – «необхідно обрати одну систему і використати її як еталонну систему координат, приводячи описи (рівняння) інших систем до опису в термінах цього еталону (моделювати)» [180, с.12]. Тензорна методологія носить міждісциплінарний характер, тому що вона дозволяє виступати в якості єдиного, "наскрізного підходу" при вивченні складних систем різної природи.

Система правил використання методів, прийомів та операцій становить суть методики дослідження. Набір конкретних методів дослідження визначається характером фактичного матеріалу й метою дослідження. Методи є упорядкованою системою, де їхнє місце визначене відповідно до конкретного етапу дослідження, використання технічних прийомів і проведення операцій з теоретичним і фактичним матеріалом у певній послідовності.

Нормативно-правовою основою роботи стали як Конституція та законодавство України, зарубіжних країн, міжнародно-правові акти, що регулюють питання національної та державної безпеки, інформаційного протиборства та характеризують інформаційно-правові засади СІО.

Слід також зауважити, що кожна складова в структурі методології має своє особливе призначення, і одночасно несе в собі системотвірну функцію. Іншими словами, на сучасному етапі вирішення питань ефективності КРЗ потребує застосування синергетичного підходу, зокрема одночасного використання

різних методів досліджень.

Для синергетики властивий підхід щодо виявлення одного, головного фактору, який здійснює основний вплив на процес руху до “порядку”, і якому підкорені всі інші зміни [181, с. 64]. Цей фактор умовно називається “параметр порядку”, що не дозволяє безпосередньо керувати розвитком системи, тобто переводити її в інший, заздалегідь визначений стан. Оскільки синергетика має справу з конкретними системами (в юриспруденції – це правова система, а її однією з мікроструктур є правовідносини, у нашому випадку пов’язані з інформаційно-правовим забезпеченням СІО), то слід констатувати, що “параметром порядку” цієї мікроструктури вони й мають бути. Відповідно, найкращим варіантом формування теоретичних, організаційних та правових засад СІО буде виділення відповідного фрагменту дійсності, який має значення і викликає інтерес у суб’єктів права [181, с. 160-161].

У свою чергу, основні засади будь-якої діяльності, зокрема й проведення СІО, визначають принципи, що формують загальні напрями і правила в конкретній сфері суспільних відносин. До загальнонаукових принципів дослідження належать: історичний, термінологічний, функціональний, системний, когнітивний, метод моделювання тощо.

Історичний принцип дає змогу дослідити виникнення, формування і розвиток теорії та практики інформаційно-правового забезпечення СІО, в хронологічній послідовності з метою виявлення внутрішніх та зовнішніх зв’язків, закономірностей та суперечностей. У межах історичного підходу активно застосовується порівняльно-історичний метод – сукупність пізнавальних засобів, процедур, які дозволяють виявити схожість і відмінність між організацією діяльності в різних галузях соціальних відносин та діяльністю щодо інформаційно-правового забезпечення СІО, визначити їхню генетичну спорідненість (зв’язок за походженням), загальне й специфічне в їхньому розвитку. В основі загальнонаукового принципу історичного підходу лежить діалектичний закон руху як способу існування матерії і свідомості. Врахування цього закону у поєднанні з принципом системності є обов’язковою вимогою наукового пошуку. У цьому контексті при історичному підході до

інформаційно-правового забезпечення СІО на перший план виступають закономірності становлення цього напряму діяльності у забезпеченні національної безпеки, що застерігає від суб'єктивізму й однобічного підходу, забезпечує системність дослідження.

Слід наголосити, що природа науки та її методології принципово системна, відтак у загальнонауковій методології широко застосовується системний підхід, який для дослідження інформаційно-правового забезпечення СІО грає визначальну роль. Сутність його полягає в комплексному дослідженні великих і складних об'єктів (систем), вивченні їх як єдиного цілого з узгодженим функціонуванням усіх елементів і частин.

Визначальною основою дослідницького етапу конкретно-наукової методології є сукупність ідей або специфічних методів юридичної науки, які є базою для розв'язання конкретної дослідницької проблеми та на які ми опираємось в нашому дослідженні. Конкретна наукова методологія потребує також звертання до загальновизнаних концепцій провідних учених. Наші пошуки методологічних засад дослідження здійснювалися за такими напрямами: історіографія, в межах якого було проведено вивчення наукових праць провідних учених як з теорії безпекознавства, так і в галузях міжнародного, інформаційного, військового, кримінального, адміністративного права тощо, які застосовували загальнонаукову методологію для вивчення конкретного напрямку організації діяльності в сфері правозастосування; узагальнення ідей науковців, які безпосередньо вивчали проблеми правозастосування у зазначених галузях; проведення досліджень специфічних підходів для вирішення наукових питань в сфері практичної діяльності структур сектору безпеки і оборони, які не лише розробили, а й реалізували на практиці свої ідеї; аналіз концепцій у правовій сфері міжнародної діяльності та зарубіжних учених і практиків.

Прикладним показником істинності наукової інформації, як відомо, є практика. Однак практику не можна розуміти лише як суто емпіричний досвід сьогоднішнього дня. Більш широке розуміння практики включає насамперед суспільно-історичну практику розвитку людського суспільства в цілому.

Проблема достовірності результатів наукової роботи може бути вирішена тільки в процесі одержання достовірного знання про досліджуваний об’єкт, де всі етапи аналізу і прогнозування представляють органічні складові частини єдиного цілісного пізнавального процесу.

Шлях пізнання певного процесу може бути традиційним: від аналізу конкретних явищ до їх абстракції – поняття, а від них до тієї реальної дійсності, з якої починалося пізнання [50, с. 73-74]. На сучасному рівні розвитку юридична практика та наука накопичили широкий масив наукових знань щодо різноманітних юридичних фактів стосовно інформаційно-правового забезпечення СІО, а також достатній теоретичний та методологічний потенціал цих знань, які сьогодні потребують узагальнення з позиції виникнення, розвитку, функціонування, призначення і сутності правових явищ. Наукове дослідження теоретичних, правових та організаційних засад інформаційно-правового забезпечення СІО як цілісного й гармонійного явища потребує застосовування усієї сукупності пізнавальних засобів, що вироблені наукою та практикою. Загальним при цьому виступає діалектичний метод, основу якого складає зв’язок теорії і практики, взаємодія зовнішнього і внутрішнього, адже діалектичний закон загального зв’язку явищ лежить в основі загальнонаукового принципу системності, що поширився на норми права та правозастосування. З іншого боку, правові норми формулюють умови переходу суспільних відносин в інший якісний стан – правові відносини. Тут наявна загальна закономірність єдності форми і змісту, переходу кількості в якість [107, с. 68]. Враховуючи викладене, цю єдність з її кількісно-якісною характеристикою складають цілі, завдання, функції, принципи та методи інформаційно-правового забезпечення СІО та наявність відповідного організаційного механізму їх проведення.

Як бачимо, дослідження теоретичних, правових та організаційних засад інформаційно-правового забезпечення СІО, як процес пізнання, що протікає відповідно до загальних законів діалектики, має свою специфіку, обумовлену особливостями об’єкта пізнання і правозастосовної діяльності. Разом з тим, потрібно враховувати, що юридичне пізнання спирається на дослідження філософських, спеціально-юридичних та прикладних наук.

Вирішення завдань інформаційно-правового забезпечення СІО має здійснюватися із обов'язковим застосуванням аксіологічного підходу як гуманістичної та моральної основи. Аксіологічний підхід до організації діяльності полягає в тому, що його учасники, складаючи частину правовідносин, є внутрішньою структурою. Він має важливе значення для суб'єкта правовідносин, вирішуючи певні протиріччя. Аксіологія у вивченні права має важливе наукове, практичне та моральне значення, адже це загальна стратегія дослідження, що визначає розгляд правозастосування в інформаційно-правовому забезпеченні СІО крізь призму відповідності певним цінностям, що можуть забезпечуватись правом та бути його основою.

Як вже зазначалося, емпіричні проблеми у нашому дослідженні вирішуються насамперед з урахуванням матеріалів, даних та здобутків вітчизняних науковців та практиків. Проте, пошук шляхів розв'язання цих проблем не можливий без порівняльних досліджень та використання світових доробок у теорії та методології організації діяльності іноземних спеціальних служб з врахуванням особливостей правових систем держав їх належності. Порівняльно-правовий аспект дослідження особливо актуалізується в умовах реалізації євроінтеграційних прагнень України.

Водночас не слід забувати, що цей аспект базується на тому, що правові системи світу демонструють розмаїття фактологічних передумов національного правового регулювання, що визначається способами юридичної ідентифікації форм, методів діяльності, їх "виділення" з поведінки, життєвих ситуацій. Звідси, врахування особливостей іноземного досвіду проведення СІО не може бути безумовним, адже організаційні та правові засади проведення СІО у будь-якій країні формуються в умовах саме її геополітичних і правових реалій, які не є характерними для України.

Таким чином, методологія цього дослідження, яку обрано з урахуванням його мети, завдань, об'єкта і предмета, передбачає інтегроване використання загальнонаукових та спеціальних методів дослідження, що застосовуються у філософській та управлінсько-правовій науці.

За застосування системного підходу, в процесі дослідження об'єкт

дослідження уявно поділяється, виокремлюється його елементи, його зовнішні і внутрішні зв’язки, окреслюється його структура і висувається припущення про механізм його функціонування та розвитку. Кожну конкретну науку, діяльність, об’єкт можна розглядати як певну систему, що має множину взаємопов’язаних елементів, компонентів, підсистем, визначені функції, цілі, склад, структуру. До загальних характеристик системи відносять: цілісність; структурність; взаємозв’язок із зовнішнім середовищем; ієрархічність; цілеспрямованість; самоорганізацію.

У тісному зв’язку із системним підходом також широко використовувався структурно-функціональний метод. Цей метод передбачає розгляд будь-якого явища як системного з обов’язковим аналізом функцій взаємодіючих елементів.

У дослідженні теоретичних, правових та організаційних засад проведення СІО та їх інформаційного забезпечення використовувалося два основних рівня наукового пізнання: емпіричний і теоретичний. Ці рівні зумовлюють формування в межах методів, використовуваних нами, як теоретичних, так і емпіричних процедур і прийомів, систематичне застосування яких приводить до досягнення поставленої мети.

Емпіричні методи пізнання є не лише основою для закріплення теоретичних передумов, а й часто становлять предмет нового відкриття, нового наукового дослідження. Характерною особливістю емпіричного пізнавального рівня є те, що він включає в себе безпосередній контакт дослідника з предметом дослідження; дає знання зовнішніх, видимих зв’язків між формою та змістом їх діяльності. Кінцевою метою емпіричного пізнання є фіксація повторення явищ, що приводить до обґрунтованих узагальнень. Емпіричні знання у нашому дослідженні спираються на емпіричні факти практики шляхом вивчення навчальної, навчально-методичної літератури, публікацій у ЗМІ, аналітичних матеріалів тощо. Використання результатів практичної діяльності – це найбільш загальний емпіричний метод пізнання, який не лише включає спостереження й оцінювання, а й здійснює трансформацію, зміну об’єкта дослідження тощо.

У свою чергу, теоретичним рівнем пізнання є, по-перше, логічне

узагальнення практичного досвіду управління; по-друге, протилежні емпіричним методам наукові методи пізнання. Теоретичне знання має загальний і необхідний характер, містить відомості про внутрішні закономірності спостережуваних явищ. На цьому рівні можна отримати певні знання не тільки за допомогою досвіду, але й абстрактного мислення. В теорії пізнання превалює застосування способу сходження від абстрактного до конкретного як метод дослідження, при якому науковий пізнавальний процес веде від менш змістовного до більш змістовного знання. У теоретичному дослідженні, де в основному використовується здатність суб'єкта до абстрактного мислення, будь-яке поняття асоціюється з певною сукупністю сприйнять і наочних образів. Тобто, емпіричне пізнання теоретично навантажене, а будь-яка абстрактна теорія має емпіричну інтерпретацію [239, с. 37-38]. Головним пізнавальним завданням емпіричного рівня є опис явищ, тоді як на теоретичному рівні таким завданням є пояснення явищ, що вивчаються. Співвідносно відрізняються й методи, спрямовані на отримання цих типів знань.

На емпіричному рівні пізнання основними методами є спостереження, вимірювання, експеримент, порівняння, індуктивне узагальнення.

На теоретичному рівні пізнання використовуються такі методи, як аналіз, синтез, індукція, дедукція, аналогія, гіпотеза тощо [239, с. 36-37].

При цьому нами враховано, що з позиції сфери застосування загальні методи наукового пізнання, на відміну від спеціальних, використовуються в дослідницькому процесі в різних галузях науки. Вони умовно поділяються на три великі групи: методи емпіричного дослідження (спостереження, порівняння, вимірювання, експеримент); методи, що використовуються як на емпіричному, так і на теоретичному рівнях дослідження (абстрагування, аналіз і синтез, індукція і дедукція, моделювання та інші); методи або методологія, що використовуються на теоретичному рівні дослідження (сходження від абстрактного до конкретного, системний, структурно-діяльнісний підхід) [252, с. 25]. Так, теоретико-прикладна частина дослідження здійснювалась із застосуванням комплексу загальнонаукових методів:

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

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

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

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

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

Зі спеціальних методів під час дослідження використано:

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

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

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

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

– соціологічний і статистичний – у процесі вивчення кількісних та якісних

параметрів, що вказують на необхідність покращання інформаційно-правового забезпечення СІО, характеризують його стан, процес забезпечення національної безпеки в цілому (розділи 2, 3);

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

ВИСНОВКИ ЗА РОЗДІЛОМ

Проведене дослідження підтверджує, що глобальна історична тенденція просування світової цивілізації в інформаційну епоху свого розвитку обумовлює актуальність проблеми інформаційного протиборства в діяльності органів державного й військового управління щодо забезпечення інформаційної безпеки та національної безпеки в цілому в сучасних умовах. Не зважаючи на те, що інформаційний вплив використовувався в ході соціальних конфліктів (в тому числі збройних) з давніх давен, хвиля технічного прогресу внесла істотні зміни в методи вирішення геополітичних, військових, економічних, торговельних і інших конфліктів, тож силові методи наразі поступаються місцем методам інформаційним. У міру накопичення досвіду практичного здійснення інформаційного впливу на цільову аудиторію у більш широкому розумінні у військових конфліктах, економічних суперечках, політичній боротьбі тощо виникла потреба в його теоретичному осмисленні, що викликало до життя науковий інтерес до проблематики інформаційної війни та застосування інформаційної зброї, проведення інформаційних операцій тощо. Втім наразі залишаються недостатньо вивченими проблеми правового забезпечення СІО, котрі є інструментом ведення інформаційних війн та засобом забезпечення національної безпеки (зважаючи на цільовий характер застосування інформаційної зброї в ході інформаційної війни, тут і далі поняття «інструмент» і «засіб» щодо СІО вжито у широкому сенсі [49[1]], для позначення структурованих способів цілеспрямованого впливу на ті чи інші об’єкти, і

[1] Засіб – 1. Прийом, якась спеціальна дія, що дає можливість здійснити що-небудь, досягти чогось; спосіб; 2. Те, що служить знаряддям у якій-небудь дії, справі.
2. Інструмент – 1. Знаряддя для праці. 2. Сукупність таких знарядь.
3. Знаряддя – 1. Пристосування, прилад, механізм і т.ін., за допомогою якого виконується певна дія; 2. Те, що служить засобом у якійсь дії, справі.

фактично терміни «інструмент» і «засіб» застосовані як синоніми).

Поняття та категорії, що використовуються у дослідженні проблематики правового забезпечення СІО є доволі різноманітними, однак ключовими поняттями в даному випадку слід визнати наступні: інформаційна безпека, інформаційна загроза, інформаційна війна, інформаційна зброя, інформаційні операції, правове та інформаційно-правове забезпечення тощо. Більшість з цих категорій належать до базових категорій інформаційного права.

Інформаційна безпека в рамках комплексного підходу до її сутності може бути визначена як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, за якої забезпечуються формування, використання та розвиток інформаційної сфери в інтересах її суб‘єктів, сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці шляхом розвитку власного інформаційного простору, зведення до мінімуму заподіяння шкоди через неповноту, невчасність і недостовірність інформації, інформаційний вплив, негативні наслідки функціонування інформаційних технологій несанкціоновані дії з інформацією, а також постійний процес діяльності компетентних органів, спрямований на забезпечення й підтримання відповідного стану захищеності. Поняття інформаційної безпеки перебуває у тісному зв’язку із більш загальним щодо нього поняттям національної безпеки.

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

Особливістю інформаційних загроз є те, що впливаючи безпосередньо на інформаційну безпеку, вони можуть нести негативні наслідки для будь-яких складових національної безпеки. Інформаційна війна, з урахуванням існуючих точок зору на її природу, може бути визначена як сукупність цілеспрямованих

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

Інформаційну зброю характеризує передусім її цільове призначення і адресний контекст, адже фіксованих форм та змісту вона не має. Так, інформація «стає» інформаційною зброєю в разі включення до цілеспрямованої програми впливу на інформаційну систему, здатної призвести до досягнення запланованих суб‘єктом впливу результатів. Як інформаційна зброя можуть використовуватися й інформаційні технології - не лише як потенційно призначені для обробки, передачі та виконання інших запланованих дій з інформацією, а й у поєднанні з передачею адресатові інформації певного характеру, зокрема, задля впливу на інформацію, що циркулює в інформаційних системах, або її одержання. Застосування інформаційної зброї та настання в результаті запланованих наслідків опосередковуються належним сприйняттям змісту інформаційного впливу тією мішенню, проти якої інформаційну зброю було застосовано. Нищівна здатність інформаційної зброї та її цільове призначення є контекстно залежними від якостей мішені (при цьому як мішені можуть виступати технічні й біологічні інформаційні системи, через безпосередній вплив на які інформаційна зброя також може чинити руйнівний вплив на соціальні утворення), а також визначаються потенційною спроможністю ефективно викликати в стані, структурі або поведінці мішені інформаційного впливу наслідки, бажані для суб‘єкта впливу. Інформаційна зброя є засобом здійснення інформаційних операцій, в тому числі й СІО.

Оскільки СІО можуть проводитись не лише в ході наступальної інформаційної війни, але й з метою забезпечення національної безпеки, СІО у функціональному аспекті доцільно розглядати як алгоритм застосування інформаційної зброї/ нейтралізації загрози в інформаційній сфері, використання якого забезпечує досягнення мети інформаційної війни/

забезпечення інформаційної безпеки.

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

Методологія дослідження організаційно-правових і теоретико-методологічних засад інформаційно-правового забезпечення СІО становить систему методів (способів і прийомів), а також сукупність принципів, застосування яких уможливлює одержання нових знань щодо організації та проведення СІО. Зазначене дослідження базується на використанні комплексу загальнонаукових і спеціальних методів, властивих дослідженням з інформаційного права. Зокрема, застосовуються системно-структурний, формально-логічний, порівняльно-правовий, історичний, діалектичний, моделювання, порівняльного аналізу, соціологічний та статистичний методи, що дає змогу вивчити досліджувані об'єкт і предмет, активно вплинути на них з метою зміни й удосконалення. Особливу роль у дослідженні відіграє тензорна методологія, яка дозволяє обґрунтовано пов'язувати процес і структуру, що має особливе значення для проведення СІО як складової системи стратегічних комунікацій. Застосування тензорної методології також дозволяє поширити на СІО закономірності здійснення стратегічних комунікацій. Це забезпечує єдність методів, практичної діяльності й теорії, емпіричних і наукових знань.

РОЗДІЛ 2. Теоретико-методологічні та організаційно-правові засади інформаційно-правового забезпечення спеціальних інформаційних операцій

2.1. Спеціальні інформаційні операції у веденні інформаційної війни та забезпеченні національної безпеки

Інформаційну війну можна охарактеризувати як війну без зафіксованих кордонів, без чітко встановленої приналежності інформаційних систем тій або іншій стороні, що бере участь у протиборстві. При цьому виділяють наступні основні форми інформаційної війни: психологічна, економічна, хакерська, управлінська, розвідувальна, електронна, кібервійна тощо.

Використання СІО дозволяє досягати бажаного результату як у військових конфліктах, так і в політичній, економічній і соціальній сферах, зокрема, технологічно знищувати, спотворювати, викрадати інформацію, припиняти або обмежувати доступ до неї, виводити з ладу або порушувати роботу телекомунікаційних систем, що використовуються у забезпеченні життєдіяльності суспільства й державних структур. Об'єктом впливу за таких умов стають не лише інформаційні ресурси, алей й об'єкти матеріальної культури та власне люди (людська свідомість – як правило, кінцевий об’єкт впливу для СІО). Застосування в ході СІО інформаційної зброї дозволяє здійснювати прихований вплив не тільки на технічні системи протиборчої сторони, але й на індивідуальну, групову й суспільну свідомість, поведінку людей й на соціальну систему загалом.

Головна небезпека інформаційної війни - відсутність наочних руйнувань, характерних для звичайних війн. Населення навіть не відчуває, що воно зазнає впливу. У результаті суспільство не пускає в хід наявні в його розпорядженні захисні механізми, не відчуваючи небезпеки. Зауважимо, що використовувати специфічні можливості нових інформаційних технологій можна не тільки в районах бойових дій, але й проти будь-якої держави, великих корпорацій, бізнесменів тощо. Чим більше інформаційно розвинена країна, тим вище для

неї ризик, адже під загрозою може виявитися національна, регіональна й, в остаточному підсумку, глобальна безпека [253].

Як справедливо відзначають С.Жабчик і К.Токарєв [103], в епоху інформаційної революції руйнуються практично всі традиційні імперативи "класичної" геополітики, оскільки сьогодні три головні принципи, на яких базувалися класичні уявлення про міжнародні відносини (територія, суверенітет, безпека), не можуть більше вважатися такими, що адекватні сучасним реаліям. Феномен масової міграції людей, потоків капіталів, циркуляції ідей, деградації навколишнього середовища, поширення зброї масового знищення девальвують звичні уявлення про безпеку держави, національні інтереси, політичні пріоритети тощо, тоді як когнітологія стає наріжним каменем нового світогляду. Вітчизняний дослідник Ю.Канигін визначає її як інтелектуалізм, який становить нове бачення соціально-економічної динаміки, за якої інформаційно-семантична складова прогресу виступає визначальною [113, с. 41]. При цьому базовими факторами суспільного розвитку є інформаційно-комунікативні, тобто інтелектуальні, а провідною системою сучасної економіки - сфера переробки, передачі й використання знань. Відповідно, установлюється новий вид суспільних відносин - інформаційні, які детермінують інші суспільні відносини. Це обумовлює й докорінні зміни в системі здійснення геостратегії.

Зокрема, детермінаційний характер інформаційних відносин зумовлює той факт, що провідне місце серед тенденцій сучасного силового протистояння наразі належить геополітичному інформаційному протиборству. Це одна із сучасних форм боротьби між державами, а також система заходів, яка здійснюється однією державою з метою порушення інформаційної безпеки іншої держави, при одночасному захисті від аналогічних дій з боку супротивника. І. Панарин пропонує виділити два види інформаційної боротьби: інформаційно-технічну й інформаційно-психологічну, яка ведеться на стратегічному, оперативному й тактичному рівнях [177, с. 156-169]. СІО, як вже зазначалося, також можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки

інформаційного протиборства.

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

При проведенні СІО інформаційно-психологічного характеру (саме їх зазвичай розуміють як класичні приклади СІО) основними об'єктами впливу стають психіка представників політичної еліти й населення конфронтуючих держав, а також система формування суспільної свідомості, думки й прийняття державно-управлінських рішень у сфері національної безпеки. СІО психологічної спрямованості, таким чином, становить цілеспрямоване виробництво й поширення спеціальної інформації, яка безпосередньо впливає (позитивно або негативно) на функціонування й розвиток інформаційно-психологічного середовища суспільства, психіку й поведінку політичної еліти й населення конкретної країни.

Найважливішим поняттям, уведеним в одному зі звітів корпорації "RAND", є класифікація стратегічного інформаційного протиборства (фактично – інформаційних війн) на перше й друге покоління. Інформаційні війни першого покоління більше орієнтовані на дезорганізацію діяльності систем управління й проводиться скоріше як забезпечення дій традиційних сил і засобів ведення війни. Зокрема, під час війни в Панамі в 1989 р. уперше був апробований метод створення так званих журналістських пулів, який потім постійно використовувався військовим командуванням США. Зміст цього методу полягає в тому, що ще до початку бойових дій командування підбирає обмежений контингент (як правило, кілька десятків, рідше - сотень людей)

представників лояльно налаштованих і впливових ЗМІ, інструктує цих людей і направляє в район конфлікту. На першому етапі проведення воєнної операції практично вся інформація з району збройного конфлікту виходить тільки від цих журналістів. Потім поступово дозволяється присутність інших представників ЗМІ. Але журналісти, що не входять у пули, мають набагато менші можливості. Наприклад, у ході війни в Перській затоці в 1990-1991 рр. усі представники ЗМІ, які не входили в пули центрального командування Багатонаціональних Сил, не допускалися на передову. Таким чином, більшості журналістів, що бажали брати участь у висвітленні війни в Перській затоці, довелося залишитися в готелях Ер-Ріяда й Дархана й задовольнятися інформацією, що надавалася пулами в ході щоденних брифінгів. Однак і для журналістів, що входять у пули, "Правила діяльності ЗМІ" передбачали значні обмеження. Так, усі матеріали повинні були зазнавати попередньому перегляду з метою з'ясувати, не чи міститься там яка-небудь інформація, здатна "наразити на небезпеку американські або інші сили коаліції". Звичайно, крім роботи з журналістами, використовуються також інші засоби й методи інформаційної війни. Наприклад, розкидання з літаків над позиціями ворожих військ листівок, що призивають солдатів скласти зброю. Цей метод, як ми вже бачили, застосовується ще з часів Першої світової війни.

Інформаційні війни другого покоління у звіті визначені як "принципово новий тип стратегічного протиборства, викликаний до життя інформаційною революцією, що вводить у коло можливих сфер протиборства інформаційний простір і ряд інших областей (насамперед економіку) і триває довгий час: тижні, місяці й роки". Стратегічне інформаційне протиборство другого покоління є самостійним видом стратегічного протиборства, здатним (в ідеалі) дозволяти конфлікти без застосування збройної сили.

Таким чином, ведення інформаційної війни другого покоління передбачає вирішення в ході СІО наступних завдань:

- створення атмосфери бездуховності й аморальності, негативного відношення до культурної спадщини супротивника;

- маніпулювання суспільною свідомістю й політичною орієнтацією

соціальних груп населення країни з метою створення політичної напруженості й хаосу;

- дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції й навіть громадянської війни;

- зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;

- дезінформація населення стосовно роботи державних органів, підрив їхнього авторитету, дискредитація органів управління;

- провокування соціальних, політичних, національних і релігійних зіткнень;

- ініціювання страйків, масових заворушень, інших акцій економічного чи соціального протесту;

- ускладнення прийняття органами управління важливих рішень;

- підрив міжнародного авторитету держави, її співробітництва з іншими країнами;

- завдання збитків життєво важливим інтересам держави в політичній, економічній, оборонній й інших сферах.

Основні елементи інформаційних війн другого покоління активно використовувалися ще в ході "холодної війни" Сполученими Штатами проти СРСР. СІО, що здійснюються в ході інформаційної війни цього формату, передбачають, зокрема, використання так званих «вікон Овертона».

Так, запропонований співробітником «Mackinac center» Дж.Овертоном метод "переконання", що одержав назва "вікно Овертона", дозволяє втілити в життя будь-які ідеї й навіть закріпити їх законодавчо. Згідно із цим методом, у суспільстві є так зване "вікно можливостей" для будь-якої ідеї. У рамках такого "вікна", наприклад, певну ідею неможливо обговорювати або відкрито підтримувати. "Зрушивши" це "вікно", можна настільки змінити "віяло можливостей", що дана ідея, що раніше категорично відкидалася суспільством, у результаті послідовних і завуальованих СІО з'являється в повістці "актуальної

політики". А коли суспільство починає сприймати її як важливу проблему, цій ідеї можна вже додати й форму закону (за допомогою цього методу відбувається, наприклад, популяризація толерантного відношення до ЛГБТ-спільноти на пострадянському просторі).

Інформаційні війни третього покоління пов'язуються з розвитком так званої доктрини СІО, «що базуються на досягненні ефектів" (effects-based operations). Мета цього концепту - за допомогою СІО впливати на супротивника таким чином, аби він змінив свою поведінку в бажаному напрямку. У цьому контексті як окремий "ефект", так і їхня сукупність стає своєрідною інформаційно-психологічною зброєю [53]. Головна мета, яку забезпечує використання СІО, таким чином, це зміна поведінки інформаційних систем у потрібному для суб'єкта впливу напрямку. Зокрема, впливаючи на свідомість людей, досягають управління їх поведінкою, причому з'являється можливість маніпулювання свідомістю не тільки окремих людей, але й масового інформаційно-психологічного програмування населення. У зв'язку із цією обставиною, особливе значення набуває соціальна інформація, та, яка пов'язана з функціонуванням різного роду суспільних утворень і структур. Оскільки соціально-інформаційну технологію й ресурси можна використовувати не тільки як безсумнівні факти або об'єктивне знання, але й для досягнення політичних, економічних та інших переваг або тиску однієї держави, партії, соціальної групи, особистості тощо на інші, застосовуючи при цьому незаконні, а часом і аморальні методи. Інформація такого роду може викликати різного роду широкомасштабні акції протесту, у тому числі, екстремістські акції, терористичні акти тощо.

Наприклад, в ході збройних конфліктів концепція інформаційної війни третього покоління передбачає, що при плануванні й проведенні СІО слід ураховувати наступні фактори:

- проведені СІО повинні викликати такі ефекти, які забезпечують бажану для ініціатора операцій дію на поведінку супротивника, що є переважним за розгром його збройних сил.

- відповідні ефекти повинні впливати не тільки на військову, але й на

політичну, суспільну, економічну ситуацію й стан в інших сферах.

- відповідні ефекти повинні виявити вплив не тільки на супротивника, але й на союзників і нейтральні країни.

Отже, доктрина інформаційної війни третього покоління передбачає здійснення сукупності СІО, спрямованих на формування моделі поведінки супротивників, союзників і нейтральних сил в умовах миру, кризи й війни.

У концепції «ефект-орієнтованих» СІО знищення супротивника стає лише одним з інструментів досягнення мети війни - у фреймі більш широко здійснюваної політики примусу супротивника до певної лінії поведінки. Із цього погляду СІО потрібно сприймати скоріше як систему мислення, ніж нову форму війни, що припускає здатність оперувати категоріями національної безпеки й, отже, вимагає виходу за межі військової сфери. Дійсно, сьогодні підходи, пов'язані з «ефект-орієнтованими» СІО, почали застосовуватися практично у всіх сферах стратегічного планування. Це, у свою чергу, змусило говорити не тільки про концепцію й методології планування СІО, але й про мислення, що базується на досягненні ефектів і припускає наступні постулати:

- для досягнення оперативних і стратегічних результатів необхідно системно об'єднати всі кроки й дії (політичні, дипломатичні, економічні й військові тощо);

- необхідна безперервна оцінка вироблених ефектів і, за необхідності, адаптація планів і дій до складної бойової обстановки й реалій конфлікту;

- необхідне продумування й оцінка ефектів і їх наслідків у довгостроковій перспективі.

Таким чином, «ефект-орієнтованих» СІО за своїм змістом є аналітичною формою війни, що прагне не тільки планувати, здійснювати й оцінювати операції, але й передбачати процеси й можливі відповідні дії супротивника, а відтак – базується передусім на культурі прогнозування [52].

Як вже зазначалося вищу у попередніх підрозділах, наразі науковцями й практиками діагностовані й інформаційні війни четвертого покоління [222]. Мова йде про інформаційно-психологічні війни, у яких відсутні поняття фронту й тилу, а об'єктом впливу стає все населення країни і її державний апарат.

Кожна держава має унікальний культурний код (духовним, соціальним, психологічним, національною пам'яттю). Культурний код містить у собі цілісну історично сформовану систему установок населення й несвідому його реакцію на ситуацію, пов'язану з погрозою для країни й життя народу. Елементами культурного коду є культура й національні інтереси.

З позиції загальної теорії виділяють шість узагальнених стратегічних пріоритетів управління суспільством: світоглядний; хронологічний пріоритет; фактологічний пріоритет; економічний пріоритет; зброя геноциду; зброя знищення. Заявлені пріоритети дають підставу вважатися, що, впливаючи на них, країна-агресор може добитися поставлених цілей.

Сучасний інформаційно-психологічний вплив необхідно розглядати в рамках теорії й практики ведення війн четвертого покоління (the 4th Generation of Warfare), або стратегії 4GW - самостійного виду впливу на супротивника, спрямованого на позбавлення його волі до опору. Ціль стратегії 4GW - зламати культурний код і підкорити своїй волі передбачуваного супротивника.

Теорія й практика ведення війн четвертого покоління (стратегії 4GW) була реалізована Сполученими Штатами Америки у воєнних операціях в Іраку, Афганістані, Лівії тощо. Російська Федерація наразі намагається здійснювати відповідні СІО в Україні (проект «Руська весна») (Додаток Б).

Спробуємо позначити основні принципи стратегії 4GW:

- асиметричність конфлікту. В умовах трансформації сучасного суспільства під впливом процесів глобалізації учасниками конфлікту є транснаціональні корпорації й держави. Формально це виглядає як конфлікт між державами, оскільки вплив на супротивника здійснюється за допомогою "третьої сторони". Принцип асиметричності конфлікту полягає в застосуванні таких методів боротьби і технологій, які радикально перевершують можливості супротивника. Держава-агресор озброює, навчає й фінансує сили цього "агресивного недержавного суб'єкта", планує й забезпечує його підривні операції, виявляє їм політичну, інформаційну і юридичну підтримку;

- маневреність. У стратегії 4GW традиційна військова сила втрачає своє значення, бойовий потенціал держави перестає бути вирішальним фактором.

«Мішенню» та "полем бою" стає все суспільство супротивника з матеріальними й духовними цінностями, зникає поняття стратегічного тилу. Удару зазнають будь-які вразливі місця - це можуть бути критично важливі об'єкти, пам'ятники культурної спадщини, особи, здатні консолідувати суспільство тощо. Основний принцип - не силове руйнування держави, а моральний вплив на населення й керівництво країни;

- взаємодія мережевих співтовариств. Зони відповідальності військових керівників заміняються на окрему бойову одиницю інформаційних операцій з використанням глобальних ЗМІ. Формується багатопотокова система управління мережевого типу з декількома універсальними центрами прийняття рішень (у результаті вдало проведених СІО населення починає відкрито підтримувати супротивників свого уряду);

- «народна партизанська війна», або «війна без правил». СІО передбачають "аморфні", але добре скоординовані атаки з єдиною метою в різних напрямках. Поняття фронту відсутнє. Моральна перемога над супротивником досягається за допомогою нанесення ударів по його слабких сторонах;

- «керований хаос», або створення атмосфери повної невизначеності. Вплив спрямований на розколювання ідеологічної основи держави й витиснення її зі сфер, що потрапили під вплив супротивника;

- «спецефекти». Увага супротивника фокусується на економічних, політичних, культурних засадах безпеки держави-жертви за допомогою введення різноманітних санкцій, торговельних війн, застосування різних психологічних прийомів, спрямованих на "розгойдування" суспільства.

- «бойова зграя», тобто принцип роботи автономними або напівавтономними бойовими групами, пов'язаними з децентралізованою, нешаблонною тактикою в рамках втілення єдиної стратегічної мети;

- індивідуалізація відповідальності, або "перемога без управління". Величезне значення набуває індивідуальна підготовка сил СІО. У ситуації ліміту часу у відриві від управлінської ланки кожна окрема одиниця повинна бути здатна самостійно ухвалювати рішення, визначати головне.

Методом стратегії 4GW є концепція MISO (Military Information Support

Operations), що полягає в передачі потрібної інформації й орієнтирів іноземним аудиторіям задля справляння на них необхідного впливу з метою корегування поведінки «ключових гнізд» суспільства.

Оскільки метою боротьби є злам волі супротивника до опору, звідси випливає, що в стратегії 4GW лежать політичні, соціальні й моральні мотиви, спрямовані на зниження ролі впливу держави на суспільство.

Дослідники проблем сучасних інформаційних війн відзначають, що в процесі глобальної геополітичної інформаційної боротьби з метою захисту або руйнування матриць свідомості політичної еліти й населення країни використовують так звану інформаційно-психологічну зброю, до складу якої входять концептуально-методологічна, хронологічна (історична), фактологічна та лінгвістична зброя [190]. Концептуально-методологічна зброя як засіб інформаційного впливу містить у собі світоглядну й методологічну складову, що дозволяє виділити загальний і частковий хід подій. На базі цієї інформації формуються: світоглядна картина людини, її ціннісна свідомість і методологічна культура; визначаються напрямки розвитку й стратегія захисту базових цінностей суспільства (безпека, добробут, справедливість тощо). Сформована в такий спосіб парадигма мислення є методологічною основою функціонування парадигми діяльності. Конструктивне застосування цього виду зброї спрямоване на формування критичного мислення людини, що значно знижує ймовірність перетворення останньої на жертву "маніпулятивних" війн. Результатами ж деструктивного застосування цієї зброї є: світоглядний хаос, некритичність мислення й диктат забобонів, що дозволяє здійснювати екзистенціальне маніпулювання суспільною свідомістю; комплекс неповноцінності в народу або навіть психологія раба; громадянський інфантилізм; деспотизм "картезіанського" розуму; концептуальна залежність і гіпостазування еліти; украй низький рівень або навіть відсутність правової і стратегічної культури. У хронологічній (історичній) зброї засобом впливу на суспільну свідомість є зміна інформації хронологічного порядку проходження фактів і явищ, їх взаємозв'язків. За умови володіння відповідною методологією ця зброя дозволяє розглядати явище як включення в глобальний історичний

процес і точно визначити вектор національної політики. Саме фундаментальні знання про історичну реальність - знання законів, протиріч, тенденцій, рушійних сил суспільного розвитку й визначення його перспектив шляхом наукового передбачення – забезпечує можливість застосування історичної зброї для цілеспрямованого впливу на формування історичної свідомості суспільства. За змістом цей вплив охоплює такі взаємозалежні поняття, як історична пам'ять, історичні традиції, уроки минулого, історичний досвід тощо. Основу формування історичної свідомості становить цілепокладання, адже мета як закон визначає спосіб і характер відповідних операцій, спрямованих на створення свідомості певного типу, визначає вибір необхідних для цього засобів. Конструктивне застосування історичної зброї спрямоване на формування історичної свідомості народу, що є запорукою його самоідентифікації на тлі історичної наступності й розвитку національної ідеології. Результатом деструктивного застосування цієї зброї, або так званих "історичних" війн, є інформаційна моральна ліквідація всіх національних і видатних людей, знищення історичної пам'яті, історичних традицій народу і його відомість до категорії неісторичної. Фактологічна зброя - це інформація прикладного характеру: релігія, ідеологія, політичні міфи, виборчі технології, технології маніпуляції свідомістю засобами масової інформації. Конструктивне застосування цієї зброї спрямоване на консолідацію нації, деструктивне - на розкол нації й підрив історичних основ духовної цілісності народу, його дезорієнтацію й дезорганізацію. В обох випадках передбачається можливість використання, як просторової, так і тимчасової парадигми формування так званого ідеологічного поля нації. Необхідно також зауважити, що віра як основа будь-якої релігії утворює найбільш сильне ідеологічне поле порівняно з іншими ідеологіями. При цьому досить небезпечною є зміна ідеологічного поля протягом трьох - чотирьох поколінь, оскільки, з погляду масової психології, це приводить до психомутації, що характеризується масовою втратою віри, світоглядним хаосом і хаотичним рухом у соціальній сфері. Усе зазначене призводить до проникнення в сферу суспільної свідомості вірусу тоталітарного сектантства різного характеру. Лінгвістична зброя являє собою засіб впливу за

допомогою мови. Остання є одночасно засобом спілкування та контролю, оскільки мовна форма дозволяє передавати інформацію й спростовувати її. Мовний фактор також впливає на зміну освітніх моделей. Якщо в аграрній і індустріальній цивілізації освіта виступала, переважно, транслятором знань, традицій культури, то в інформаційній цивілізації вона стає своєрідним посередником у придбанні знань, тобто мова є засобом не тільки передачі готових знань, але й навчанням здобувати, знаходити й застосовувати їх. Інформаційно-психологічна зброя застосовується з метою руйнування тонких структур суспільства (мораль, традиції) і формування інформаційного колоніалізму активною стороною, і може бути застосована як самостійно, так і в складі так званої організаційної зброї, яка є зброєю другого пріоритету. Таким чином, проведення СІО психологічної спрямованості припускає маніпуляції, які зводяться до виправданих і невиправданих підмін знаків і значень, іміджеву маніпулятивну гру значеннєвими полями. Наприклад, мова може йти про проведення СІО для штучного підвищення рівня ентропії регіону, з метою створення умов так званої "керованої нестабільності"[103].

Стратегія 4GW припускає широкий набір технологій, які утворюють тактики MISO, спрямовані на виснаження військових і фінансових ресурсів країни-супротивника в ході постійно триваючої «партизанської війни» та терористичної діяльності. Таких тактик декілька: тактика "юридичної війни" як одна з форм асиметричного конфлікту (незаконне застосування норм внутрішнього й міжнародного права з метою завдання збитків опонентові); тактика економічних і політичних санкцій (всі форми тиску на жертву, зокрема, організація демонстрацій, пікетів, мітингів і кампанії ненасильницької непокори із застосуванням політико-економічних технологій); тактика терору або "військового компонента" (організація повстанських рухів і терористичних дій різного характеру в країні - об'єкті впливу. Завдання - підірвати бойовий дух народу й армії, викликати сум'яття й спровокувати паніку); тактика руйнування традиційних сімейних цінностей, або "цивільний" компонент (сюди входять технології, спрямовані на роз'єднання суспільства, руйнування традиційної громади й родини. MISO формує цілеспрямовані агресивні атаки на традиційні

культурно-історичні цінності населення); тактика "високошвидкісних операцій" (MISO проводить витончену й високотехнологічну психологічну війну, що полягає в маніпулюванні засобами масової інформації з метою формування глобальної суспільної думки на конкретні події).

Отже, інформаційна війна четвертого покоління являє собою інформаційно-психологічну війну або політико-психологічний процес, який спрямований на зміну відносини масової свідомості населення умовного супротивника до, що сформувалися на території цієї держави цінностям, національним інтересам. Це здійснюється шляхом підриву унікального культурного коду даного народу, впливу на його стратегічну культуру з метою руйнування впевненості в правоті власних ідей та їх здійсненності. Кінцева мета інформаційно-психологічної війни - викликати невдоволення й деструктивні дії в масовій свідомості відносно опонентів. Це масові виступи для повалення політичної режиму, порушення інтересу до соціально-політичних конструкцій альтернативного характеру. Інформаційно-психологічна війна впливає на несвідомі, ірраціональні стани людей, на їхні емоції, почуття, інстинкти, забобони, упередження, міфологічні конструкції населення потенційного супротивника. Відбувається перенесення спрямованості боротьби з однієї сфери в іншу, на рівень повсякденної, повсякденної психології. Це досягається за рахунок масованого впровадження у свідомість людей безлічі неправильних стереотипів сприйняття й мислення, перекручених вистав про пануючих у їхнім середовищі поглядах, а також на події, що відбуваються у світі.

В ході сучасної інформаційної війни СІО обох типів – як інформаційно-технічного, так і інформаційно-психологічного, - а так само комплексні СІО можуть проводитися з метою оперативної або стратегічного маскування конфліктуючими сторонами своїх реальних військових, геополітичних, політичних, економічних задумів, завдань і намірів, а також з метою дискредитації дій імовірного супротивника, його державної політики, економічних структур тощо. При цьому СІО можуть бути проведені на оперативно-тактичному, стратегічному й глобальному рівнях.

СІО оперативно-тактичного рівня зазвичай має локальний вузько спрямований разовий характер й проводиться вибірково. «Ударна сила» таких СІО спрямовується на реперні точки ймовірного супротивника на невеликій ділянці інформаційного простору. Зокрема, операція може плануватися й проводитися з метою дискредитації правлячої політичної еліти, опозиції, конкретних посадових осіб, локалізації деструктивних ЗМІ, компрометації суб'єктів господарювання або бізнес-проектів тощо. Стратегічний рівень проведення СІО вимагає застосування нетрадиційних форм і методів широкомасштабного інформаційного впливу на груповий об'єкт атаки. В операції можуть бути задіяні агенти, резиденти, розробники і їх інформаційно-ударні комплекси, розташовані на території ймовірного супротивника. Операція може проводитися на території декількох держав одночасно, протягом значного проміжку часу. Планування й реалізація СІО на глобальному рівні є вкрай складним і багаторівневим завданням. У нетрадиційній ударній комбінації цілеспрямованого інформаційного впливу необхідно задіяти всіх основних світових геополітичних суб'єктів, за діяння яких є доцільним в інтересах конкретної держави. З метою реалізації СІО також доцільно задіяти всі інформаційні ресурси держави, а так само сили й засоби інформаційного протиборства системи національної безпеки.

В цілому матеріали узагальнення досвіду збройних конфліктів останніх десятиліть дозволяють вести мову про систему багаторівневих СІО, у яких значна роль приділяється існуючим, а також перспективним силам і засобам радіоелектронної боротьби. Так, на етапі зародження збройного конфлікту тактичного рівня, який, на думку більшості експертів, буде основним способом вирішення міжрегіональних протиріч у найближчі 15-20 років, першою в системі спеціальних інформаційних операцій слід вважати СІО державного масштабу. При проведенні СІО державного масштабу головні зусилля будуть зосереджуватися на міждержавному рівні й зводитися в основному до дипломатичних і економічних заходів і способів впливу, відтак застосування сил і засобів радіоелектронної боротьби на даному етапі конфлікту не буде, як правило, виходити за рамки заходів і дій, обумовлених керівними документами,

що регламентують повсякденну діяльність сектору безпеки і оборони країни [198]. У разі поглиблення конфлікту, його перехід до етапу загострення напруженості й активної підготовки держав-супротивників до воєнних дій зміст і спрямування боротьби в інформаційній сфері може значно розширитися й привести до необхідності проведення нового виду СІО - на військовому рівні. Досягнення мети даної операції буде здійснюватися переважно в "інтелектуальний спосіб", сутність якого полягає в митецькому застосуванні в першу чергу демонстраційних дій, впровадженні дезінформації в підсистеми добування й збору інформації супротивника, щоб створити в нього неправильне уявлення про обстановку в районі конфлікту. У такий СІО сили й засоби радіоелектронної боротьби можуть залучатися головним чином за планом здійснення оперативного маскування. У цей час і тим більше в перспективі обов'язковою й невід'ємною частиною заключного етапу кризи (попереднього етапу початку активних військових (бойових) дій) стає наступний вид СІО, який зорганізується проводиться на фронтовому рівні, супроводжуючи фактичні бойові дії. Основними цілями цього виду СІО можуть бути примус супротивника до відмови від загострення конфлікту до військової фази або завоювання й утримання інформаційної переваги над ним до початку активних бойових дій [100].

За експертними оцінками, гібридна агресія РФ відносно України є різнорівневою комбінацією диференційованих форм і методів негативного впливу, серед яких домінуючим напрямком є інформаційний і кібернетичний. Важливим аспектом негативних СІО, які намагаються здійснювати російські спецслужби, є їх спрямованість на руйнування української державності починаючи з базового рівня - історичної пам'яті й самосвідомості нації як такої. Із цією метою російськими спецслужбами використовуються підконтрольні їм ЗМІ, інтернет-ресурси, групи у соціальних мережах, блогери, інтернет-тролі та навіть поштові сервіси. З використанням цієї розгалуженої мережі не тільки збирається розвідувальна інформація про українських громадян, але й проводяться деструктивні пропагандистські СІО. Ще одним напрямком гібридної війни є виснаження фінансових і матеріальних ресурсів України,

створення передумов до втрати нею енергетичної незалежності, ослаблення транзитного потенціалу й дискредитація нашої держави на міжнародній арені з наступною реалізацією СІО. Деструктивний інформаційний вплив і маніпулювання суспільною свідомістю спецслужби РФ поєднують з проведенням цинічних за задумом і катастрофічних за наслідками кібератак на об'єкти критичної інфраструктури [121]. Якщо звернутися до кількісних показників, за експертними оцінками лише за період з 2014 до 2018 року проти України проведено понад 30 комплексних багатоепізодних СІО [109].

Досліджуючи проблематику використання СІО в ході інформаційних війн також слід звернути увагу й на те, що в сучасних умовах виділяють дві складові інформаційної війни: наступальну й оборонну. Наступальна інформаційна війна припускає використання ініціатором інформаційної війни різноманітних засобів і методів впливу на інформаційні системи супротивника з метою зниження ефективності функціонування його системи прийняття рішень. Оборонна ж інформаційна війна передбачає проведення СІО з використанням засобів і методів протидії ефективному застосуванню інформаційної зброї супротивником [247].

Класичним прикладом використання СІО в оборонній інформаційній війні, тобто, як засобу забезпечення національної безпеки, можуть вважатися антитерористичні СІО. Важливою складовою антитерористичних СІО є інформаційно-психологічний вплив не тільки на терористів, але й на цивільне населення, у тому числі на суспільну думку як у власній, так і у закордонних країнах. Це обумовлене тим, що антитерористичні СІО: викликають, як правило, більший суспільний резонанс, ніж СІО, проведені збройними силами під час воєнних дій; можуть мати явних супротивників в особі політиків, правозахисників і журналістів, у тому числі й заангажованих; при оцінці різними державами майже завжди використовується подвійний стандарт, залежно від політичної кон'юнктури й власної вигоди.

Як показує досвід, строки завершення антитерористичних СІО можуть бути значно розтягнуті за часом, що, безсумнівно, вимагає значних зусиль в інформаційній сфері: по-перше, щоб знизити негативний психологічний ефект

і соціальні наслідки серед населення й особливо його політично активної частини; по-друге, щоб підготувати відповідну інформаційну й психологічну обстановку, сприятливу для безкровного вирішення ситуації або перехід до активної (силовий) фазі операції по знешкодженню терористів.

У ході антитерористичних СІО використовуються наступні заходи: вплив на певні групи людей і окремих осіб, щоб викликати в них такий настрій і поведінку, яка сприяла б досягненню цілей боротьби з тероризмом; деморалізація бойовиків, дискредитація терористичних організацій і терористичних методів в очах суспільства й у формуванні в населення доброзичливого ставлення до антитерористичної політики держави; забезпечення безпеки громадян (зокрема інформаційно-психологічної) тощо.

СІО антитерористичного характеру поділяються на: превентивні, розраховані на запобігання масових проявів будь-яких форм тероризму; операції на підтримку (для забезпечення) спеціальних операцій щодо боротьбі з терористами й тероризмом; операції з використання у сфері інформації й комунікації результатів дій антитерористичних підрозділів (як успішних, так і невдалих); операції прикриття. У превентивних СІО може ефективно використовуватися вітчизняний і закордонний досвід уже проведених операцій і акцій (позитивний і негативний) і висновки з аналізу психологічних наслідків терористичних акцій і заходів щодо знешкодження терористів.

Деякі СІО, що називають в ЗМІ «акціями залякування», представляються спірними з погляду міжнародного права й викликають неприйняття в частини політиків, правознавців і преси. Однак досвід показує, що використання залякування може бути виправдане з погляду ефективності впливу на психіку терористів, які, у більшості випадків, розраховують на безкарність і власну невразливість. Тож такі СІО виступають невід'ємним "силовим елементом" антитерористичної політики багатьох держав. У свою чергу, їх результати широко використовуються в психологічній боротьбі проти тероризму як явища.

2.2. Організаційно-правові засади проведення спеціальних інформаційних операцій.

Теоретичні дискусії з питань інформаційної безпеки та інформаційної війни, в тому числі щодо проведення СІО, переважно звертають увагу на технологічні проблеми, втім лишають поза увагою правове середовище, у якому відбуваються суспільні зміни, пов'язані з розвитком інформаційних технологій. Це може привести до прогалин та колізій у неврегульованих правових питаннях, які повинні бути вирішені в ході розв’язання проблем забезпечення інформаційної безпеки та розвитку інформаційного права в Україні. Зокрема, як зазначає О.Баранов, «Використання мережі Інтернет та інтернет-технологій може обумовити появу особливостей в реалізації звичайних суспільних відносин. Саме ці особливості … можуть стати причиною необхідності певного вдосконалення традиційного правового регулювання або, навіть, причиною появи нових правових норм в межах традиційної системи правового регулювання» [55]. Зауважимо, що правове регулювання використання мережі Інтернет – це лише один з напрамків розвитку інформаційного права та законодавства, в тому числі в частині правової регламентації проведення СІО.

Отже, розпочинаючи дослідження організаційно-правових засад проведення СІО, передусім слід звернути увагу на те, що правове підґрунтя проведення СІО може бути окреслено наступними напрямками:

- нормативно-правові акти, що визначають обмеження і заборони при проведенні СІО (до цієї групи належать міжнародно-правові акти з питань протидії інформаційним загрозам, забезпечення інформаційної безпеки й регулювання інформаційного протиборства, а також акти національного інформаційного законодавства, присвячені регламентації інформаційних правовідносин та інформаційної сфери);
- нормативно-правові акти, що регламентують порядок і процес проведення СІО (до цієї групи належать національні нормативно-правові акти відомчого характеру, які переважно мають закритий характер).

Як уже зазначалося у попередньому розділі цього дослідження,

найнебезпечнішою загрозою інформаційній безпеці, зокрема й на міжнародному рівні, наразі виступає інформаційна війна, причому СІО одночасно можуть використовуватись як інструмент ведення інформаційної війни, так і інструмент забезпечення інформаційної безпеки. Наразі інформаційні відносини не просто достатньо розвинені – вони набувають характеру визначальних, багато в чому опосередковуючи інші суспільні відносини, тож загрози інформаційній безпеці, особливо коли мова йде про індустріально-розвинені країни, сьогодні досить реальні. Відсутність міжнародно-правового регулювання у питаннях інформаційної безпеки та інформаційного протиборства може дати можливість деяким державам здійснювати напади в рамках інформаційної війни, уникаючи відповідальності за зазначені дії [7]. Тож забезпечення інформаційної безпеки й заборона ведення інформаційних війн - це та сфера, де міжнародно-правове регулювання необхідне вже сьогодні.

Розвиток концепції інформаційних війн актуалізує низку міжнародно-правових питань, які передусім стосуються тих дій у рамках інформаційних війн, у яких використовуються комп'ютери, телекомунікації або інформаційні комунікаційні мережі. Деякі правові обмеження, передбачені чинним міжнародним правом, можуть застосовуватися до інформаційних війн, оскільки ці обмеження регулюють певні дії, здійснювані в рамках інформаційних війн, або внаслідок того, що до таких дій можуть бути застосовані загальні принципи міжнародного права. Проте, новітній характер певних засобів ведення інформаційних війн може вивести застосування цих засобів зі сфери міжнародно-правового регулювання. Таким чином, можна сформулювати основні проблеми міжнародно-правового регулювання у сфері інформаційного протиборства:

- можливість передачі сигналів через міжнародні мережі, а також можливість впливу на системи у певних країнах з використанням інформаційних мереж третіх країн торкається принципу державного суверенітету.

- наразі відсутнє чітке розуміння того, чи становлять інформаційні напади в ході інформаційної війни застосування сили, або вторгнення на територію держави, втручання у внутрішні справи держави або збройний напад, адже вирішення цього питання може залежати від наслідків, які спричинили ці напади.

Тож лишається невизначеним, чи вважатися правомірним для держави, яка потерпає від нападу в рамках інформаційної війни, почати дії у відповідь, і чи мають ці дії також ознаки прояву інформаційної війни, або ж можна використовувати інші засоби силової відповіді;

- лишається відкритим питання, чи можна застосовувати до дій у рамках інформаційної війни положення гуманітарного міжнародного права в період збройних конфліктів, і якщо так, те чи є збиток, що може бути завданий в ході інформаційної війни, збитком, який забороняється міжнародним гуманітарним правом;

- у випадку якщо напади здійснюються через міжнародні мережі, державі може знадобитися допомога інших держав у визначенні джерела нападу. У цьому випадку зачіпаються питання юрисдикції, правової допомоги й міжнародної відповідальності держав.

Дійсно, як вже зазначалося, використання, наприклад, таких засобів, як комп'ютерне вторгнення й комп'ютерних вірусів, переносить війну з фізичного, кінетичного світу до нематеріального інформаційного простору, породжуючи нові форми конфліктів. Напади можуть здійснюватися на відстані, з використанням радіохвиль або міжнародних комунікаційних мереж, без фізичного порушення кордонів держави. Збитки внаслідок інформаційної війни можуть варіюватися від заподіяння смерті військовим або цивільним особам, системних збоїв, припинення виконання функцій об’єктами критичної інфраструктури, поширення паніки, економічної кризи тощо [10, 17].

Розвиток інформаційних технологій як уможливлює для супротивників атаку у новий спосіб і з використанням нових форм заподіяння збитків, так і провокує виникнення нових цілей для нападу. Це становить досить суттєву проблему в оцінці правомірності СІО. Це обумовлене тим, що розвиток інформаційних технологій характеризується так званим явищем конвергенції, яке можна визначити як зближення або злиття якихось, до певного моменту різних структур, систем або об'єктів. Для проведення СІО у рамках інформаційних війн, велике значення має конвергенція цивільних і військових систем, адже інфраструктури держави, що забезпечують безпеку, у тому числі військові

системи, усе більше використовують технології цивільного призначення, а також об'єкти й комунікаційні мережі, які виконують, у тому числі й функції, необхідні для діяльності громадянського суспільства. Таким чином, подвійне призначення багатьох інформаційних систем і інфраструктур може розмити відмінність між військовими й цивільними цілями. Це приводить до того, що в рамках інформаційної війни важко визначити цілі нападів як суто військові (і, отже, легітимні) або суто цивільні (напад на які заборонено). Крім того, вид нематеріального збитку, який такі напади можуть спричинити, може суттєво відрізнятися від фізичних руйнувань внаслідок традиційної війни. Порушення роботи інформаційних систем, включаючи викривлення даних або маніпуляцію ними, може спричинити нематеріальний збиток у вигляді порушення функціонування громадянського суспільства й держави.

Наразі у міжнародному праві відсутні норми, які однозначно забороняють або у певний спосіб регламентують проведення СІО в ході інформаційної війни. Водночас, відсутність норми не є дозволом до дії, відтак в даному випадку можуть застосовуватися загальні принципи міжнародного права [19]. Зокрема, вирішення міжнародним правом питання, чи становлять інформаційні напади в рамках інформаційної війни застосування сили, або вторгнення на територію держави, втручання у внутрішні справи держави або збройний напад, залежить від наслідків, які спричинили ці напади.

Збройний напад, у традиційному розумінні цього терміну, обов'язково передбачає застосування збройних сил, військового примусу й насильства. Для визначення поняття збройного нападу необхідно звернутися до Статуту ООН [237], а також до міжнародно-правових документів, прийнятих у рамках ООН у цій сфері. Так, у статті 2(4) Статуту ООН міститься один з основних принципів міжнародного права, відповідно до якого забороняється застосування сили або погрози силою до територіальної цілісності або політичної незалежності іншої держави. З моменту прийняття Статуту ООН, зазначений принцип застосовувався тільки до фізичного застосування сили. Під час розробки Статуту ООН, коли Бразилія запропонувала включити економічні заходи впливу у поняття використання сили, ця пропозиція була відхилена. Натомість у період Арабського

нафтового ембарго 1973 року багато держав висловлювали сумнів у тому, що застосування сили передбачає економічного примусу, втім США наполягали на тому, що положення Статуту ООН не поширюються на економічний примус [12].

У Резолюції Генеральної Асамблеї ООН 3314 (XXIX) "Визначення агресії", прийнятої 14 грудня 1974 року, агресія визначається як застосування збройної сили державою проти суверенітету, територіальної недоторканності або політичної незалежності іншої держави, або у будь-який інший спосіб, несумісним зі Статутом ООН. У статті 3 цієї Резолюції зазначено, що не є вичерпним перелік дій, що становлять агресію. Зокрема, згідно зі статтею 4 Резолюції, Рада Безпеки може визначити, що інші акти становлять собою агресію, згідно з положеннями Статуту ООН [165, с.3-5].

Зауважимо, що відповідно до практики ООН, агресія обмежується застосуванням збройних сил. В 1953 році Іран виступив в ООН з ініціативою про визнання того, що будь-яка дія, що безумовно слугує цілям збройного нападу або примус, що піддає небезпеці незалежність держави, є агресією, але ООН не прийняла цю точку зору. При цьому, якщо відповідно до документів ООН не є можливим однозначно відповістити на питання, чи є напад у рамках інформаційної війни збройним нападом або агресією, то зовсім інша ситуація складається з питанням про інформаційний вплив як втручанні у внутрішні справи держави.

Відповідно до Декларації про принципи міжнародного права, що стосуються дружніх відносин і співробітництва між державами відповідно до Статуту ООН [91] (прийнято 24 жовтня 1970 року Резолюцією 2625 (XXV) Генеральної Асамблеї ООН) жодна держава або група держав не має права втручатися прямо або опосередковано з будь-якої причини у внутрішні й зовнішні справи будь-якої іншої держави. Також жодна держава не повинна застосовувати чи заохочувати застосування економічних, політичних заходів або заходів будь-якого іншого характеру з метою підпорядкувати собі іншу державу у здійсненні нею своїх суверенних прав і одержання від цього будь-яких переваг [12]. Аналогічні положення можна виявити й у Декларації ООН про неприпустимість втручання у внутрішні справи держав, про захист їх

незалежності та суверенітету [90] (прийнято 21 грудня 1965 року Резолюцією 2131 (XX) на 20-й сесії Генеральної Асамблеї ООН): «Жодна держава не має права втручатися прямо або опосередковано з будь-яких підстав у внутрішні й зовнішні справи іншої держави. Внаслідок цього засуджуються не тільки збройне втручання, але також усі інші форми втручання й усякі погрози, спрямовані проти правосуб'єктності держави або проти її політичних, економічних і культурних елементів». Незважаючи на те, що ні в Декларації принципів міжнародного права, ні в Декларації про неприпустимість втручання не дається чіткого поняття втручання у внутрішні справи держав, у зазначених документах позначені заходи, що становлять таке втручання, причому перелік цих заходів не є вичерпним. Отже, інформаційний вплив в ході інформаційних війн, в тому числі у формі СІО, може розглядатися як втручання у внутрішні справи держави.

Вкрай важливе значення для вирішення питань інформаційної безпеки має Декларація про неприпустимість інтервенції й втручання у внутрішні справи держав (прийнято 09 грудня 1981 року Резолюцією 36/103 на 36-ой сесії Генеральної Асамблеї ООН) [89]. Відповідно до цієї декларації, принцип відмови від інтервенції й невтручання у внутрішні й зовнішні справи держав передбачає наступне:

- право держав і народів мати вільний доступ до інформації й повністю розбудовувати без втручання свою систему інформації й ЗМІ й використовувати власні засоби інформації з метою сприяння своїм політичним, соціальним, економічним і культурним інтересами й сподіванням;
- обов'язок держав утримуватися від будь-яких наклепницьких кампаній, образливої або ворожої пропаганди з метою здійснення інтервенції або втручання у внутрішні справи інших держав;
- право й обов'язок держав боротися, у рамках своїх конституційних повноважень, проти поширення неправдивих або перекручених повідомлень, які можуть розглядатися як втручання у внутрішні справи інших держав або які завдають збитків зміцненню миру, співробітництва й дружніх відносин між державами й націями.

Таким чином, відповідно до зазначеної декларації, деякі форми поширення

неправдивих або перекручених повідомлень можуть розглядатися як втручання у внутрішні справи держави, припускаючи, таким чином, певні заходи відповідальності держави порушника.

Окремі питання в сфері інформаційної безпеки торкаються положення таких галузей міжнародного права, як міжнародне право електрозв'язку, космічне право, міжнародне право в період збройних конфліктів.

Зокрема, будь-яка діяльність із використанням мереж і телекомунікацій, у тому числі діяльності в рамках інформаційної війни, може підпадати під дію Статуту Міжнародного союзу електрозв'язку [202], який застосовується до міжнародного радіозв'язку й до дротового електрозв'язку. Зазначений Статут й адміністративні регламенти, прийняті на його виконання, можуть застосовуватися до СІО, при здійсненні яких використовується електромагнітний спектр або міжнародні телекомунікаційні мережі. По-перше, відповідно до положень Статуту, усі станції, незалежно від їхнього призначення, повинні встановлюватися й експлуатуватися таким чином, щоб не заподіювати шкідливих перешкод радіозв'язку або радіослужбам інших членів Союзу електрозв'язку або визнаних експлуатаційних організацій і інших правочинних експлуатаційних організацій, які мають право здійснювати радіозв'язок і працюють відповідно до положень Регламенту радіозв'язку. Радіорегламентний комітет Міжнародного союзу електрозв'язку розподіляє електромагнітний спектр для запобігання створення перешкод. При цьому військові установки повинні дотримуватися вимог неспричинення шкідливих перешкод радіозв'язку, а радіостанції, що перебувають у відкритому морі, заборонені, відтак держави не можуть здійснювати передачу неправильних сигналів або сигналів, що вводять в оману. Нарешті, уряди повинні захищати безпеку міжнародної кореспонденції, хоча вони залишають за собою право зупинити радіопередачі або передачі іншими каналами електрозв'язку з міркувань національної безпеки. Втім, правила щодо нестворення перешкод радіомовленню й електрозв'язку не застосовуються в разі збройного конфлікту.

Через важливість супутників для міжнародних телекомунікацій, а також для військових комунікацій і розвідувальних дій, багато нападів в ході інформаційної війни можуть використовувати штучні супутники Землі. Отже, така діяльність

підпадає під дію норм міжнародного космічного права.

Основний документ космічного права - багатосторонній Договір 1967 року про принципи діяльності держав з дослідження й використання космічного простору, включаючи Місяць та інші небесні тіла (Договір щодо космосу) [98], передбачає, що всі держави вільні й рівні в дослідженні й використанні космосу, й держави-учасниці Договори зобов'язуються не виводити на орбіту навколо Землі будь-які об'єкти з ядерною зброєю або будь-якими іншими видами зброї масового знищення, не встановлювати таку зброю на небесних тілах і не розміщати її у космічному просторі у будь-який інший спосіб. Аналогічні зобов’язання містить Угода 1979 року щодо діяльності держав на Місяці й інших небесних тілах (Договір про Місяць) [236]. Відповідно до Конвенції 1976 року про Міжнародну організацію морського супутникового зв'язку (INMARSAT) [129], організація здійснює свою діяльність винятково в мирних цілях. Угода 1971 року про Міжнародну організацію супутникового зв'язку (EUTELSAT) також торкається телекомунікацій і використання космосу, але їх відношення до інформаційної війни обмежується принципами недискримінації відносно держав, що використовують відповідні супутники[132]. На думку західних вчених, зокрема, Р.Олдрича, жодна із зазначених конвенцій безпосередньо не забороняє дії в рамках інформаційної війни, для здійснення яких використовуються супутники, адже термін "мирне використання" тотожний до "неагресивне використання", в т.ч. й військового [7, 40].

Концепція міжнародного гуманітарного права заснована основана на тріаді гуманність - бойова необхідність - домірність". Основними принципами міжнародного гуманітарного права є: гуманізація збройних конфліктів; обмеження воюючих у виборі методів і засобів ведення війни; міжнародно-правовий захист жертв війни; охорона цивільних об'єктів і культурних цінностей; захист інтересів нейтральних держав. Основними джерелами міжнародного гуманітарного права вважаються такі акти, як Гаазька конвенція про закони й звичаї сухопутної війни [48]; Женевська конвенція про захист цивільного населення під час війни [105]; Женевська конвенція про поводження з військовополоненими [106]; Конвенція про поліпшення долі поранених і

хворих у діючих арміях [130], Конвенція про поліпшення долі поранених, хворих та осіб, які зазнали корабельної аварії, зі складу збройних сил на морі [131]; Додаткові протоколи I, II 1977 року до Женевських конвенцій 1949 року; Гаазька конвенція про захист культурних цінностей у випадку збройного конфлікту [71]; Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію і Протоколи I, II, III до неї [127] тощо.

Одним з фундаментальних принципів міжнародного гуманітарного права є те, що законні методи заподіяння шкоди супротивникові не є необмеженими, а жорстокість війни повинна мати межі. Цивільні особи самі по собі не можуть бути об'єктом нападу, адже напад можливий тільки на військові об'єкти (ті, які за своєю природою, місцем розташування, призначенням або використанням можуть принести значну допомогу у воєнних діях і повне або часткове руйнування, захоплення або нейтралізація яких у поточних обставинах надасть певну військову перевагу). При здійсненні нападу також слід брати до уваги пропорційність між збитком цивільному населенню й очікуваним військовим ефектом. На думку західних учених, наразі важко дати відповідь, чи становлять порушення міжнародного гуманітарного права напади, що не тягнуть за собою тотальних руйнувань об’єктів матеріального світу, а спричинюють як порушення функціонування фінансової системи, системи соціального страхування або розкриття конфіденційної персональної інформації [7]. Також вважається, що подвійне використання багатьох телекомунікаційних мереж і устаткування ускладнює питання застосування міжнародного гуманітарного права як запобіжника інформаційної війни. Подвійна природа приводить до розмивання відмінностей між військовими й цивільними системами, а, отже, між військовими цілями й цілями цивільними, напад на які заборонений [30, с.41].

Сучасні технічні засоби уможливлюють здійснювати маніпулювання свідомістю населення та політичних лідерів держави-супротивника, зокрема, шляхом надання недостовірних розвідувальних відомостей, втручання в урядові комунікації, поширення фейкових новин. Не зважаючи на те, що подібні дії в

цілому не розглядаються як порушення міжнародного гуманітарного права, розцінюючись як «воєнна хитрість» [30, с.44-45]. Втім в окремих випадках маніпулювання новинами або даними розвідки може розглядатися навіть як прояв геноциду або інших жорстоких злочинів. Так, Р.Шафранські зазначає, що маніпулювання свідомістю населення держави-супротивника настільки , що її громадяни й лідери стають відірваними від реальності, особливо коли ефекти цього не можуть бути передбачені або піддані контролю, може бути не менш протиправним, ніж доведення націй до голодної смерті [39], зокрема, вважається, що радіопередачі слугували розпаленню геноциду в Руанді та колишній Югославії.

Слід зауважити, що відповідно до договірного, а також звичаєвого права територія нейтральних держав не повинна порушуватися збройними силами воюючих сторін. Вочевидь, у випадку здійснення СІО через мережу, яка перетинає нейтральну територію, або з використанням супутників або комп'ютерів нейтральної держави або її мереж, може порушуватися недоторканість території нейтральної держави. І хоча нейтральні держави не повинні дозволяти кожній з воюючих сторін переміщення військ через їхню територію, або зведення військових радіостанцій на своїй території, вони не мають подібних зобов'язань відносно використання воюючими сторонами їх загальнодоступних комунікаційних пристроїв і мереж [220].

Отже, питання допустимості СІО з правової точки зору передусім пов’язане з проблемою класифікації дій у рамках інформаційної війни. При цьому теоретичні ускладнення класифікації проявів інформаційної війни як застосування сили, війни, або агресії у міжнародному праві не означає, що міжнародно-правові інститути не в змозі дати оцінку таким проявам. Наприклад, Глава 7 Статуту ООН надає Раді Безпеки ООН повноваження визначати існування будь-якої загрози миру, будь-якого порушення миру або акту агресії й робити рекомендації або вирішувати, які заходи слід розпочати відповідно до ст. 41- 42 Статуту для підтримки або відновлення міжнародного миру й безпеки. Таким чином, міжнародне право має механізм визначення загрози миру або акту агресії [8].

Для того щоб дії у відповідь на напади в рамках інформаційної війни, зокрема СІО, були правомірними, необхідно:

- визначення того, що, наприклад, збої в інформаційних або комунікаційних мережах є результатом саме нападу в рамках інформаційної війни, а не ненавмисних помилок або технічних проблем;

- встановлення джерела мережних нападів і проблема територіальної юрисдикції, аби дії у відповідь були спрямовані саме на того суб'єкта, який здійснив напад. Оскільки відповідно до принципу суверенітету кожна держава має виняткові повноваження щодо подій в межах своїх державних кордонів, для встановлення джерела нападу необхідний співробітництво з іноземними державами [22]. В даному випадку протиріччя між міжнародним характером інформаційних і комунікаційних мереж і державним суверенітетом може перешкодити зусиллям держави, яка постраждала від інформаційного нападу, щодо здійснення адекватних дій у відповідь;

- визначення правомірного та співрозмірного характеру заходів, що здійснюватимуться у відповідь на інформаційний напад. Так, правомірним випадком застосування сили, крім колективних дій з підтримки миру під егідою ООН, є індивідуальна або колективна самооборона проти збройного нападу. Втім інформаційні напади з використанням мереж або інформаційної зброї, наприклад вірусів, не можуть бути однозначно кваліфіковані як збройний напад за Статутом ООН за загальним визначенням під збройним нападом розуміють застосування збройних сил, насильства, а також втручання в суверенні права держави) [36].

Таким чином, у сучасному міжнародному праві однозначно не вирішене питання про співвідношення між транскордонним характером інформаційних мереж і принципом державного суверенітету, а також відсутнє чітке розмежування таких понять як збройний напад, застосування сили, акт агресії й інших дотичних понять, відтак невизначеним лишається статус СІО, передусім здійснюваних в мирний час.

Зауважимо також, що основними об'єктами міжнародного гуманітарного права в інформаційній сфері є: цивільне населення; комбатанти й некомбатанти; особи, що перебувають під владою сторони конфлікту; жертви

війни (загиблі й поранені); військовополонені; культурні цінності й місця відправлення культу; установи, що слугують цілям науки й мистецтва, а також історичні пам'ятки. Захист цивільного населення в інформаційній сфері регламентований нормами, які передбачають заборону на примус громадян давати які-небудь відомості за будь-яких обставин, на примус громадян присягати на вірність новій владі тощо. Відповідальність за діяння окремих осіб забороняється покладати на все населення або групу осіб. Учасники конфлікту зобов'язані поважати сімейні цінності й права цивільного населення, переконання кожного громадянина. Заборонено зобов'язувати цивільних осіб брати участь у війні проти своєї батьківщини. Відносно осіб, що перебувають під владою конфліктуючої сторони, передбачені норми, що забезпечують їхній захист в інформаційній сфері: учасники конфлікту зобов'язані будь-якими шляхами вказувати допомога у возз’єднанні родин, на них накладає обов'язок документально засвідчувати факт і адреса евакуації дітей. Накладена заборона на наругу над людською гідністю. Журналісти, що виконують свої функції у військах, захищаються як цивільні особи. Заборонене насильство над психічним станом людини.

Міжнародно-правові аспекти забезпечення інформаційної безпеки у контексті допустимості проведення СІО доцільно розглядати і у світлі проблем протидії комп'ютерній злочинності. Уперше на міжнародному рівні спроба комплексного розгляду проблем комп'ютерної безпеки в кримінальному праві була розпочата Організацією економічного співробітництва й розвитку (ОЕСР). В 1986 році за результатами роботи свого правового комітету ОЭСР рекомендувала віднести до кримінально-карних діянь наступне: зміну комп'ютерних даних з метою незаконного збагачення; зміну комп'ютерних даних з метою підробки; зміну комп'ютерних даних з метою порушення функціонування комп'ютерів; порушення авторського права на комп'ютерні програми з метою наживи; доступ до комп'ютера або перехоплення інформації без дозволу відповідальної особи шляхом порушення охоронних заходів.

Зростання комп'ютерної злочинності змусило ще одну міжнародну організацію - Раду Європи, узгодити підхід до вироблення кримінально-

правових приписів, спрямованих на боротьбу з нею. Комітет Міністрів країн-членів Ради Європи рекомендував в 1989 році вважати злочинами: комп'ютерне шахрайство; комп'ютерну підробку; комп'ютерний саботаж; несанкціонований доступ; неправомірне відтворення охоронюваних авторським правом виробів і програм. У 2001 році Радою Європи була прийнята Європейська конвенція про кіберзлочинність [128], яка відносила до злочинів наступні діяння: протиправний доступ до інформації, перехоплення; порушення цілісності; втручання в роботу комп'ютерів та їх мереж; виробництво, обіг і використання спеціальних засобів для вчинення комп'ютерних злочинів; підробка, шахрайство з використанням комп'ютерів; дитяча порнографія; порушення авторського права.

Наразі міжнародним співтовариством визнається факт неповноти норм міжнародно-правового режиму інформаційної безпеки в умовах стрімкого підвищення рівня інформатизації суспільства. У рамках ООН іде активний переговірний процес щодо правового режиму інформаційної безпеки. Починаючи з 1998 року проблеми інформаційної безпеки обговорювалися на всіх сесіях Генеральної Асамблеї ООН. Основними з них є: визначення основних понять; створення міжнародної системи моніторингу загроз інформаційній безпеці; розробка міжнародно-правового режиму інформаційної безпеки; розробка договору про боротьбу з інформаційним тероризмом; запобігання появи нової - інформаційної - сфери конфронтації; визначення загальних поглядів на використання інформаційних технологій як зброї; оцінка руйнівних властивостей шкідливих програм для критично важливих елементів інфраструктури держави; відмова від дезінформації з метою ерозії духовного середовища. В Окінавській хартії глобального інформаційного суспільства [175] й актах Шанхайської організації співробітництва [73] особливо відзначене прагнення вдосконалити нормативну базу, що регулює інформаційні відносини. Однак реальне просування в області регулювання інформаційної безпеки, у тому числі при вирішенні транскордонних правових проблем, пов'язане з досвідом застосування міжнародних стандартів інформаційної безпеки.

Загальна увага до ефективного управління інформаційними системами й

технологіями привела до швидкого розвитку безлічі галузевих, національних і міжнародних стандартів управління ними взагалі і їх безпекою зокрема. Визначення відповідальності операторів інтернеткомунікацій стало ключовим питанням у правовому регулюванні інформаційних відносин низки країн Європейської Співдружності, а також США й Канади.

Так, наприклад, у Законі США "Про авторське право в цифрову епоху" 1998 року (Digital Millennium Copyright Act) [45] установлюється обмежена відповідальність оператора інтернет-зв'язку, що забороняє в певних випадках порушення авторських прав застосовувати до них санкції. Згідно із другим розділом Закону до таких випадків належать ситуації, коли оператор не ініціював сам передачу інформації, не вибирав кінцевого користувача за винятком автоматичної відповіді на запити, не змінював змісти переданого матеріалу, здійснював передачу інформації в автоматичному режимі без її відбору тощо. Крім цього в зазначеному законі визначаються умови тимчасового зберігання інформації, що порушує авторські права, за яких оператор інтернет- зв'язку також звільняється від відповідальності. У подібний спосіб вирішується також питання з інформацією наклепницького характеру. В 1996 році Конгрес США схвалив норму, що фактично виключає можливість розпочинати провадження про наклеп в Інтернеті проти операторів інтернет-зв'язку. Згідно з Комунікаційним Актом (Telecommunications act) 1996 року [44] оператор не відповідає за інформацію, що походить від третіх осіб, навіть якщо він має повідомлення про непристойний зміст, і нічого не вдіяв із цього приводу. Що стосується захисту публічних інтересів, то відповідальність операторів інтернет-зв'язку тут зводиться до обов'язку надання інформації про його абонентів. У цій області найбільш показовий "Закон патріота США" («Патріотичний акт») (USA patriot act) 2001 року [46], а точніше - його розділ II "Посилені процедури спостереження". Згідно зі статтею 210 на операторів інтернет-зв'язку покладено обов'язок щодо зберігання докладних записів електронних повідомлень абонента, включаючи ім'я, адресу, записи місцевих і міжміських телефонних з'єднань або сесійні записи й час сесій, тривалість надання послуг і тип послуги, номер телефону, обладнання або інший номер

абонента, включаючи тимчасово привласнений мережну адресу, а також засобу платежу за послуги, включаючи номер кредитної карти або банківського рахунку. У ст. 212 установлюється порядок надзвичайного розкриття інформації про електронні повідомлення з метою захисту життя й здоров'я, поділяючи його на добровільний (при якому оператор може розкрити інформацію державному органу, якщо провайдер обґрунтовано вважається, що розкриття інформації виправдане загрозою життю або серйозного збитку здоров'ю) і на вимогу державного органа. Ст. 216 поширила режим одержання санкції на відстеження телефонних номерів при обміні повідомленнями електронною поштою й відвідуванні сайтів в Інтернеті. При цьому зазначена санкція може бути видана суддею в будь-якому місці США. Без санкції суду інформація про абонентів повинна надаватися оператором на запит органів слідства (ст. 505), якщо така інформація потрібно для проведення санкціонованого розслідування міжнародного тероризму або таємницею розвідувальної діяльності, за умови, що таке розслідування відносно громадянина США проводиться тільки лише через його діяльність, охоронювану 1 поправкою до Конституції США.

Схожа схема регулювання використовується Європейським співтовариством відповідно до таких нормативних актів, як: Декларація про свободу комунікацій в Інтернеті 2003 року [92], Директива 97/66/ЄС Європейського Парламенту і Ради "Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі" [97], Директива 2000/31/ЄС 2000 року "Про електронну комерцію" [96], Конвенція Ради Європи про кіберзлочинність 2001 року [128]. Ці та інші документи становлять основу європейської правової бази у сфері Інтернету. Так, у Декларації про свободу комунікацій в Інтернеті визначені основні принципи, покликані гарантувати дотримання прав людини при користуванні глобальною комп'ютерною мережею. Документ закликає всі країни дотримуватися наступних принципів: не слід накладати на інформацію в Інтернеті які-небудь обмеження, які б перевищували обмеження, накладені на інші ЗМІ; слід заохочувати самоврядування й спільне управління в тому, що

стосується поширення інформації в Інтернеті; слід утримуватися від використання технологій, що блокують або фільтрують інформацію; з іншого боку, можливе застосування фільтрів, покликаних обмежити певні групи людей (наприклад, дітей) від небажаної для перегляду інформації; необхідно зробити все можливе, щоб усунути явища, що перешкоджають доступу в Інтернет, створенню й підтримці вебсайтів; слід уникати встановленню реєстраційних порядків, які перешкоджали б наданню послуг за допомогою Інтернету; слід обмежити відповідальність операторів інтернет-зв'язку, які не зобов'язані відслідковувати інформацію, передану через них; слід гарантувати надання права на анонімність і поважати бажання користувачів Інтернету не розкривати свої персональні дані.

Більшість європейських країн також адаптували стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 «Безпека в організації Північноатлантичного договору (НАТО)» [16], офіційній політиці НАТО у сфері кіберзахисту [32, 37], стратегічній концепції кібербезпеки, сформульованій за результатами Лісабонського саміту[33] й уточненій за результатами Варшавського саміту[35] тощо. Слід також зауважити, що практичне регулювання суспільних відносин в області використання інфраструктури інформаційного суспільства здійснюється в розвинених країнах у напрямку застосування міжнародних стандартів інформаційної безпеки, таких як ISO 17799 [115], COBIT [14], BS 7799-2 [11] тощо.

Вочевидь, міжнародне співтовариство має знайти загальне розуміння підходів, згаданих в Резолюції 60/45 Генеральної Асамблеї ООН «Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» [218], і використовувати його надалі як основу багатостороннього договору (конвенції), що створює універсальний режим міжнародної інформаційної безпеки. При цьому основною ідеєю нового міжнародного договору могло б стати зобов'язання учасників не вдаватися в інформаційному просторі до дій, метою яких є завдання збитків інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо, заради здійснення підриву політичної, економічної й соціальної систем, масованої психологічної обробки

населення, що здатні дестабілізувати життєдіяльність суспільства й держави.

Втім аналіз відкритих джерел свідчить про те, що сьогодні фахівці оборонних відомств, розвідувального співтовариства, інших урядових відомств і представники академічних кіл багатьох країн ведуть посилене опрацювання нових концепцій і принципів досягнення геополітичних переваг. Зокрема, у законодавстві Російської Федерації, терміни "інформаційна війна" і "протиборство в інформаційній сфері" уперше з'явилися в 2000 році, у другій редакції указу Президента РФ "Про затвердження Концепції національної безпеки Російської Федерації". Зокрема вказувалося, що "протиборство в інформаційній сфері" є однією з найважливіших завдань забезпечення національної безпеки РФ. Концепція містила посилання на "розробку низкою держав концепції інформаційних війн, що передбачає створення засобів небезпечного впливу на інформаційні сфери інших країн світу...". Так само це формулювання вживається в Доктрині інформаційної безпеки РФ [174], позначаючи одне із зовнішніх джерел загроз інформаційній безпеці країни. На даний момент документ втратив силу і був замінений більш свіжим аналогом. Наразі у Військовій доктрині РФ [68] мова йде про тенденцію "зсуву військових небезпек і військових загроз в інформаційний простір". Вказується така характерна риса сучасних військових конфліктів, як комплексне застосування заходів невоєнного характеру, у тому числі й інформаційних. Конкретно згадується така внутрішня військова небезпека, як "діяльність по інформаційному впливу на населення, передусім на молодих громадян країни, що має метою підрив історичних, духовних і патріотичних традицій в області захисту Батьківщини". Вказується одна з основних завдань оснащення збройних сил: "Розвиток сил і засобів інформаційного протиборства". Доктрина інформаційної безпеки РФ [174] одним з першочергових заходів щодо реалізації державної політики забезпечення інформаційної безпеки Росії називає комплексну протидія загрозам інформаційної війни. Так само в доктрині згадується поняття "інформаційно-психологічного впливу", однак визначення даного поняття в документі не наводиться. Крім іншого, відповідно до Указу Президента РФ від 16.08.2004 № 1082, Міністр оборони зобов’язаний подавати

Президентові РФ на затвердження План інформаційного протиборства [70].

Особливу увагу у цьому контексті привертає концепція "інформаційного панування", розроблювальна Управлінням повітряної розвідки США. Ідея завоювання інформаційної переваги над супротивником шляхом проведення СІО послідовно втілювалася в документах Міністерства оборони США "Чотирирічний огляд оборонної політики» [250], а також "Єдині перспективи 2010" і "Єдині перспективи 2020" [94, с.82-83]. Ці документи визначають мету, завдання й основні принципи інформаційного протиборства, обов'язки керівних органів і посадових осіб щодо організації й плануванню СІО в мирний час і в кризовій обстановці. У рамках цієї концепції, що передбачає широке використання наявного перспективного технологічного заділу й методів моделювання під "інформаційним пануванням" розуміється можливість "випереджального" одержання необхідних відомостей і даних про тактичну або стратегічну ситуацію, що дозволяє ухвалювати своєчасні рішення щодо нейтралізації й стримуванню дій сторони супротивника відповідно до стратегії «кризового реагування». Провідне місце, яке інформаційні системи займають в обґрунтуванні й вирішення завдань зазначеної стратегії, на сучасному етапі визначається наступними особливостями:

- розвиток інформаційних систем (на відміну від подальшого нарощування озброєнь) не викликає гострої негативної реакції в широких колах американської громадськості;
- розвиток таких систем є певною мірою «безпрограшним», оскільки інформаційні військові системи можуть використовуватися й у мирних цілях. Так, у США засоби космічного спостереження передбачається використовувати в комерційних цілях, для екологічного моніторингу, і в ході боротьби з міжнародним тероризмом і наркобізнесом;
- домінуючий статус США в розвитку засобів розвідки, зв'язку й управління закріплює їхню монополію на володіння військовою, економічною, політичною інформацією, необхідної для досягнення стратегічної раптовості у випадку наростання міжнародної напруженості [94, с.81-88].

У Стратегічній концепції НАТО з оборони й безпеки відзначається, що

альянс здійснюватиме всі необхідні заходи для запобігання, виявлення й захисту від кібератак, а також відновлення після них. З цією метою передбачене координування національних зусиль в галузі кібербезпеки, включення кіберзахисту в оборонні плани, забезпечення централізованого кіберзахисту всіх військових і цивільних структур НАТО [229, 231]. Про важливість питань кібербезпеки для Альянсу говорить і той факт, що в оновленій версії політики НАТО у сфері кібероборони 2011 року дія статті 5 поширюється на кіберзагрози. Підкреслюється, що НАТО буде надавати широку підтримку союзникам і партнерам з метою запобігання й протидії кібератакам, а також допомогу країнам, що потерпатимуть від атак у відновленні критично важливих інформаційних систем [15].

Поширення ст. 5 Вашингтонського договору [228] на кібератаки залишає відкритим питання, якого саме масштабу атаки можуть спричинити активацію механізмів колективної оборони. І хоча стаття 5 була задіяна лише одного разу (після терористичних атак на США у вересні 2001 року), дана ініціатива, хоча й цілком виправдана, може спровокувати ескалацію конфлікту у випадку некоректної оцінки кіберзагрози та її джерела. Найбільш активними прихильниками розширення дії принципу колективної відповідальності в сфері забезпечення інформаційної безпеки в системі НАТО виступають Естонія й, частково, США. Зокрема, професор Дж. Голдгейєр відзначає, що за своїм визначенням кібератаки не є «збройним нападом», тобто не підпадають під дію ст. 5, однак робить висновок про те, що Альянс «має об'єднатися у протидії атакам, що загрожують безпеці будь-кого зі членів НАТО» [20, с.4]. Необхідно зазначити, що питання протидії загрозам інформаційній безпеці, зокрема й кібербезпеці, відносять до сфери «м'якої безпеки» (soft security), у той час як головним завданням НАТО традиційно вважають протидію конвенційним викликам безпеки – забезпечення «жорсткої безпеки» (hard security) [116, с.109]. То ж ще одним проблемним фактором, що проявляється на трансатлантичному рівні, є «поділ праці» між членами НАТО, внаслідок якого одні країни спеціалізуватися на темах «м'якої безпеки», тоді як інші проводять «тверді» військові місії. Наслідком цього є розбіжність у підходах до протидії,

адже США, Франція, Великобританія й Німеччина зіставляють інформаційну безпеку з військовою стратегією, тоді як Естонія, яка не володіє потужним військовим потенціалом, наголошує на провідній ролі громадянського суспільства [29].

В грудні 2013 року Постійна рада ОБСЄ схвалила "Первісний перелік заходів зміцнення довіри в рамках ОБСЄ з метою зниження ризиків виникнення конфліктів у результаті використання інформаційних і комунікаційних технологій" [219]. Розробка даного документа стала можлива завдяки вже досягнутим між ключовими гравцями домовленостям з питань зміцнення заходів довіри в кіберпросторі. Це важливий перший крок міжнародного співтовариства убік підвищення транспарентності, передбачуваності й стабільності в кіберпросторі [99, с.58-61].

Необхідно також нагадати, що власне термін «інформаційні операції» запроваджено фахівцями оборонних відомств США у польових статутах FM 100-23 «Миротворчі операції» та FM 33-5 «Ведення психологічної війни» [67], а також у Доктрині Повітряних сил США 2-5 «Інформаційні операції» (Air Force Doctrine Document 2-5 «Information operations») від 2005 року[1], які передбачають СІО не тільки під час бойових дій, а й у мирний час.

Відповідно до Настанови Збройних сил США3-13 «Інформаційні операції» (Joint publication 3-13 «Information operations») від 2006 року інформаційні операції – це інтегроване застосування ключових можливостей електромагнітних засобів, комп'ютерних мереж, психологічних операцій, військового мистецтва та безпекових операцій разом із спеціальною підтримкою та відповідними можливостями з метою впливу, руйнування, завдання шкоди, захоплення процесу ухвалення рішень (людиною чи технічними засобами) при одночасному захисті власного [25]. Редакція цієї ж настанови від 2012 року передбачає, що інформаційні операції – це інтегроване застосування під час військових операцій можливостей, що стосуються інформації, разом з іншими засобами операції, з метою впливу, руйнування, завдання шкоди, захоплення процесу ухвалення рішення ворожою стороною або потенційним ворогом при одночасному захисті власного» [26]. Обґрунтовуючи перехід до нового

визначення, керівник Департаменту Оборони США в меморандумі «Стратегічні комунікації та інформаційні операції в Департаменті Оборони», зазначив, що «попередньому визначенню не вистачало посилань на інформаційне середовище і робився занадто великий акцент на ключових можливостях. Це призводить до розмивання відмінностей між цими можливостями та інформаційними операціями як інтегральною функцією персоналу. Успішні інформаційні операції вимагають виявлення можливостей, що стосуються інформації, для досягнення бажаного ефекту, а не просто застосування цих можливостей. Нове ж визначення вносить зміни до чинної концепції ще й у тому контексті, що ключові можливості мають бути під контролем однієї особи» [47]. При цьому під можливостями, що стосуються інформації, розуміють інструмент, технологію або діяльність, які застосовуються в межах інформаційного середовища, що може бути використано для створення впливу та бажаних умов операції. Як слушно зауважує з цього приводу В.Панченко, таким чином відбулося закріплення на офіційному рівні розуміння СІО як складової частини системи стратегічних комунікацій сектору безпеки та оборони [178].

Політика стратегічних комунікацій НАТО 2009 року (NATO Strategic Communications Policy) визначає «інформаційні операції» як військові рекомендації та координацію інформаційних військових заходів НАТО з метою створення бажаного впливу на наміри, розуміння (уявлення) та здатність ворожої сторони й інших суб'єктів (потенційного ворога, осіб, що ухвалюють рішення, культурних груп, представників міжнародного співтовариства тощо) на підтримку операцій, місій та цілей Альянсу [34]. У межах стратегічних комунікацій НАТО виокремлюється сфера психологічних операцій – спланована психологічна діяльність з використанням методів комунікації та інших засобів, спрямована на визначену аудиторію з метою впливу на свідомість, схильність та поведінку для досягнення політичних і військових цілей.

Як зазначають П. Кітон та М. Маккен, ще у зв'язку з переходом від воєнних дій і протидії тероризму в Афганістані до стану протидії надзвичайним ситуаціям, відновлення інфраструктури та розвитку, змінилися роль і значення присутнього там військового контингенту. За таких умов провідну роль почала

відігравати інформаційна підтримка військової операції, що призвело до появи нових підходів у комунікативній стратегії командування, створення нової структури функціонування, взаємодії та підпорядкованості підрозділів «інформаційного фронту» – зв'язків із громадськістю (Public Affairs), інформаційних операцій (Information Operation), психологічних операцій (Psychological Operations), і фактично стало поштовхом для формування системи стратегічних комунікацій [28], яка об'єднала всі три складові інформаційної підтримки відповідно до єдиного задуму, і призвело до їх агрегації в межах системи стратегічних комунікацій [178].

Доктрина інформаційної безпеки України наразі 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, а Служба безпеки України протидіє проведенню проти України СІО, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій [205]. Втім згадана Доктрина жодним чином не регламентує власне проведення СІО та не дає уявлення про їхню сутність. Як і Воєнна доктрина України[204], Доктрина інформаційної безпеки України яка опосередковано визначає СІО як елемент стратегічних комунікацій, що в цілому відповідає загальносвітовому тренду – такого висновку можемо дійти, спираючись на досвід США. Стратегічні комунікації при цьому визначаються як скоординоване і належне використання комунікативних можливостей держави - публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави.

Правову основу здійснення стратегічних комунікацій, зокрема й СІО, в Україні складають Конституція України та закони України (передусім Закон України "Про національну безпеку України»), Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року №

287, Воєнна доктрина України, затверджена Указом Президента України від 24 вересня 2015 року № 555, Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО, підписана 22 вересня 2015 року, Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14 березня 2016 року № 92, Стратегічний оборонний бюлетень України, уведений в дію Указом Президента України від 06 червня 2016 року № 240, Державна програма розвитку Збройних Сил України на період до 2020 року, уведена в дію Указом Президента України від 22 березня 2017 року № 73, Доктрина інформаційної безпеки, затверджена Указом Президента України від 25 лютого 2017 року № 47, Річна національна програма під егідою Комісії Україна - НАТО на 2017 рік, затверджена Указом Президента України від 08 квітня 2017 року № 103, Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України, затверджена Наказом Міністерства оборони України від 22 листопада 2017 року № 612, а також інші нормативно-правові акти, що регламентують функціонування і розвиток сектору безпеки і оборони.

Зокрема, відповідно до Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України [195], під інформаційними операціями розуміють узгоджені 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 їх поведінки у спосіб, що сприятиме досягненню політичних і військових цілей України. Такі визначення видаються

недосконалими, адже, з одного боку, психологічні операції становлять окремий випадок інформаційних операцій, а з іншого боку, на відміну від психологічних, інформаційні операції за змістом Концепції мають деструктивний наголос.

Зауважимо також, що 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 [199]. Це визначення може застосовуватись і 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 т.ч. СІО, розглядаються як форма воєнних дій.

Визначаючи правові межі для проведення стратегічних комунікацій, п.2.7 Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України [195] вказує, що у ході реалізації стратегічних комунікацій відповідно до компетенції Міністерства оборони та Збройних Сил встановлюються такі обмеження: всі заходи у сфері стратегічних комунікацій Міністерства оборони та Збройних Сил проводяться без порушення законних прав та свобод людини та громадянина, крім випадків обмежень, передбачених чинними нормативно-правовими актами; інформаційні та психологічні операції як складові стратегічних комунікацій не проводяться стосовно громадян України (крім тих, які є членами терористичних угруповань та незаконних

збройних формувань - хоча цими категоріями не вичерпується коло осіб, причетних до протиправних дій; так, як потенційна «аудиторія» СІО можуть розглядатися, наприклад, також учасники організованих злочинних угруповань). 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.

В 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, мова йде про проведення СІО «захисного» характеру, метою яких є забезпечення безпеки [232], а відповідно – така законодавча новація є непозбавленою сенсу умовах гібридної війни. Слід також зауважити, що відсутність такого роду змін до чинного законодавства ускладнює можливість проведення СІО не лише Збройними Силами України та іншими військовими формуваннями, але й правоохоронними органами України та іншими складовими сил оборони для виконання завдань. Крім того, залишається фактично позбавленим належного правового підґрунтя проведення СІО силами безпеки відповідно до їх компетенції, в тому числі й з метою протидії деструктивним СІО.

2.3. Теоретико-методологічні засади інформаційного забезпечення спеціальних інформаційних операцій

Як вже зазначалося у розділі 1 цього дослідження, СІО можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, тобто, охоплювати всі напрямки інформаційного протиборства.

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

При проведенні СІО інформаційно-психологічного характеру основними об'єктами впливу стає певна цільова аудиторія, тобто, психіка представників політичної еліти й населення конфронтуючих держав, а також система формування суспільної свідомості, думки й прийняття державно-управлінських рішень у сфері національної безпеки. СІО психологічної спрямованості, таким чином, становить цілеспрямоване виробництво й поширення спеціальної інформації, яка безпосередньо впливає (позитивно або негативно) на функціонування й розвиток інформаційно-психологічного середовища суспільства, психіку й поведінку політичної еліти й населення конкретної країни.

Термін «psychological operations» (PSYOP) - психологічні операції з'явився після закінчення Другої Світової війни. Засновані на психологічному впливі на керівництво, населення й особовий склад збройних сил іноземних держав, PSYOP мають на меті змінити поведінку цільових аудиторій для підтримки національних інтересів США. У кризовій ситуації й у ході бойових дій головна мета PSYOP - знизити моральний потенціал і психологічну стійкість супротивника до ведення війни й тим самим сприяти досягненню результатів власних військових і спеціальних операцій. Після завершення війни PSYOP спрямовуються на консолідацію суспільства, на забезпечення лояльності громадян до окупаційних військ, установленого режиму або тимчасової адміністрації [184].

Сьогодні більшість фахівців у питаннях інформаційної війни вважають, що термін «психологічні операції» не повною мірою відповідає сучасному рівню розвитку комунікацій. Наприклад, Д.Альбертс, Дж.Гарстка, Р. Хейз, Д.Сіньорі у своїй статті "Розуміння інформаційної епохи війни" найважливішими елементами стратегії інформаційного домінування визначають: інформаційний менеджмент (системи управління, зв'язку, комп'ютерного забезпечення, розвідки, спостереження й рекогносцировки), що забезпечує інформаційну перевагу над супротивником у будь-якому проблемному регіоні світу (у тому числі наявність ефективних засобів і методів ведення боротьби в інформаційній сфері - так званої інформаційної зброї, здатної дискредитувати інформаційні системи й комунікації, використовувані супротивником у даному регіоні); інформаційні операції - дії, спрямовані на порушення інформаційного управління супротивника (інформаційна блокада, дезінформація, привнесення надмірної невизначеності тощо), а також на захист власних інформаційних систем (забезпечення їх інформаційної безпеки, зниження рівня уразливості) від ворожого дискредитую чого впливу [6].

Відповідно, у червні 2010 року міністр оборони США затвердив пропозицію про заміну у терміна «психологічні операції» (PSYOP) терміном «Military Information Support Operations» (MISO), який можна перевести як "військові операції з інформаційного забезпечення" або ж "операції з інформаційного забезпечення дій Збройних сил". Запровадження цього нового терміну, на думку американського військового командування, означає "повну зміну доктрини, організаційної структури й практичної діяльності" щодо здійснення інформаційних операцій, а також має привести до активізації зусиль щодоо впливу на Конгрес США з метою проведення політики, спрямованої на перетворення інформаційних операцій в найважливіший інструмент політики держави [54].

Для повного розуміння змісту СІО важливо виділити суб'єкт і об'єкт інформаційного впливу. Наприклад, суб'єктами інформаційного впливу під час військових конфліктів у першу чергу будуть держави, що беруть участь у конфлікті. Державні органі зацікавлені у формування "правильної" суспільної

думки як усередині своєї країни, так і в інших країнах. Таким чином, будь-який інформаційний вплив під час збройних зіткнень максимально контролюється державою, і при цьому тільки вона має достовірну інформацію про події на території конфлікту. Зі становленням інформаційного суспільства все більший вплив у цій сфері одержують символічні аналітики, агенти впливу, медіа-активісти, колумністи тощо. Зокрема, Ф.Уебстер вважає, що сьогодні в американському суспільстві частка тих, хто працює з інформацією становить більше 59 % [238, с. 292-298]. Відповідна категорія суб'єктів інформаційного впливу може використовуватись організаторами СІО у власних цілях, тож у будь-якому випадку основними суб'єктами слід вважати саме організаторів СІО.

Для визначення об'єкта інформаційного впливу слід окреслити два підходи. За першим з них, запропонованим Є.Єгоровою-Гантман, об'єктом впливу є особи, що приймають рішення, або групи таких осіб - уряд, штаб, аналітики, групи населення, військовослужбовці супротивника [102, с.14-15].

У.Ліппманн пропонує інший підхід, обґрунтовуючи ідею про те, що головним об'єктом інформаційного впливу є суспільна думка [147, с.10-11]. Суспільна думка тісно пов'язана із соціальною природою людей. Це - стан масової свідомості, що містить у собі відношення (сховане або явне) людей до подій і фактів соціальної дійсності, до діяльності різних груп і окремих особистостей. Залежно від змісту висловлювань суспільна думка виражається в оціночних, аналітичних, конструктивних судженнях, вона регулює поведінку індивідів, соціальних груп і інститутів у суспільстві, виробляючи або асимілюючи (запозичаючи зі сфери науки, ідеології, релігії тощо) і насаджуючи певні норми суспільних відносин. Залежно від знаку висловлювань, вона виступає у вигляді позитивних або негативних суджень. Суспільна думка характеризується поняттями й установками, з якими згодна більшість членів даного співтовариства, відтак окрема людина може мати яку завгодно особисту думку, але якщо вона не прагне бути ізольованою від суспільства, втратити його підтримку, то змушена враховувати суспільну думку. Важливу роль у суспільній думці відіграє якийсь образ події, людини або процесу, властивий тій або інший соціальній групі. Під образом розуміється суб'єктивна картина

світу або його фрагментів, що припускає інтерпретацію лавиноподібного потоку інформації, одержуваної органами відчуттів, на основі особливої категоріальної системи, яка складалася в людини. Такі категорії становлять інтеріоризований суспільний досвід, закріплений у мові, впливаючи на суспільну думку [102, с.9-10].

На нашу думку об'єктом інформаційного впливу в ході СІО є, як вже зазначалося, є цільова аудиторія, а також інформаційні ресурси й інформаційні системи, вплив на які у низці випадків опосередковує вплив на цільову аудиторію (при цьому об’єкт впливу та об’єкт спрямування («мішень») СІО можуть не співпадати). Натомість власне об’єктом СІО є людина, суспільство, держава – ті об’єкти національної безпеки, на захист яких або проти яких спрямовується СІО за основним задумом. При цьому «мішенню» СІО інформаційно-психологічного спрямування є суспільна думка людей як у країнах, які беруть участь у військовому конфлікті, так і в тих, які лише беруть участь у дискурсі з даної проблематики. Так, Е.Гі Дебор передбачав становлення так званого «Суспільства Спектаклю». У такому суспільстві люди втрачають здатність сприймати реальність так, як вони сприймали її раніше - виходячи із суспільних і особистих відносин, знання й досвіду - і починають сприймати її винятково виходячи зі способів репрезентації предмета на телебаченні (“телекартинок“). Інтерес влади у створенні «спектаклю» полягає в тому, аби за допомогою технологій «спектаклю» людей позбавити можливості самостійно ухвалювати рішення [88, с.31]. Гі Дебор розділяє два види Спектаклю: розпилений, властивий країнам капіталістичного Заходу, і концентрований, властивий, наприклад СРСР та Китаю. Різниця між ними полягає в способах впливу: концентрований Спектакль відрізняє нетерпимість до будь-якої, навіть віртуальної свободи слова, більш сильний репресивний апарат, однак менша фетишизація товарного виробництва. У "Коментарях до Суспільства Спектаклю" Гі Дебор висунув ідею про те, що катастрофа СРСР і становлення ринкової економіки приведе до торжества нового виду Спектаклю - інтегрованого, який буде сполучати в собі диктат споживання й сильний репресивний апарат. У Суспільстві Спектаклю споживач інформації

виховується нездатним обмірковувати будь-що самостійно, він готовий тільки до прийняття готових оцінок і відомостей. Панування Спектаклю дозволяє суб'єктові інформаційного впливу створювати свої штучні картини подій, надавати подіям не фактичну, а вигадану інтерпретацію. Так, 6 лютого 2003 року тодішній держсекретар США К.Пауелл, для забезпечення міжнародної підтримки початку розгортання військових дій в Іраку, представив у Раді безпеки ООН записи переговорів між іракськими військовими, що говорили про те, що напередодні інспекційних перевірок ООН усі заборонені хімічні й біологічні матеріали повинні бути заховані. Потім він продемонстрував супутникові світлини, на яких були зняті сховища хімічної зброї біля г. Таджи. На інших знімках, зроблених за два дні до інспекцій, видні колони вантажівок поруч із іракськими хімічними й ракетними об'єктами. Далі Пауелл навів дані, отримані від інформаторів в Іраку, згідно з якими арабська країна розташовує 18 спеціально оснащеними трейлерами, використовуваним у якості мобільних лабораторій. Крім того, держсекретар з посиланням на джерело в Іраку заявив, що там зберігається від 100 до 500 тонн хімічних отруйних речовин і близько 16 тисяч ракет. На закінчення Пауелл продемонстрував пробірку зі зразками біологічної зброї, яку нібито викрала з Іраку американська розвідка. Після початку війни, під час її ведення й до сьогоднішнього дня незважаючи на активні пошуки ніяких підтверджень жодному з тверджень держсекретаря США не було знайдено. У своєму інтерв'ю на запитання російського радіослухача, що ж насправді містилося у демонстрованій ним пробірці, Пауелл відповів: "Там, зрозуміло, не було нічого небезпечного, це не був якийсь нервово-паралітичний газ, я б нічого небезпечного в ООН не приніс, це був просто муляж, який як би повинен був виглядати, як біологічна або хімічна зброя, яку, як ми знаємо, розробляв Ірак. І ми прагнули проілюструвати, наскільки могла бути небезпечною невелика кількість цього препарату, якби це дійсно було" [112]. Отже, згадану презентацію можна вважати саме проявом Спектаклю, своєрідною СІО.

Далі слід зупинитися на структурі СІО. Наприклад, О. Литвиненко у своїй роботі [150] виділяє такі етапи проведення СІО:

1. Попередній (підготовчий) етап. На цьому етапі здійснюється підготовка до операції, а саме планування, визначення та формування плану, цілі та мети операції, визначається арсенал сил, засобів, прийомів та методів впливу на аудиторію. На нашу думку, варто додати, що під час цього етапу має здійснюватись і інформаційна підготовка до наступного етапу, з метою гармонічності проходження інформаційного приводу та максимальної акцентуації мас-медіа, залучення цільової аудиторії до нього, відповідно досягнення максимальної ефективності зазначеного етапу. Це може бути досягнуто попередніми СІА чи/та СІО;

2. Обрання та/або створення інформаційного приводу (події, яку можливо використати як привід СІО). Головна мета цього етапу – привернення уваги до ситуації, події, явища, процесу якомога ширшої аудиторії та/або безпосередньо цільової аудиторії. Необхідно підкреслити, подія може бути вигаданою і не відбутись де-факто, тобто, мова йде про так звані «фейки» (від англ. «fake» - підробка, несправжні, вигадані новини);

3. «Розкрутка» інформаційного приводу. Цей етап є головною частиною СІО – його сутність полягає у використанні інформаційного приводу задля досягнення цілей операції. Метою цього етапу є примус, провокація цільової аудиторії до потрібних дій чи бездіяльності або направлення цільової аудиторії відповідно до задуму організаторів СІО;

4. Етап «виходу» із СІО або «закріплення». Завдання цього етапу - забезпечення плавного завершення СІО після досягнення поставлених цілей та фіксації отриманих результатів. Він має визначну роль у проведенні СІО, адже сучасний темп життя диктує необхідність отримання людиною значної кількості інформації. Відповідно, для того, щоб цільова аудиторія «засвоїла» інформацію необхідно її зробити достатньо значущою та/або такою, що добре запам’ятовується.

Успішність СІО залежить передусім від їх вдалого планування. Наразі методологія планування СІО найбільш розвинена у країнах НАТО, адже Альянсом впроваджені стандарти їх організації та проведення. З урахуванням того, що НАТО стандартизує процедури, які можуть бути віднесені до сфери

оборони, відповідні стандарти стосуються переважно СІО, що проводяться спільно з воєнними діями та в інтересах забезпечення їх проведення. Це стосується, зокрема, «електронної війни», введення супротивника в оману та фізичного знищення командних пунктів і вузлів зв'язку. В цілому планування СІО, засноване на загальній послідовності планування військових операцій НАТО, включає наступні стадії: ініціювання планування; орієнтування; розробка концепції операції; розробка плану операції та інших документів планування, врахування нових даних та уточнення плану операції.

На стадії ініціювання планування СІО за вказівкою уповноваженого керівника формується робоча група, до якої залучаються представники як підпорядкованих підрозділів, так і взаємодіючих штабів силових та інших структур. За потреби проводиться додаткова нарада, в ході якої уповноважений керівник доводить до членів робочої групи початковий намір щодо проведення СІО. Метою першої стадії процесу планування є створення необхідних умов для планування перспективних та поточних СІО на основі вказівок вищого керівництва. На стадії орієнтування здійснюється повний аналіз завдання на основі отриманого попереднього розпорядження та інших документів із вироблення відповідних вказівок керівника. Зокрема, на цій стадії група планування: отримує інформацію щодо початкового наміру керівника щодо виконання завдання; встановлює часову послідовність планування; віддає попередні розпорядження підпорядкованим підрозділам; оцінює обстановку; проводить аналіз наказів і розпоряджень вищого керівництва; здійснює оперативний аналіз і розробляє задум дій залучених підрозділів; визначає вимоги керівника щодо збору критично-необхідної оперативної інформації; проводить брифінг щодо аналізу завдання; готує та доводить до залучених підрозділів попереднє розпорядження керівника щодо планування СІО. Стадія розробки концепції СІО передбачає: уточнення вказівок керівника, які були опрацьовані протягом другої стадії; відпрацювання варіантів дій в ході СІО (зокрема шляхом проведення розіграшу відповідних сценаріїв та порівняння сценаріїв); визначення методу ведення обліку та виведення результатів; проведення брифінгу з прийняття рішення щодо затвердження концепції СІО.

Четверта стадія процесу планування СІО полягає в деталізації й уточненні концепції СІО, синхронізації дій підрозділів, уточненні наявних сил, які будуть задіяні для проведення СІО, опрацювання структури управління, деталізації додатків до плану. Остаточним результатом четвертої стадії є складання розгорнутого плану СІО. П'ята стадія процесу планування передбачає перевірку розробленого плану СІО шляхом моделювання, за результатами якого, а також у випадках зміни обстановки до плану вносяться необхідні корективи. Перевагою планування СІО за стандартами НАТО є детальний аналіз багатьох факторів обстановки, групові методи роботи, відпрацьовані й перевірені провідними зарубіжними країнами при забезпеченні національної безпеки прийоми й способи планування [43, 109]. При цьому для впровадження у практику планування та проведення СІО в Україні можуть бути рекомендовані, зокрема, наступні стандарти: AC / 322 CP / 1 Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) [13]; Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability (STANAG 4586) [42]; AJP-3.4.4 Allied Joint Doctrine for Counterinsurgency (COIN) [3]; AJP-3.9 Allied Joint Doctrine for Joint Targeting [4]; AJP-3.10 Allied Joint Doctrine for Information Operations [2]; AJP-5 Allied Joint Doctrine for Operational-Level Planning [5] тощо.

Аналіз зазначених документів дозволяє дійти висновку, що проведення СІО за стандартами НАТО передбачає врахування особливостей інформаційного середовища, як середовища, у якому «люди і автоматизовані системи спостерігають, орієнтують, вирішують та реагують на інформацію, відтак це є основне середовище прийняття рішень».

Інформаційні цілі являють собою очікувану вимірювану відповідь, яка відображає умови інформаційного середовища, змінювані внаслідок інформаційних дій. Під ними розуміються дії, що здійснюються, аби «зачепити» інформацію або інформаційні системи, і можуть носити як наступальний, так і захисний характер. Інформаційні цілі включають аналіз, планування, виконання, управління й оцінку пов'язаних дій або ефектів. При цьому інформаційні цілі можуть бути досягнуті за допомогою летальних або

нелетальних засобів, втім перевагу слід віддавати саме нелетальним заходам. При цьому інформаційні дії спрямовуються на здійснення: впливу на наміри та єдність сил супротивника; підриву довіри до владних інституцій супротивника; введення в оману, маніпулювання інформацією, погіршення можливостей супротивника щодо користування інформацією, управління інформаційними потоками та прийняття управлінських рішень; захисту власних сил, інформації та інформаційної інфраструктури, сил, інформації та інформаційної інфраструктури союзників; забезпечення власних сил та сил союзників інформацією з метою оптимізації процесу прийняття рішень.

СІО можуть поводитись на стратегічному, операційному і тактичному рівнях. При цьому принципами планування та проведення СІО є наступні:

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

Основні інструменти та методи, що використовуються в ході СІО:

- психологічні операції, покликані впливати на сприйняття, ставлення та

поведінку обраних осіб або груп (цільової аудиторії);

- демонстрація присутності (сили), статусу та соціального профілю;
- забезпечення інформаційної безпеки (комунікаційної безпеки, комп'ютерної безпеки, безпеки мереж, включно) та власне безпеки операції;
- введення в оману (маніпуляція, викривлення інформації, фальсифікація тощо) супротивника на всіх рівнях;
- «радіоелектронна війна», в тому числі з метою підтримання психологічних операцій, введення в оману та інших методів, що застосовуються. У СІО «захисного спрямування» використовуються радіоелектронні захисні заходи відповідно;
- фізичне руйнування з метою створення інформаційного ефекту (за умови врівноваження потенційного негативного впливу та очікуваних переваг);
- забезпечення лідером (керівником СІО) визначення ролей та адаптивних взаємовідносин між виконавцями СІО;
- комп'ютерні мережеві операції (комп'ютерна мережева атака; експлуатація комп'ютерних мереж; захист комп'ютерних мереж);
- зв'язки з громадськістю та військово-цивільне співробітництво задля встановлення довірчих стосунків між збройними силами, цивільними агентствами та мирним населенням;
- з метою забезпечення доступу до джерел інформації - участь у виконанні завдань зв'язку, розвідки, наданні консультативної допомоги, координації управління інфраструктурними проектами, рятувальних операціях.

Ключові месседжі СІО, які ілюструють спрямування інформаційних дій та очікуваний ефект: оцінити; змусити; зорієнтувати; зібрати інформацію; стримати; приховати; переконати; пошкодити; скоординувати; ввести в оману; погіршити; заперечити; зруйнувати; виявити; утримати; виставити; вплинути; повідомити; керувати; контролювати; нейтралізувати; попередити; дослідити; просувати; гарантувати; підтримати; спрямувати; перехопити; узурпувати.

При формуванні команди виконавців СІО до неї, окрім керівника та його заступників, які здійснюватимуть керівництво СІО «на місцях», мають включатися щонайменше: політичний радник; юрисконсульт; культурний

радник; відповідальний за зв'язки з громадськістю; представники Стратегічного командування НАТО з операцій (СКО) – J1-J9, тобто фахівці з персоналу, розвідки, оперативної та бойової підготовки, тилового забезпечення, перспективного планування, зв'язку та інформаційних систем, організації навчання, фінансового менеджменту та військово-цивільного співробітництва; фахівець з проведення психологічних операцій; представник сил спеціальних операцій; офіцер зв'язку; фахівець з радіоелектронної боротьби; фахівець з комп'ютерних мережевих операцій; «фахівець з обману»; фахівець з планування, синхронізації дій та оцінювання ефектів; фахівець з безпеки операцій.

В ході планування СІО особливо має враховуватися вплив так званої «чутливої інформації». Як дії з використанням «чутливої інформації» мають оцінюватися дії, що передбачають введення в оману, використання сили на підтримку СІО (з використанням Сил спеціальних операцій), використання спеціальних інформаційних технологій. Доступ до планів етапів СІО, які передбачають проведення відповідних дій, має обмежуватись, а до їх реалізації залучається обмежене коло виконавців СІО. План СІО в цілому має передбачати деталі стратегічного і політичного наміру, існуючі обмеження, очікувані ефекти інформаційних дій тощо. Все це підлягає узагальненню у вигляді матриці інформаційно-правового забезпечення СІО (етап СІО – кроки етапу СІО – планування – інформаційні продукти), яка надалі деталізується шляхом оцінювання інформаційного середовища, акторів, визначення пріоритету цілей, можливих ефектів в інформаційному середовищі.

Проведення СІО також має передбачати постійний зворотний зв'язок та оцінювання успішності проведених заходів, що у сукупності з необхідністю забезпечувати безпеку СІО робить доцільним застосування до планування й проведення СІО методології управління ризиками.

Далі перейдемо до аналізу механізму реалізації СІО, провідну роль у якому відіграють принципи організації комунікацій і безпосередні інформаційно-комунікаційні технології, адже динамічне становлення інформаційного суспільства, активне поширення у всіх сферах людської життєдіяльності

інформаційних інновацій затверджуєнові принципи соціальної комунікації: мережний, віртуальний інтерактивний [160, с.62-63].

Мережний принцип, який ствердив себе в економіці, політиці, соціальних процесах, спирається на теорію розподіленої мережі, яка не має центрального вузлового пункту. Перехід від ієрархічних до мережних структур інтенсивно відбувається не лише у сфері інформаційних технологій, але й у військовій справі, досить згадати тут концепцію мережоцентрических війн [186, с.117-125]. Мережний принцип реалізують сьогодні й асоціальні структури: терористичні групи, наркобізнес, організована злочинність. Сучасна мережна культура активно формує й нові спільності, інтерактивні переваги яких зосереджуються поза структурованою реальною владою соціальності або всупереч їй.

Віртуальний принцип заснований на моделюванні за допомогою нових інформаційних технологій можливої реальності буття. Штучними віртуальними технологіями, що слугують засобом занурення у віртуальну реальність, є сьогодні ЗМІ, іміджеві технології, піар-технології, комп'ютерні віртуальні технології тощо. Поринаючи в це середовище у ролі глядача, учасника, творця, людина має можливість використання його графічних, акустичних, пластичних, вербальних властивостей. Інтерактивне середовище віртуальних реальностей формується у різний спосіб. Так мас-медіа задають учасникові інтеракції свої параметри середовища й тему для комунікації. Інтерактивне середовище Інтернет, за яке йде сьогодні політична й комерційна боротьба, формується, у тому числі, і самими учасниками інтерактивного процесу. Призначена для ігрових зустрічей віртуальність, насправді стає новою реальністю й усе більш істотним фактором життєдіяльності людини як "людини, яка грає". Відтак саме з віртуальними суспільствами, що підтримують ту або іншу самобутню ідею, доведеться рахуватися всім без винятку як політичним, так і економічним структурам.

Інтерактивний принцип заснований на діалоговій, інтерактивній взаємодії користувача з комп'ютерними обладнаннями. У глобальному мережному просторі складаються власні, багато в чому альтернативні соціальним, процеси

самовизначення й самоврядування: від соціальної комунікації, що використовує множинні самоідентичності й способи взаємодії, до міжнародного тероризму, наркобізнесу та інших форм асоціальної комунікації, що ідентифікуються на мережній основі.

За словами У. Эко всі нові технології комунікацій надають безперервний потік інформації в реальному часі, який "щосекундно слугує рупором ворога (у той час як мета будь-якої військової політики - заглушити пропаганду супротивника) і знижує ентузіазм громадян кожної воюючої сторони стосовно їхніх власних урядів. А умовою перемоги є моральна єдність націй. У всіх війнах, відомих історії, народ, вважаючи свою війну справедливою, палко бажав знищити ворога. Наразі ж безмежна інформація не тільки розхитує ідеологію громадян, але й робить їх вразливими до страждань супротивника: смерть ворога перестає бути далекою й неясною подією, а перетворюється в конкретне й зовсім нестерпне видовище" [258].

В.Якунін, В.Багдасарян і С.Сулакшин вважають, що стратагеми сучасної міждержавної боротьби, заснованої на відмові від прямого насильства являють собою сукупність психологічних, інформаційних і політичних методів - soft power (м'яка або липка сила) - комплекс послідовних взаємообумовлених кроків, ланцюг, що викликає в кінцевій своїй ланці ефект соціального руйнування [261, с.5-6]. Тож в цілому інформаційно-комунікаційні технології можуть бути визначені як систему процедур, які, виходячи з певної програми дій, забезпечують фіксацію інформації, обробку й обмін інформацією (передачу, поширення, розкриття) з метою управління комунікацією соціального суб’єкта та передбачають будь-який соціальний комунікативний вплив (в тому числі одержання зворотної реакції) для вирішення будь-якого соціально-значущого завдання [72].

На думку І.Мальковської, у практичному аспекті більшість людей включені в соціальну комунікацію як виконавці і учасники її програм: публічних, рекламних, комерційних, партійних тощо. Про інші рівні соціальної комунікації, побудованих на засадах інтерактивності, люди часом і не здогадуються [160, с.51-55]. Так, перший рівень конструйованої соціальної

комунікації – це технології PR, маркетингу, реклами і т.ін. представляє типову сферу діяльності, що формує відносини людини з навколишнім інституціональним і соціальним середовищем у якості споживача будь-яких її пропозицій і послуг. Але для того, аби цю діяльність реалізовувати цілеспрямовано й продуктивно, потрібна ідеологія комунікації. Тому другий рівень комунікації - це ідеології, безліч ідеологій, які формують і розробляють для себе й під себе практично всі діючі в соціально-політичному просторі актори (термін акцентує дію, виставу, гру) і інститути (термін у більшій мері констатує формальну даність і легітимність): від університетів до політичних партій, від приватних фірм до супермаркетів, ця діяльність спрямована на управління людською ментальністю, формування прихильності людини багатьом формам реальних і уявних ідентичностей, потреб, послуг тощо. При цьому ідеології комунікації не завжди можуть бути ідентифіковані з їхніми носіями. Змішаність ідеологій створює для індивіда якийсь "комунікативний вінегрет" з новими ефектами, про яких може бути не догадуються й самі їхні творці. Вищої рівень комунікації - філософія комунікації. В основі соціальних технологій і ідеологій впливу на масову свідомість лежить більш глибокий шар, пов'язаний з архетипами, алгоритмами, мовними дискурсами, "археологією" і історією соціального знання й дії.

Виділення зазначених складових комунікації дозволяє "прояснити сучасні технології інформаційного панування, що використовують технологічні носії з метою отримання привілеїв існуючої нерівноправної системи вже не на рівні країни, держави, а в планетарному вимірі. У той же час бачення комунікації в семіологічному ключі дає підставу для аналізу символічних кодів, форм символічного насильства, драматургічних вистав, що розігруються на їхній основі, процесів формування публічної сфери, а також становлення мовних практик і міжкультурних діалогів" [160, с.57]. Тож соціальний простір сучасного суспільства усе більш набуває комунікативних властивостей, що в практичному плані відкриває нові інформаційні можливості для людини, та одночасно створює більш витончені механізми інформаційно-деструктивного впливу, до яких належать інформаційно-комунікативні технології.

Методологічно можна виділити низку інформаційно-комунікативних технологій, що використовуються при проведенні СІО, зокрема, фабрикацію фактів, маніпулятивну семантику, спрощення, стереотипізацію, відволікання уваги тощо, кожна з яких передбачає певні специфічні прийоми [76].

Технологія фабрикації фактів передбачає наступні прийоми: замовчування інформації; пряма неправда - поширення інформації, яка є свідомо неправдивою навіть із погляду її розповсюджувача. Джерела постійно себе компрометують, тому виникає інформаційна незадоволеність (особливо популярна "неправда задля порятунку" - народ не треба хвилювати кількістю заручників або загиблих у катастрофі, тому повідомляються менші цифри); створення інформаційного шуму, коли небажане повідомлення, витік якого до засобів масової комунікації неможливо уникнути, просто втрачається в потоці беззмістовної інформації; створення видимості плюралізму думок, коли різні засоби масової комунікації неначебто у різний спосіб відбивають одну й ту саму подію, у той же час наводячи на ті самі висновки; посилання на неіснуючі підстави - інформація подається як достовірна на підставі, яка не має ніякого реального змісту (сюди належать наприклад, публікації некоректно проведених соціологічних і маркетингових досліджень); інформаційні табу - інформація з деяких питань вважається забороненою за визначенням. Вона відрізняється від умовчування тим, що про наявність такої інформації всім відомо, втім вона приховується.

Технологія маніпулятивної семантики полягає в зміні змісту слів і понять передбачає наступні прийоми: конструювання повідомлення з обривків тексту або відео, що радикально змінює зміст сказаного або відзнятого; використання великої кількості складних для сприйняття й малознайомих громадськості термінів; використання понять, що перебувають на слуху, але не мають визначення, і, по суті, є такими, що не мають змісту; «зсув понять», коли загальновизнані терміни використовується не за призначенням, і його зміст у суспільній свідомості зміщується (наприклад, змішуються поняття «віра», "релігія" і "церква"); активне використання метафоричних лінгвістичних конструкцій; «негативна інформація сама себе продає, а за позитивну хтось

повинен платити» - негативна інформація одержує пріоритет над позитивною, що практично призводить до самознищення ЗМІ як джерела інформації; "на городі бузина, а в Києву дядько" - підставою сумнівного висновку представляється достовірна або загальновідома інформація, яка жодного відношення до висновку не має; розробка й впровадження в інформаційне середовище медіавирусов тощо [172].

Наприклад, Д.Рашкофф у своїй книзі "Медіавируси" описує так звані "мемы" [217, с. 299-322]. Ті люди, які позбавлені політичної влади в традиційному її розумінні, але прагнуть впливати на розвиток культури - "медіаактивисти", - розглядають інфосферу як кровоносну систему, у якій циркулюють інформація, ідеї й образи вони постійно вводять у неї нові ідеї, які автор вважає подібними до троянського коня, адже «вони проникають у наш будинок під якоюсь личиною, але, опинившись усередині, починають поводитися зовсім не так, як ми очікували. Ці інформаційні "бомби" за лічені секунди розлітаються по всій інформаційній мережі». Тож усередині кожної медіасенсації закладені ідеї, питання й концепції - найчастіше навмисно туди поміщені - які опосередковановпливають на аудиторію. Найбільш творчими й підступними вірусмейкерів Д.Рашкофф вважає так званих «приколістів», адже «приколи» впливають на нас на метафоричному рівні незалежно від того, чи є їх зміст правдою або містифікацією. "Приколизм - це війна за допомогою символів, знаряддя соціальної інженерії, який дозволяє втілити форми від медіасатири до квазітероризму.

Технології спрощення й стереотипізації також значну роль у сучасних засобах масової комунікації. Прості повідомлення швидше сприймаються масами, адже вони призначені саме для масової свідомості. Тому в них встановлені тверді обмеження на складність і оригінальність повідомлень (навіть на довжину слів, виключення становлять лише спеціально включені терміни, які мають заплутати чи спантеличити споживача). Загалом, журналістами було сформульовано таке правило: "Повідомлення завжди повинне мати рівень зрозумілості, відповідний до коефіцієнта інтелектуальності приблизно на десять пунктів нижче середнього

коефіцієнта того соціального шару, на який розраховано повідомлення" [169, с.138]. Дані технології передбачають наступні прийоми: твердження й повторення; дроблення й терміновість - у даному прийманні цілісна інформація розділяється на фрагменти, аби індивід не зміг з'єднати їх у єдине ціле і у нього не вистачило б часу осмислити проблему; сенсаційність.

Ще однією дієвою технологією, що використовується при проведенні СІО, є формування міфів. Міф становить оповідання про архетипічні події, що мають символічне значення, яке вказує на необхідність його копіювання в ритуальному акті й переконуєв реальності цієї події шляхом емоційного переживання від виконання ритуалу. Це легко досягається за допомогою переопису наявного й підключення уяви як засобу проживання в переописаному світі [188]. У розумінні Є.Кассирера міф має здатність "розшаровувати" буття на різні семантичні поля,а відтак - трансформувати сприйняття реальності, перетворюючись, зокрема, на політичну зброю [119, с.61; 146]. Міф становить особливу комунікативну систему. Р.Барт зазначає, що "міф нічого не приховує й нічого не демонструє - він деформує", тому що його завдання - "протягти якусь понятійну інтенцію". Барт називає міф "викраденою мовою", що свідчить про перекручення комунікативного процесу - зміст перетворюється у форму: створюючи умовно-правдоподібний антураж, форма полегшує засвоєння міфологічного повідомлення [56, с.233-278]. Отже, міф видозмінює реальність у свідомості людини, користуючись різноманітними прийомами й схемами.

Технологія відволікання уваги передбачає, що увага людини, яка збирає інформацію, залучається до незначущих подій, відтак людина відволікається від істотних подій**.** При цьому наведений перелік технологій, що можуть використовуватися при проведенні СІО, не є вичерпним.

Тож слід дійти висновку, що наразі теоретико-методологічні засади інформаційного забезпечення СІО характеризуються розгалуженим інструментарієм, який може успішно використовуватись як у військовий, так і у мирний час для різної цільової аудиторії. Відтак взяття відповідних теоретико-методологічних напрацювань «на озброєння» сектором безпеки і оборони України та його нормативно-правове закріплення, передусім інструментарію,

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

ВИСНОВКИ ЗА РОЗДІЛОМ

Результати наукових пошуків, відображені у цьому розділі, дали змогу визначити, що концепція інформаційної війни, у становленні якої наразі вирізняють чотири покоління, передбачає використання інформаційної зброї шляхом проведення інформаційних операцій, різновидом яких є СІО. СІО можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки інформаційного протиборства. СІО обох типів, а так само комплексні СІО можуть проводитися на оперативно-тактичному, стратегічному й глобальному рівнях з метою оперативної або стратегічного маскування конфліктуючими сторонами своїх реальних задумів, завдань і намірів, а також з метою дискредитації дій імовірного супротивника, його державної політики, економічних структур тощо. Класичним прикладом використання СІО у забезпеченні національної безпеки можуть вважатися антитерористичні СІО. Їх важливою складовою є інформаційно-психологічний вплив не тільки на терористів, але й на цивільне населення, у тому числі на суспільну думку як у власній, так і у закордонних країнах.

Виходячи з того, що на світовій арені відбувається геополітичне інформаційне протиборство, можна констатувати, що силові маневри держав, у сферу стратегічних інтересів яких входить Україна (мова йде в першу чергу про РФ, що вступила у відкриту фазу силового протистояння з нашою країною), спрямовані на нав'язування нашій незалежній державі своєї політичної волі й бачення майбутнього, установлення й досягнення стратегічних обріїв, які визначаються геоекономічною конкуренцією. Сили країни-агресора в більшості випадків перевершують вітчизняний потенціал, що змушує Україну звертатися до ідеї асиметричної протидії, у якій СІО відіграє одну з першорядних ролей.

Досліджуючи питання організаційно-правових засад інформаційно-правового забезпечення СІО слід констатувати, що правове підґрунтя проведення СІО може бути окреслено наступними напрямками: нормативно-

правові акти, що визначають обмеження і заборони при проведенні СІО (міжнародно-правові акти з питань протидії інформаційним загрозам, забезпечення інформаційної безпеки й регулювання інформаційного протиборства, а також акти національного інформаційного законодавства, присвячені регламентації інформаційних правовідносин та інформаційної сфери); нормативно-правові акти, що регламентують порядок і процес проведення СІО (національні відомчі нормативно-правові акти, переважно закритого характеру).

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

З урахуванням положень Закону України "Про оборону України" СІО можуть розглядатися як сукупність узгоджених і взаємопов’язаних за метою, завданнями, місцем та часом спеціальних дій підрозділів Сил спеціальних операцій ЗС України, спрямованих на створення умов для досягнення стратегічних (оперативних) цілей в інформаційному просторі, які проводяться за єдиним задумом самостійно або у взаємодії з військовими частинами, іншими підрозділами ЗС України, інших військових формувань,

правоохоронних органів України та інших складових сил оборони для виконання завдань. Ч.2 ст.4 вказаного Закону розглядає СІО (в числі інших спеціальних операцій) розглядаються як форма воєнних дій. Воєнна доктрина України і Доктрина інформаційної безпеки України опосередковано визначають СІО як елемент стратегічних комунікацій, що в цілому відповідає загальносвітовому тренду. При цьому правові межі для проведення стратегічних комунікацій визначені п.2.7 Концепції стратегічних комунікацій МО України та ЗС України, де, зокрема, визначено, що СІО не проводяться стосовно громадян України (крім тих, які є членами терористичних угруповань та незаконних збройних формувань - хоча цими категоріями не вичерпується коло осіб, причетних до протиправних дій; так, як потенційна «аудиторія» СІО можуть розглядатися, наприклад, також учасники організованих злочинних угруповань), а також 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 ЗС. Слід також зауважити, що відсутність правової регламентації проведення СІО у мирний час ускладнює можливість проведення СІО не лише ЗС України та іншими військовими формуваннями, але й правоохоронними органами України та іншими складовими сил оборони для виконання завдань. Крім того, залишається фактично позбавленим належного правового підґрунтя проведення СІО силами безпеки відповідно до їх компетенції, в тому числі й з метою протидії деструктивним СІО.

Теоретико-методологічні засади інформаційного забезпечення СІО наразі характеризуються розгалуженим інструментарієм, який може успішно використовуватись як у військовий, так і умирний час для різної цільової аудиторії. Відтак взяття відповідних теоретико-методологічних напрацювань «на озброєння» сектором безпеки і оборони України та його нормативно-правове закріплення на рівні відомчих докмуетів (передусім мова йде про той інструментарій, що передбачений у відповідних стандартах НАТО), значно посилить спроможності нашої держави у веденні інформаційного протиборства в умовах гібридної війни.

РОЗДІЛ 3. Правове забезпечення спеціальних інформаційних операцій: сучасний стан та напрями вдосконалення

3.1. Спеціальні інформаційні операції в системі заходів протидії загрозам національній безпеці України

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. У свою чергу, національні інтереси у загаданій статті визначаються як життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [198].

Ст. 1 Закону України «Про національну безпеку України» [198] 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. При цьому п. 3 чинної Стратегії національної безпеки України[203] актуальними загрозами національній безпеці визначені:

- агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, а саме: військова агресія, участь регулярних військ, радників, інструкторів і найманців у бойових діях на території України; розвідувально-підривна і диверсійна діяльність, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі і ненависті, сепаратизму і тероризму, створення і всебічна підтримка, зокрема військова, маріонеткових квазідержавних утворень на тимчасово окупованій території частини Донецької та Луганської областей;

тимчасова окупація території Автономної Республіки Крим і міста Севастополя та дальші дії щодо дестабілізації обстановки у Балто-Чорноморсько-Каспійському регіоні; нарощування військових угруповань біля кордонів України та на тимчасово окупованій території України, у тому числі розміщення на півострові Крим тактичної ядерної зброї; блокування зусиль України щодо протидії монополізації стратегічних галузей національної економіки російським капіталом, щодо позбавлення залежності від монопольних постачань критичної сировини, насамперед енергетичних ресурсів; торговельно-економічна війна; інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу (пп.3.1);

- неефективність системи забезпечення національної безпеки і оборони України: несформованість сектору безпеки і оборони України як цілісного функціонального об'єднання, керованого з єдиного центру; інституційна слабкість, непрофесійність, структурна незбалансованість органів сектору безпеки і оборони; недостатність ресурсного забезпечення та неефективне використання ресурсів у секторі безпеки і оборони; відсутність ефективних зовнішніх гарантій безпеки України; діяльність незаконних збройних формувань, зростання злочинності, незаконне використання вогнепальної зброї (пп.3.2);

- корупція та неефективна система державного управління: поширення корупції, її укорінення в усіх сферах державного управління; слабкість, дисфункціональність, застаріла модель публічних інститутів, депрофесіоналізація та деградація державної служби; здійснення державними органами діяльності в корпоративних та особистих інтересах, що призводить до порушення прав, свобод і законних інтересів громадян та суб'єктів господарської діяльності (пп.3.3);

- економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення: монопольно-олігархічна, низькотехнологічна, ресурсовитратна економічна модель; відсутність чітко визначених стратегічних

цілей, пріоритетних напрямів і завдань соціально-економічного, воєнно-економічного та науково-технічного розвитку України, а також ефективних механізмів концентрації ресурсів для досягнення таких цілей; високий рівень "тінізації" та криміналізації національної економіки, кримінально-кланова система розподілу суспільних ресурсів; деформоване державне регулювання і корупційний тиск на бізнес; надмірна залежність національної економіки від зовнішніх ринків; неефективне управління державним боргом; зменшення добробуту домогосподарств та зростання рівня безробіття; активізація міграційних процесів унаслідок бойових дій; руйнування економіки та систем життєзабезпечення на тимчасово окупованих територіях, втрата їх людського потенціалу, незаконне вивезення виробничих фондів на територію Росії (пп.3.4);

- загрози енергетичній безпеці: спотворення ринкових механізмів в енергетичному секторі; недостатній рівень диверсифікації джерел постачання енергоносіїв та технологій; криміналізація та корумпованість енергетичної сфери; недієва політика енергоефективності та енергозабезпечення (пп.3.5);

- загрози інформаційній безпеці: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства (пп.3.6);

- загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом (пп. 3.7);

- загрози безпеці критичної інфраструктури: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення (пп.3.8);

- загрози екологічній безпеці: надмірний антропогенний вплив і високий рівень техногенного навантаження на територію України; негативні екологічні наслідки Чорнобильської катастрофи; значний обсяг відходів виробництва та

споживання і неналежний рівень їх вторинного використання, переробки та утилізації; незадовільний стан єдиної державної системи та сил цивільного захисту, системи моніторингу довкілля (пп.3.9).

Відповідно до п. 4 Доктрини інформаційної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначені:

- здійснення 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;

- проведення державою-агресором СІО в інших державах з метою створення негативного іміджу України у світі;

- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

- інформаційне домінування держави-агресора на тимчасово окупованих територіях;

- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

- неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [205].

Наведені переліки загроз національній безпеці не є вичерпними і включають найбільш актуальні загрози поточного періоду. Втім, як бачимо, всі відповідні загрози можуть зумовлювати необхідність вжиття заходів

реагування у вигляді СІО, тож далі доцільно зосередитись на місці СІО в системі заходів протидії загрозам національній безпеці України.

На сьогодні можуть бути виділені такі групи основних 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.

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 деяких видів надмірності (структурної, функціональної, інформаційної, часової тощо) і 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.

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

СІО при цьому 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:

- 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.

Теорія проведення розвідувальних СІО лежить в основі концепції «цифрового поля бою», згідно з якою одержання оперативної інформації з району бойових дій, проведення контррозвідувальних або інших необхідних заходів в інтересах безпеки і оборони забезпечується комплексним застосуванням систем сенсорів і датчиків з різними рівнями деталізації одержуваної інформації. Усього прийнято виділяти чотири такі рівні: системи далекого виявлення, представлені, передусім, космічними системами спостереження, сейсмодатчиками й акустичними системами; системи оперативно-тактичного рівня; системи тактичного рівня, що включають оптичні, гравіметричні, біохімічні, акустичні та інші сенсори й датчики; засобу навігації й управління зброєю й бойовими платформами або соціальними групами. Створення багаторівневої системи засобів «наступального» збору даних

дозволяє одержувати максимально повну картину ситуації і полегшує розподіл інформації між користувачами. Разом з тим, для загальної інтеграції компонентів такої системи потрібна розробка особливих алгоритмів координації їх роботи, що являє собою досить складне завдання. Ця обставина обумовлює інтенсифікацію прикладних розробок в області штучного інтелекту й систем підтримки процесу прийняття рішень.

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. Не менш важливим є також і те, що такі викривлення мають тенденцію до зростання в міру проходження й обробки інформації від рівня до рівня, у зв'язку із чим усе більшу актуальність здобувають роботи зі створення систем порівняння й оцінки вхідної інформації в умовах невизначеності [114].

Зауважимо, що розвідувальний і контррозвідувальний аспект СІО проявляється на всіх етапах СІО незалежно від їх спрямування (детальніше див. підрозділ 3.3).

Далі слід перейти до аналізу й визначення прикладних методів ведення

інформаційного протистояння, які використовуються в ході проведення СІО як наступального, так і оборонного спрямування.

Зокрема, метою *електронної боротьби*, як прикладного методу ведення інформаційного протистояння, є зниження інформаційних можливостей супротивника, відповідно до чого вона підрозділяється на радіоелектронну боротьбу (створення умов, у яких передача або приймання інформації супротивником стає неможливим, зокрема, через постановку активних і пасивних перешкод), криптографічну боротьбу (викривлення й ліквідація властиво інформації) і боротьбу з комунікаційними системами супротивника.

Радіоелектронна боротьба як комплекс заходів забезпечення СІО, здійснюється з метою виявлення радіоелектронних засобів і систем супротивника. Слід зазначити, що раніше, коли засоби приймання-передачі інформації працювали на фіксованій частоті, завдання їх пригнічення вирішувалося простіше, чим у цей час, коли широко використовуються відповідні засоби зі змінюваною робочою частотою. У цьому зв'язку засоби й методи ведення радіоелектронної боротьби постійно удосконалюються, зокрема, передбачається не тільки влаштування перешкод, що ускладнюють або не допускають передачу інформації, але й використання параметрів випромінюючої апаратури супротивника для наведення на них засобів фізичного враження. Оскільки при такому наведенні на мету використовуються не пасивні параметри об'єкта ураження (теплове випромінювання, візуальний образ), а активні, можливість застосування протирадіолокаційної зброї може утруднити або навіть привести до відмови від використання засобів приймання-передачі інформації [156].

Боротьба з комунікаційними системами (лініями зв'язку) супротивника є більш складним завданням, ніж ведення радіоелектронної боротьби, що визначається насамперед тим, що засоби приймання-передачі інформації уже в силу свого функціонального призначення є джерелами випромінювання, що досить легко виявляється, натомість випромінювання ліній і каналів зв'язку за можливості знижується до мінімально досяжного рівня. Зокрема, ізоляція й екранування таких ліній зв'язку, а також використання волоконної оптики й

лазерної техніки дозволяє значною мірою уникнути не тільки втрат і викривлення інформації в силу природних причин, але й перехоплення супротивником даних, що передаються лініями зв’язку. Проте, у низці випадків канали обміну інформацією залишаються потенційно вразливими, особливо для бездротової передачі інформації з об'єктів (наприклад, супутників), місце розташування яких може бути з достатньою точністю визначене й зафіксоване. У цьому випадку такі канали комунікацій неможливо повністю ізолювати або екранувати, і досить ефективним способом боротьби з ними стає постановка хаотичних перешкод, чиїм завданням стає не глушіння (придушення) сигналу, а заповнення фоновими або загороджувальними шумами того середовища, у якому здійснюється передача інформації. Можливе також і перехоплення переданої інформації, навіть у випадку використання вузькоспрямованих систем зв'язку, однак вирішення цього завдання здійснюється вже в сфері криптографічної боротьби.

Криптографічна боротьба, як засіб ведення інформаційного протиборства, полягає у приховуванні (зашифровці) власних даних і одержанні доступу до даних, приховуваним супротивником. При цьому основний принцип захисту інформації полягає в тому, що розшифрування (яке потенційно завжди можливе) захищеної сучасними методами криптографії інформації є трудомістким і складним процесом, що вимагає потужної обчислювальної техніки, й займає, як правило, досить значний час, протягом якого інформація може застаріти. Спільне використання різних методів криптозахисту, наприклад комбіноване застосування довгих ключів і багаторазового перешифрування даних робить швидке розшифрування інформації украй малоймовірним. Відтак одним з головних завдань, що стоять перед підрозділами криптографічної боротьби структур сектору безпеки і оборони при розшифруванні інформації супротивника, є попереднє визначення її цінності й того часу, протягом якого дешифрована інформація не втратить своєї цінності. Аналогічне завдання повинне вирішуватися також і при шифруванні власних даних, оскільки невиправдане застосування ускладнених методів криптозахисту може викликати суттєве збільшення обсягу переданої

інформації, зниження швидкості її передачі/приймання й загальне перевантаження каналів зв'язку. Таким чином, необхідний ступінь криптозахисту слід визначати залежно від цінності інформації.

Методи психологічного впливу. У випадках, коли використання методів інформаційного протиборства спрямоване не проти інформаційних систем супротивника, а безпосередньо проти людської психіки, мова йде про методи психологічного впливу, котрі у загальному вигляді можна визначити як маніпулювання суспільною свідомістю й суспільною думкою на різних соціальних рівнях. СІО, що базуються переважно на використанні методів психологічного впливу, можуть спрямовуватись проти структур державного управління, військового командування, збройних сил, конкретних соціальних утворень, або становити так звану «війну культур» («культуркампф») [241].

В ході СІО, спрямованих проти структур державного управління головними об'єктами інформаційного впливу є суспільство в цілому й основні структури державного управління. При цьому найбільш сприйнятливим до такого роду впливу є суспільна думка, адже державні структури, внаслідок властивої їм консервативності відносно менш сприйнятливі до стандартних методів маніпулювання суспільною свідомістю. Для проведення СІО, метою яких є дестабілізація внутрішнього становища в країні супротивника, найбільш ефективним інструментом виступають ЗМІ. При цьому можуть застосовуватися різні способи впливу через ЗМІ, у тому числі й пов'язані із впливом на інфраструктуру самих ЗМІ. Можна виділити наступні етапи такого впливу, які нижче розташовуються в порядку убування їх ефективності:

- справляння впливу через національні ЗМІ супротивника;
- у випадку якщо це неможливо, а також з метою досягнення більшого ефекту - формування альтернативних каналів інформаційно-психологічного впливу (альтернативні ЗМІ, іномовлення тощо). Ключову роль в цьому наразі відіграє глобальна інформаційна мережа Інтернет;
- справляння зовнішнього тиску на політичне керівництво й суспільну думку держави-супротивника, створення міжнародного клімату, що перешкоджає реалізації планів супротивника;

- придушення існуючих систем національного віщання (знищення ретрансляційних супутників, телевізійних і радіомовних станцій тощо).

Якщо вести мову про СІО, спрямовані проти структур військового командування, слід зазначити, що на думку аналітиків INSS [23], пряма пропагандистська боротьба проти командування навряд чи матиме успіх. Якщо розглядати типову модель державної будови, то військове керівництво будь-якого рівня є інструментом, що виконує волю політичного керівництва держави а отже - не відіграє вирішальної ролі в процесах прийняття політичних рішень. Тож основним засобом, що використовуваних у ході СІО проти командних структур, є дезінформація. Так, оскільки будь-які рішення ухвалюються військовим командуванням на основі аналізу складних подій, які переважно слабко піддаються прогнозуванню подій, надання супротивникові надлишкової й суперечливої інформації про події, що відбуваються, в умовах обмеженого часу прийняття адекватних рішень, дозволяє значною мірою зашкодити процесу командування й бойового управління. Не менш важливу роль у дезорганізації діяльності командних структур може відігравати залякування. Зокрема, ефективним вважається формування в супротивника стійкої думки про перевагу іншої сторони й про безглуздість опору. Однак така інформація може бути й об'єктивною. Тож ключовим моментом у дезорганізації супротивника є стирання грані між можливим, реально існуючим і неможливим. Для досягнення цієї мети була запропонована «стратегія нав'язаної вартості». Її автор, полковник ВПС США Дж.Уорден вважає, що якщо супротивникові вдасться нав'язати такий спосіб дій, який згодом виявиться занадто витратним для нього, він, зрештою, відмовиться від продовження боротьби [18]. Реалізація цієї стратегії припускає проведення наступних заходів: оцінку цінностей, сил і засобів супротивника, його сильних і слабких сторін; визначення на основі отриманої системи оцінок "бойового порогу" супротивника; здійснення інформаційних акцій, спрямованих на досягнення й перевищення цього порогу з метою викликати частковий параліч і створити загрозу повного паралічу в діяльності командних структур.

Вважається, що у низці випадків дії в кризовій ситуації можна буде

обмежити тільки демонстрацією можливостей, тобто, конфлікт буде вирішений вже на фазі психологічної обробки керуючої ланки супротивника.

З розглянутою стратегією значною мірою корелює так звана «стратегія паралічу», мета якої - унеможливити подальше продовження опору з боку супротивника. При цьому формулюється наступна ієрархія основних цілей впливу в ході СІО: політичне й військове керівництво країни; базове виробництво (промисловість, енергетика); інфраструктура (транспорт, комунікації); населення; військові підрозділи. Що стосується ступеня впливу на систему в цілому, то вона буде визначатися вибором конкретної мети або сукупності цілей.

СІО проти особового складу збройних сил супротивника базуються на використанні двох основних почуттів, що притаманні людині: страху смерті й взаємної ворожості, а також на відсутності безпосереднього зв'язку між передовою й тилом. Для вирішення завдання деморалізації особового складу задіюються як традиційні (листівки, радіомовлення тощо), так сучасні способи пропаганди. Значний ефект може бути отриманий передусім при наданні правдоподібної, але провокуючої страх або почуття незадоволеності інформації безпосередньо кожному учасникові бойових дій з боку супротивника. Іншим перспективним методом психологічного впливу в умовах конфліктів низької інтенсивності (коли "передова" і "тил" володіють обмеженою інформацією одне про одне) уважається надання їм роздільної й дозованої інформації. При цьому передбачається задіяти й національні інформаційні канали супротивника.

Війна культур («культуркампф») як метод проведення СІО відповідає відомій тезі С.Хантінгтона про зіткнення цивілізацій, згідно з якою основними сторонами протиборства в майбутньому будуть не держави, а цивілізації [246]. У ході такого протиборства для безкровної перемоги або забезпечення контролю над супротивником необхідна передача йому власних світоглядних і культурних цінностей, тобто заміщення національної культури певним набором базисних «загальнолюдських» цінностей. Такі цінності не обов'язково повинні лежати в ідеологічній або світоглядній площині (права людини, забезпечення свобод), але можуть належати й побутовій сфері (поширення культури

харчування, книжок, фільмів і інших атрибутів, що пропагують певний спосіб життя). При цьому важливу роль у поширенні тих чи інших культурних моделей (у контексті України – євроатлантична цивілізаційна модель або модель «руського міру») відіграють сучасні комунікаційні й інформаційні можливості. Зокрема, використання мережі Інтернет і надалі слугуватиме просуванню ідей «відкритого суспільства», що надає можливість ефективно маніпулювати свідомістю. Водночас, якщо, наприклад, сьогодні культурний експорт США і країн Європи в країни Близького Сходу обмежується поширенням принципів вільної торгівлі, демократії й політичної культури, зворотний вплив східних держав полягає у суто культурному проникненні, прикладом чого слугує поширення ісламу й орієнталістських релігійних сект у США й інших західних країнах. Відтак останнім часом культурологічні аспекти концепції «культуркапф» розглядаються багатьма країнами як частина державної політики, чого не спостерігалося раніше.

Сутність так званої *«хакерської боротьби»* як методу проведення СІО зводиться головним чином до здійснення «атак» на різні компоненти комп'ютерних мереж, а також на інформаційні ресурси, що в них зберігаються. Основною особливістю хакерських "атак" є те, що вони носять не апаратний, а програмний характер, тобто, програма проникнення, що використовується хакером, здатна виявляти вразливе місце в структурі захисту комп'ютерної системи супротивника й проникати через неї, що в результаті дає можливість керувати працездатністю системи або маніпулювати інформацією, яка в ній міститься (знищувати, змінювати тощо). Конкретні прийоми хакерської боротьби можуть бути різноманітними за своїм характером. Їхньою метою може бути як повне виведення з ладу комп'ютерних систем, так і ініціювання різних періодичних або підлаштованих до конкретного моменту часу збоїв у роботі, вибіркове викривлення даних, що містяться в системі, одержання доступу до системної інформації (паролі, адреси), несанкціонований моніторинг роботи системи, викривлення трафіку повідомлень. Найбільш популярним з використовуваних у цей час засобів є так звані комп'ютерні віруси, «хробаки», «троянські коні», логічні бомби, «діри» у системі,

«прошивання» постійного запам’ятовуючого пристрою. Комп'ютерний вірус за своїм змістом є фрагментом програмного коду, що здатен до самокопіювання шляхом запису своєї копії в коди інших програм комп'ютерної системи, що зазнала хакерської атаки. Такий вірус є засобом порушення працездатності компонентів програмного забезпечення або локальної системи. Комп'ютерний вірус активується в ході запуску програми, до якої він впроваджений, після чого він може або скопіювати себе в іншу програму, або виконати дії з викривлення даних або порушенню працездатності системи. Водночас, істотним недоліком комп'ютерних вірусів з погляду цілеспрямованого інформаційного впливу в ході СІО є їх майже повна автономність (за винятком необхідності запуску програми-«хазяїна»), внаслідок чого практично не існує можливості контролювати й корегувати їхню роботу в системі супротивника.

На відміну від комп'ютерних вірусів, "хробак" - самостійний програмний пакет, призначений для самопоширення шляхом копіювання свого пакета з одного комп'ютера на інший, як правило, через мережу, у тому числі й Інтернет. Інша важлива відмінність "хробака" від вірусу полягає в тому, що він не модифікує програми комп'ютерної системи й не ушкоджує дані на локальному комп'ютері, а дозволяє відповідно до свого призначення порушувати працездатність мережі або одержувати доступ до її інформаційних ресурсів.

"Троянський кінь" являє собою фрагмент комп'ютерного коду, схований усередині інфікованої програми і є широко використовуваним механізмом маскування проникнення вірусів або "хробаків" до системи. "Троянські коні" можуть маскуватися, зокрема, під службові програми, що поставляються з комерційними й іншими програмними комплексами забезпечення безпеки комп'ютерних систем. «Троян» практично не залишає слідів своєї присутності, адже не втручається в роботу системи, тож його вкрай важко виявити.

Логічна бомба є різновидом "троянського коня" і використовується для ініціювання вірусної або іншого роду програмної атаки на комп'ютерну систему. Найбільш відомим і розповсюдженим є спрацьовування логічної бомби на заздалегідь заданий контекст (ключове слово). Логічна бомба може бути самостійною програмою або фрагментом коду певного програмного

продукту (пакета програм).

«Дірами» або «чорними ходами» називають спеціальні програмні механізми, що діють в обхід систем безпеки, які вбудовуються в систему виробником програмного забезпечення з метою одержання доступу виробника (або особи, чиї інтереси він забезпечує) до інформаційних ресурсів і налаштувань системи. Цей метод уважається найбільш привабливим для проведення СІО. Зокрема, восени 1999 року в США вибухнув гучний скандал, пов'язаний з тим, що одному із програмістів удалося виявити такі «діри» у програмних продуктах Microsoft - розроблювача популярної й найбільш широко використовуваної сьогодні операційної системи MS Windows.

Якщо у програмне забезпечення можуть бути закладені компоненти, що виконують непередбачувані функції, виробники апаратного забезпечення, насамперед, обладнань із постійними запам'ятовувальними пристроями (наприклад, BIOS) також можуть впроваджувати логічні бомби або встановлювати "діри" у комп'ютерних системах. Зміни в програмне забезпечення різних постійних запам’ятовуючих пристроїв можуть бути внесені й іншими особами, наприклад, при перепрограмуванні.

На відміну від хакерських атак, так звана *концепція «кібернетичної» або «мережної боротьби»* меншою мірою пов’язана із суто інформаційними технологіями й охоплює повний комплекс проблем і аспектів інформаційного протиборства (організаційні, доктринальні, стратегічні, тактичні й технічні сторони ведення наступальних і оборонних СІО). Зокрема, концепція кібернетичної боротьби, що належить до військових СІО, стає усе більш актуальною у військовій сфері коли мова йде про конфлікти високої інтенсивності. З іншого боку, роль мережної боротьби зростає й у конфліктах низької інтенсивності й при проведенні так званих "невійськових операцій», а також у конфліктах, що носять невоєнний характер, зокрема, терористичних та інших злочинах. При цьому поняття мережної боротьби стосується радше організаційної форми протиборства з використанням інформаційних можливостей, ніж суто боротьби з інформаційною інфраструктурою супротивника, і передбачає використання інформаційної інфраструктури

супротивника у власних цілях. За таких умов головними дієвими особами виступають невеликі взаємозалежні й координуючі свої дії групи, що не мають єдиного командування, структура яких будується не на ієрархічному, а на мережному принципі. Тож на державному рівні мережна боротьба зводиться насамперед до протидії утворенням, що використовують мережні організаційні методи, наприклад, до антитерористичної боротьби, протидії злочинності тощо.

Як окрему групу методів СІО вирізняють також *економічне інформаційне протиборство*, зокрема у формах інформаційної блокади й інформаційного імперіалізму. Так, сучасні розвинені суспільства у своєму стабільному функціонуванні залежать не лише від матеріального постачання, але й від стабільності інформаційних потоків та від можливості вчасного одержання доступу до інформаційних ресурсів. Більше того, процеси глобалізації світової економіки й розвитку негрошової економіки перетворюють залежність фінансового сектору від інформаційних і обслуговуючих технологій на абсолютну. У таких умовах економічна інформаційна блокада стає вкрай гнучким і ефективним методом впливу на потенційного супротивника. На відміну від уведення ембарго на той або інший вид товарів або інших економічних санкцій, інформаційна блокада може носити прихований характер, а відповідні інформаційні операції можуть бути завуальовані під випадкові збої інформаційних систем або хакерські атаки. При цьому, природно, не виключена й можливість відкритого державного тиску у відповідній сфері. Слід зауважити, що ефективність інформаційної блокади багато в чому визначається рівнем контролю над інформаційними ресурсами в глобальному масштабі, у зв'язку із чим постійно наростає актуальність другого напрямку економічного інформаційного протиборства - інформаційного імперіалізму, коли найбільш пристосованими до ефективної економічної діяльності в нових умовах виявилися технологічно розвинені держави, серед яких безперечним лідером виступають США, що забезпечує цій державі технічні можливості впливу на міжнародні організації, у тому числі й інформаційного порядку, зокрема, беручи участь у розробці, створенні й супроводі ряду міжнародних баз даних (в тому числі баз даних ООН, МАГАТЕ, ФАО, ЮНЕСКО, МВФ, СОТ тощо).

Більшість аналітиків відзначає, що на сучасному етапі структура інформаційних комунікацій починає суттєво змінюватися. Якщо на початку свого функціонування Інтернет розглядався переважно як множина інформаційних ресурсів, і основним його завданням вважалося надання допомоги в пошуку потрібної інформації й організації доступу до неї, то сьогодні головним завданням Інтернету вважається надання допомоги у пошуку необхідних партнерів і організації між ними потрібного виду комунікацій з необхідною інтенсивністю (збільшення "віртуальної" ділової активності). Чітко прослідковуються дві головні тенденції в розвитку інформаційних комунікаційних послуг, відповідно до яких: людина у найближчому майбутньому буде одержувати тільки ту інформацію, яка її цікавить, й безпосередньо з її джерела; будь-яка людина або компанія може з невеликими витратами відкрити в Інтернеті свій власний канал віщання, що приведе до появи мільйонів незалежних інформаційних каналів.

Це, відповідно, змінює ту частину бізнесу, яка займається випуском періодичних видань та іншої інформаційної продукції. Зокрема, уже сьогодні більшість періодичних видань мають власні електронні версії в Інтернеті. Одночасно із цим підвищується актуальність проблеми прямого проникнення іноземних кампаній на внутрішній ринок. Зміна структури світових комунікацій протягом останніх 20 років знайшла відбиття в трансформації моделі ведення комерційної діяльності в Інтернеті убік більшого використання надаваних їм інтерактивних можливостей. Якщо 20 років тому комерційна діяльність постачальників інформаційних послуг в Інтернеті здійснювалася головним чином за рахунок розміщення реклами на своїх серверах і Web-сторінках, то сьогодні відбулася зміна комерційної орієнтації в глобальній мережі, і найбільше поширення одержують багатобічні моделі генерації доходу: реклама, підписка, торгівля, абонентне обслуговування (pay-per-view), електронні банківські операції тощо. Найбільший вплив "інформаційної революції" випробувала на собі міжнародна фінансово-кредитна сфера. У результаті розвитку засобів автоматизації фінансових операцій була створена міжнародна телекомунікаційна банківська система "SWIFT", що об'єднала

понад 2000 банки в 60 країнах миру. Надійність даної системи досягається обмеженням доступу до мережі - до роботи в ній допущені тільки сертифіковані банки, а будь-яка спроба злому цієї системи спричиняє негайне видалення з неї порушника. Водночас, ця система може використовуватися для контролю й управління валютно-фінансовою ситуацією у світі з боку провідних банків розвинених країн. Процес "віртуалізації" світової економіки привів і до того, що загальний обсяг капіталів на фінансових ринках на порядок перевершує світовий внутрішній валовий продукт. Одночасний розвиток технічних можливостей засобів зв'язку, передачі і накопичення інформації призвів до зростання мобільності капіталів, а також до зростання чутливості світових фінансово-економічних і соціальних процесів до інформаційних впливу. Зокрема, наслідком прискореного переходу від розрахунків готівкою до електронних розрахунків є, з одного боку, створення достатнє міцної бази для здійснення державного контролю й регулювання фінансових потоків, а з іншого - підвищення уразливості комп'ютерних банківських мереж до різного роду махінацій. Існує також небезпека монополізації сфери електронних фінансових розрахунків.

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. Відтак СІО посідають важливе місце у системі засобів протидії загрозам національній безпеці, і як інформаційно-правовий феномен характеризуються розгалуженою системою методів.

3.2. Актуальні проблеми правового забезпечення спеціальних інформаційних операцій

Основною проблемою інформаційно-правового забезпечення СІО в умовах сьогодення є передусім відсутність достатнього законодавчого унормування їх проведення, про що вже зазначалося у попередніх розділах цього дисертаційного дослідження. Відповідно, відсутнє й достатнє законодавче підґрунтя для розробки

методологічних засад інформаційного забезпечення СІО.

Слід ще раз підкреслити, що поняття СІО тісно пов’язане із поняттям інформаційного впливу та протидії інформаційного впливу, які наразі не отримали законодавчого 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 з національних інтересів України в інформаційній сфері [205].

В цілому Стратегія національної безпеки України та Доктрина інформаційної безпеки виходячи із загроз національній безпеці, які аналізувалися у попередньому підрозділі, 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 [203].

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 ситуацій. 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 [205].

Як вже зазначалося, у Законі України «Про оборону України» наведено поняття спеціальних операцій [199], в т.ч. й СІО, а також передбачено, 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. Тож спеціальні операції в цілому, в т.ч. СІО, розглядаються як форма воєнних дій. Останнє фактично унеможливлює проведення СІО контррозвідувального 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 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 [195] визначає, що у ході реалізації стратегічних комунікацій відповідно до компетенції Міністерства оборони та Збройних Сил інформаційні та психологічні операції як складові стратегічних комунікацій (тобто, СІО у контексті нашого дослідження) 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.

Проект Закону України «Про внесення змін до Закону України «Про оборону України» щодо деяких питань підготовки держави до оборони» (реєстр. № 7272), який ми вже згадували у попередньому розділі, покликаний заповнити цю прогалину, розширивши правове поле держави щодо застосування Сил спеціальних операцій ЗС України шляхом створення правових підстав для проведення СІО не тільки в умовах дії правового режиму воєнного стану, але і в мирний час в інтересах підготовки держави до оборони [232]. Така цікава й корисна новація, водночас, не вирішує проблему фактичної відсутності належного правового підґрунтя для проведення СІО силами безпеки відповідно до їх компетенції, в тому числі й з метою протидії деструктивним СІО. Так, в масиві чинного законодавства України наразі відсутні нормативно-правові акти або конкретні норми, які б регламентували порядок правової реалізації зазначеної функції. Наприклад, Закон України «Про Службу безпеки України» не передбачає в числі повноважень вітчизняної спецслужби правообов'язку щодо проведення СІО. Втім, надання відповідних повноважень Службі безпеки України з одночасним позбавленням її статусу військового формування в новій редакції Закону України «Про Службу безпеки України» забезпечило б і дотримання згаданих вище конституційних вимог, і ефективне проведення СІО не лише в інтересах оборони, але в інтересах антитерористичної, антикримінальної, інформаційної та інших складових національної безпеки України. Аналогічні повноваження мають також бути надані і розвідувальним органам України у новому Законі України «Про розвідку», а також іншим суб'єктам сектору безпеки і оборони відповідно до їхньої компетенції.

Все це є безперечно актуальним та необхідним, адже слід враховувати той факт, що негативні інформаційні впливи можуть проводити наряду зі спецслужбами іноземних держав також і терористичні організації, тож слід

звернути увагу й на положення п 3. (с) Резолюції Організації Об'єднаних Націй 51/210 «Заходи щодо ліквідації міжнародного тероризму». Державам пропонувалось, здійснюючи заходи по боротьбі з тероризмом, в 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» [93]. Виконання зазначених вимог, зауважимо, потребує передусім проведення СІО, причому мова йде про проведення СІО в рамках так званої «контрмережної боротьби», зважаючи на мережевий характер сучасного тероризму.

При цьому основними проблемами, що виникають при веденні державної контрмережної боротьби, є наступні:

- ієрархічні державні системи, як правило, є малоефективними у боротьбі з мережними структурами. Це зв'язане насамперед з тим, що час, необхідний для прийняття рішень і адекватного реагування на зміни у безпековому середовищі, в ієрархічних системах значно перевищує аналогічні показники мережних структур;

- ефективна антитерористична боротьба вимагає формування підрозділів з протидії тероризму і злочинності, що будуються на мережній основі, а отже - наділення їх розширеними повноваженнями в питаннях прийняття рішень. Значну роль цьому можуть відіграти технічні нововведення, вироблення нових механізмів міжвідомчого координування, а також розвиток міждержавної кооперації, включаючи, у тому числі, уніфікацію національних законодавчих систем.

Зазначені особливості певним чином визначають потребу як у науковому формуванні алгоритму проведення СІО, так і у нормативному окресленні можливостей його реалізації, передусім у частині суб'єктного складу, зокрема, закріпленні можливостей залучати до проведення СІО недержавні структури, зокрема, ЗМІ або окремих лідерів громадської думки.

Не менш важливим питанням у вдосконалення інформаційно-правового

забезпечення СІО є власне визначення моделі СІО, що може вважатися першим кроком реалізації алгоритму проведення СІО:

- рефлексивна модель, яка акцентує увагу на прогнозуванні поведінки цільових аудиторій інформаційного впливу (так звана «російська модель»);

- модель, запозичена з реклами й піару (так звана «американська модель»), яка акцентує увагу на зміні ставлення до об'єкта;

- модель, котра акцентує увагу на зміні поведінки (так звана «британська модель») [193].

Як зазначає Г.Почепцов, різниця між загаданими моделями полягає у тому, що зміни в ході СІО вносяться у:

- ставлення до об'єкта (американська модель);

- поведінку (британська модель);

- світосприйняття та світоглядну картину (рефлексивна модель).

При цьому рефлексивне управління передбачає застосування наступного набору методів:

- тиск силою (в тому числі «примусова дипломатія», зміст якої полягає у реалізації концепції демонстрації сили – «силу треба демонструвати, щоб у неї повірили»);

- допомога опонентові у формулюванні розуміння вихідної ситуації;

- формування цілей супротивника (або ж – цільової аудиторії як такої);

- формування алгоритму прийняття рішень (власного та цільовою аудиторією);

- обрання вигідного часу для прийняття рішень та нав’язування часу для прийняття рішень [193].

Ще одним важелем впливу у цьому напрямку може вважатися адресація цільовій аудиторії контрольованих інформаційних повідомлень.

На нашу думку, в умовах сучасних гібридних війн та мережної боротьби при проведенні ефективних СІО необхідним є органічне поєднання всіх трьох моделей впливу та формування синергетичної моделі СІО. Водночас, важливим компонентом усіх окреслених трьох підходів, а відповідно – й потенційної синергетичної моделі проведення СІО, - є робота з цільовою

аудиторією, яка передбачає якісне знанні цільової аудиторії, ступеню її очікуваної опірності й можливостей щодо прийняття іншої точки зору. Це, у свою чергу, свідчить про визнання пріоритетом інформаційного забезпечення СІО саме вивчення цільової аудиторії, на чому наголошує Г.Почепцов у згаданій вище праці [193].

Так, перебіг анексії Кримського півострова Російською Федерацією показав, що російська пропаганда спекулювала і продовжує активно спекулювати на соціальних страхах населення Криму, а саме на національній темі, аж до геноциду, загрозі російськомовній спільноті. Окрім теми так званого «потягу дружби», піднятої, між іншим, представником українських націоналістів, а в подальшому народним депутатом, І.Мосійчуком, яку потім активно тиражували та використовували російські засоби масової інформації, розпалювали тему хаосу та безладдя у Києві, поширювались відео-сюжети про побиття та вбивства людей на Майдані під час Революції Гідності тощо.

Разом із тим самопроголошена влада Криму почала відключати від ефіру українські канали, надаючи перевагу мовленню російському мовленню, які висвітлювали події на материковій частині України виключно в негативному ключі. Таким чином російська пропаганда та окупаційна влада звузила обсяг інформаційних джерел виключно до проросійських, тим самим обмежила можливість отримувати інформацію з інших джерел, створюючи необхідну для росіян атмосферу серед населення півострову. Усвідомлюючи соціальний вплив на кримських татар, окупаційна влада також спонукала до закриття кримськотатарський канал ATR.

Під час блокувань та штурмів українських військових частин ватажки так званих «зелених чоловічків» постійно апелювали до того, що в Росії рівень соціального забезпечення військових значно вищий ніж в Україні, а серед населення поширювалась інформація щодо підвищення обсягів соціальних виплат до російських стандартів. Ці дії одночасно направлялися на такі соціальні верстви населення як військові й пенсіонери та маніпулювали їхніми соціальними очікуваннями й потребами. Активно поширювалась інформація серед українських військових стосовно суттєвого підвищення грошового та

матеріального забезпечення у випадку прийняття присяги російським збройним силам.

Крім того, пропагандисти популяризували образ президента Російської Федерації В.Путіна, як захисника та провідника «Руського міру» (рос. - «Русского мира») та «реінкарнацію» Сталіна, образу РФ як сучасного аналогу СРСР тощо. Загалом, можна стверджувати, що чинна російська влада вдало сформувала та розвинула систему політичних міфів і архетипічних паттернів з метою створення образу величі радянської влади та перенесення цього образу на сучасну Росію. Очевидно, що для широкого загалу РФ в інформаційному просторі та на рівні архетипів перетворилась на «СРСР 2.0». У цьому контексті анексія Росією Криму, підтримка так званих ЛНР та ДНР неофіційно сприймається як продовження боротьби з фашизмом та нацизмом, аналогія перемоги над нацизмом у 1945 році.

Наразі ж однією з основних тем, які поширюють російські й проросійські інформаційні ресурси є проблема так званого «націоналізму – націоналсоціалізму - фашизму». Так, продовжується акцентування уваги аудиторії на буцімто використанні українською владою націоналістичних організацій для тиску на політичних опонентів, збільшенні проявів антисемітизму на території України, утисків прав національних меншин з боку української влади та учасників націоналістичних чи інших радикальних рухів, утисків в Україні прав російськомовного населення, угорського населення, інших національних меншин тощо. Значної уваги з боку російських ЗМІ заслуговує тема героїзації й популяризації С.Бандери: демонструються відео, що висвітлюють антисемітські гасла, смолоскипні ходи з нагоди річниці його дня народження, відповідні бігборди, «націоналістичне» виховання у навчальних закладах – від дошкільних до вищих, що здійснюється на загальнодержавному рівні тощо. Надалі матеріали щодо «радикалізації української держави й активізації розвитку фашистсько-націоналістичних рухів в Україні» оприлюднюються через підконтрольні Російській федерації ресурси у США, ФРН, Польщі, Угорщині, та інших країнах. Постійною увагою відповідних ЗМІ користуються також українсько-польські відносини, причому

ЗМІ систематично залучаються російськими спецслужбами до проведення інформаційних акцій, спрямованих на компрометацію українсько-польських відносин. Зокрема, увага аудиторії акцентується на нібито зростанні націоналістичних настроїв в Україні, що ставить під сумнів дружні стосунки Польщею, вказується на погіршення відносин із сусідньою державою внаслідок шляхом штучного роздмухування націоналістичних та праворадикальних настроїв українською владою задля відвернення уваги населення від загострення актуальних проблем соціально-економічного характеру. Крім того, протягом ведення проти України гібридної війни фіксується активізація проведення Російською Федерацією інформаційних кампаній проти Президента, Міністрів внутрішніх справ та оборони, Начальника Генерального штабу ЗС України, керівників правоохоронних й контролюючих структур, в тому числі новостворених Національного антикорупційного бюро, Національного агентства із запобігання корупції, Спеціальної антикорупційної прокуратури, Національної поліції та інших вищих посадовців України. У тенденційних матеріалах, які поширюються російськими ЗМІ, акцент робиться, зокрема, на неефективній боротьбі з корупцією у вищих органах влади, в т.ч. відсутності конкретних фактів притягнення до відповідальності високопосадовців, серед іншого, вказується на те, що керівники відповідних відомств є людьми, які підконтрольні керівництву не лише України, але й західних держав, відтак виконують політичні замовлення, займаючись переслідуванням опозиційних сил тощо. Аналогічними інформаційними акціями супроводжується висвітлення подій на Сході України - російською стороною здійснюється дискредитація керівництва держави, Міністерства оборони та Генерального Штабу ЗС України, окремих військових підрозділів Національної гвардії, Національної поліції чи Збройних Сил України, зокрема, постійно поширюється інформація про те, що українські військові на Донбасі нібито постійно ініціюють бойові дії й активно обстрілюють цивільне населення із забороненого Мінськими домовленостями озброєння, а також про збільшення військової присутності України в районі лінії розмежування, її озброєння та особового складу. При російські медіаресуси наголошують на

тому, що керівництво української держави разом із своїм найближчим оточенням спекулює на темі війни внаслідок особистої зацікавленості в подальшій ескалації конфлікту (ніби то через збагачення на виробництві зброї, закупівлі за кордоном старої військової техніки за схемами «відкатів», відкритті ринків для «чорних трансплантологів» тощо.

Крім того, ЗМІ, в т.ч. й електронними медіа, систематично оприлюднюються матеріали, які демонструють зубожіння українського населення, зокрема й вибіркові опитування та відео-інтерв'ю відповідного змісту представників соціально-вразливих верств населення. Ще однією з провідних тем, яка постійно поширюється російською стороною через підконтрольні медіа-ресурси є популяризація ідей автономізації, федералізації, територіального розколу України тощо одночасно з поширенням міфів щодо етнічних чисток, заміни російськомовного населення Донбасу іншим населенням (мешканцями західних регіонів України, переселенцями з Ізраїлю тощо). На цьому тлі відбувається спроба зміни ідентифікації населення східних регіонів України та Криму, доведення до них інформації про те, що вони буцімто є чужинцями в Україні, втім їх очікують на «історичній батьківщині». Наразі вказана інформаційна стратегія отримує документальну підтримку внаслідок анонсації Російською Федерацією спрощеної процедури отримання російського громадянства для населення Донбасу та кримців, які не проживали на території півострову на момент окупації.

Зауважимо, що у цьому зв'язку істотною проблемою, яка перешкоджає ефективному здійсненню СІО сектором безпеки і оборони України, є неконтрольована інформаційна політика вітчизняних ЗМІ щодо тимчасово непідконтрольних територій. Так, з середини 2014 року український медіадискурс окреслює чітку лінію між «своїми» і «чужими», а серед конфліктно чутливих груп населення ЗМІ позитивно позиціонують учасників антитерористичної операції та операції об'єднаних сил, в той час як внутрішньо переміщених осіб згадують в 1% новинних матеріалів на центральних каналах та 3% - регіональних. Зокрема, за результатами моніторингу, який проводився громадським об'єднанням «Телекритика», у медіа-просторі простежується

умовне відокремлення України загалом від Донбасу як такого, а також подій, що розгортаються на Донбасі, зокрема, гібридної війни, створюючи у пересічного споживача інформації враження про те, що Донбас не є частиною України, а все, що має місце у згаданому регіоні, – це його окрема історія, не вплетена у загальнонаціональний контекст [256].

Цікавими для розуміння сформованих медіа-дискурсом стереотипів населення щодо окремих питань суспільного життя є такі показники дослідження, відповідно до якого 11,4 % українців категорично упереджені щодо внутрішньо переміщених осіб, 48,4 % – помірно упереджені, лояльні – 3,9 %, помірно лояльні – 36,3 %. При цьому формуванні образу «поганого переселенця» значну роль відіграє російська пропаганда, якою активно інспіруються наступні тези: «переселенці створюють конкуренцію на ринку праці та нерухомості, і через це важко знайти хорошу роботу та зростає вартість оренди житла», «з підконтрольних Україні територій Донбасу виїхали лише бандити, а нормальні люди залишаються там жити», «вимушені переселенці відмовляються працювати, їм достатньо тієї допомоги, яку надає держава» тощо. Щодо мешканців окупованих територій у телевізійному просторі досить часто культивується думка, що там залишилися лише проросійськи налаштовані та нелояльні до української влади люди.

Із самого початку збройного протистояння на Сході України і дотепер немає загальновизначеної термінології щодо висвітлення цих подій у медіа-дискурсу українського телебачення. Відтак поняття, що використовуються українськими медіа для описання стану справ у Донбасі та навколо нього, різняться залежно від підтримуваних ними політичних сил і не завжди є точними та загальноприйнятними. Зокрема, базовими залишаються поняття, використовувані щодо ситуації на Сході в офіційному дискурсі української влади. Головним серед них є визначення щодо того, як називати конфлікт на Донбасі - «антитерористична операція», «операція об’єднаних сил», «війна, розв’язана Росією», «гібридна війна» тощо, - адже різні визначення провокують абсолютно різний дискурс. Так, якщо у телевізійному просторі йдеться про «сепаратистів», «ополченців» чи «повстанців», то мається на увазі внутрішній

конфлікт, якщо ж говориться про війну та зовнішню агресію – ситуація зовсім інша [251]. Слід також звернути увагу й на те, що телевізійна риторика, націлена на глядацьку аудиторію в середині країни, може істотно відрізнятися від медіа-продукції, призначеної «на експорт». Характерною для українського медіапростору після початку збройного протистояння на Донбасі є й так звана «мова ворожнечі» або «мова ненависті» з використанням таких термінів, як «ватник», «москаль», «рашист», «лугандон», «колорад» тощо [260].

Наприклад, у 2017 році моніторинг державної комунікаційної політики щодо Донбасу зафіксував наступні тенденції: на тлі пожвавлення протестних настроїв тема Донбасу стала зручним інструментом для критики опозиції та вигідного позиціювання керівництва держави; тема Донбасу лишається заручником з'ясування стосунків всередині коаліційних сил; парламентські сили втягнулися у змагання, чия критика президентського плану реінтеграції Донбасу дошкульніша, щоб не демонструвати відсутність власних справжніх альтернатив. В той же час моніторинг державної комунікаційної політики щодо Донбасу у 2018 році засвідчив, що кожен владний гравець розмовляє зі «своїм» Донбасом, хоча всі повідомлення у телевізійному просторі так чи інакше були розраховані на якнайширшу аудиторію. Відповідні тенденції продовжились і у поточному році у ході президентської виборчої кампанії. При цьому слід констатувати, що у вітчизняному медіа просторі практично відсутні меседжі, звернені до мешканців окупованих територій. Втім з одного боку, громадяни України, які проживають на Донбасі, з точки зору повсякденних інтересів та вимог до влади не відрізняють від мешканців інших регіонів. З іншого - постійна загроза збройного конфлікту зумовлює необхідність не лише адекватного висвітлення у телевізійному просторі теми Донбасу, але й налагодження постійного зворотного зв'язку з його населенням, відсутність якого негативно позначатиметься як на ставленні до донеччан і луганчан із боку інших співвітчизників, а також посилює стереотипи про особливість регіону та очікування його особливого статусу, що навряд чи відповідає довгостроковим державним інтересам [124, 126].

Також слід брати до уваги, що Донбас і Крим належать до тих регіонів

України, в яких інформаційна присутність РФ завжди фіксувалася у вигляді потужного інформаційного впливу, що подекуди набував форм інформаційного тиску. Сьогодні у згаданих регіонах застосовуються класичні інформаційні інструменти рефлексивного впливу, метою якого є формування у об'єктів інформаційного управління контрольованого обсягу поінформованості. На тлі відсутності стабільних громадянських ідентичностей російська меншина та русифікована частина відповідних регіонів України були зорієнтовані на отримання політичної інформації з російських інформаційних джерел, тож Російська Федерація мала там сформовану глядацьку аудиторію, стосовно якої могла активно використовувати найбільш дієвий засіб наочно-образного сприйняття політичної інформації – телевізійного інформаційного впливу [58].

Слід враховувати, що Донбас і Крим продовжують існувати в складному та неоднозначному інформаційному середовищі, основними рисами якого є низький рівень довіри до різних джерел інформації, доступ до російських ЗМІ, а також ЗМІ самопроголошених «республік», «звичка» дивитися російське телебачення, низка претензій до якості та способу подачі інформації українськими медіа, що висвітлюють проблематику конфлікту та загальних процесів на тимчасово непідконтрольних Україні територіях [185].

Водночас, протягом останніх років серед населення України (в тому числі й її тимчасово непідконтрольних територій) спостерігається тенденція до зменшення використання телебачення, радіо та друкованої преси як джерела інформації та до відповідного підвищення активності використання мережі "Інтернет". Схожі тенденції характеризують динаміку ситуації у питанні довіри населення до відповідних типів медіа – до традиційних видів медіа довіра у населення падає, тоді як до інтернет-ресурсів – зростає. Зокрема, відповідно до результатів дослідження, проведеного міжнародною організацією «Репортери без кордонів» («RSF»), 82% українців використовують телебачення, близько чверті – радіо та пресу (28% та 23% відповідно), а інтернет – 67% наших співгромадян [170]. Такі тенденції, з одного боку, є природними в умовах глобалізації та інформатизації суспільства, а з іншого боку – дають привід для занепокоєння, адже діяльність ЗМІ в інтернеті на законодавчому рівні

практично не врегульована, окрім інтернет-сайтів друкованих ЗМІ.

Доречно зауважити, що основна цільова аудиторія інтернет-ресурсів - це молодь віком до 25 років, представники якої легко залучаються до участі у тих чи інших рухах чи об'єднаннях, в тому числі неформальних й навіть криміналізованих. Саме на цю вразливу аудиторію можуть націлюватись СІО іноземних спецслужб, спрямовані на організацію та проведення інформаційних диверсій, метою яких є нанесення репутаційної шкоди та розхитування внутрішньої ситуації в державі (поширення меседжів щодо невдоволення населення чинною українською владою, розшарування українського суспільства на умовні табори: політики-олігархи та ошуканий ними народ, тезисів щодо неспроможності української влади вирішувати нагальні проблеми пересічних громадян, створення поліцейської держави, обмеження свободи слова, політичні переслідування, патріоти – політв'язні нового режиму, проведення дострокових парламентських та президентських виборів, продовження революції, «третього майдану» тощо. Так, в останні роки посилилася тенденція щодо використання соціальних мереж інтернет-простору для здійснення протиправної діяльності на шкоду національним інтересам. Серед ресурсів, учасники яких активно пропагують застосування антиконституційних методів боротьби, сепаратизму, проведення акцій громадської непокори, слід відзначити функціонуючі в мережі «ВКонтакті» групи («Антимайдан» - 420 тис. користувачів; «Юго-Восток/Антимайдан» - 165 тис. осіб, «Молот Правди» - 104 тис. осіб; «Русские онлайн/антимайдан» - 72 тис. та інші). З метою мінімізації зазначених загроз, відповідно до додатку 2 Указу Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» інтернет-провайдерам заборонено надання послуг з доступу користувачам мережі "Інтернет" до ресурсів сервісів «ВКонтакте», «Одноклассники», «Mail.ru» [**Ошибка! Источник ссылки не найден.**]. Також має місце функціонування більше 10 відкритих інтернет-ресурсів (сайтів), що здійснюють деструктивну діяльність на шкоду державній безпеці України у інформаційній сфері. Так, більше 50 спільнот в соціальних

мережах «Вконтакте», «Однокласники», «Facebook» надають інформаційне сприяння квазідержавним утворенням – так званим «ДНР/ЛНР». Головною проблемою є фактичне адміністрування більшості вказаних ресурсів та спільнот з тимчасово окупованої території та Російської Федерації. Всі ці інформаційні ресурси, у тому числі інтернет-видання, інформаційні агенції, блог-платформи тощо, активно використовуються для ідейно-політичного, психологічного та соціального впливу на громадян України з метою їх політичної переорієнтації. У свою чергу, це вимагає проведення українською стороною заходів у відповідь, в тому числі й СІО, спрямованих не лише проти дійсного чи потенційного супротивника у геополітичному протистоянні, але й на відповідні вразливі сегменти вітчизняної цільової аудиторії.

Зокрема, з огляду на поточну ситуацію щодо окупованих частин територій Донецької та Луганської областей, Криму тощо, активної та агресивної діяльності проросійських ЗМІ в регіоні, вважається за доцільне в ході майбутніх СІО не лише підвищувати симпатію місцевого населення до України, а понижувати рівень довіри до РФ і місцевої окупаційної влади загалом і вже на основі отриманого результату розвивати ті чи інші напрямки діяльності. Зменшення рівня довіри населення до органів окупаційної влади спровокує збільшення прямих та опосередкованих витрат на повернення цього рівня через підвищення соціальних витрат, агресивну внутрішню пропаганду, «полювання на відьом» та інші заходи, які будуть направлені як на нівелювання реакції населення на СІО, так і спробу переключити увагу населення на інші резонансні питання.

Проведення таких СІО, як вже зазначалося, потребує попереднього здійснення низки заходів щодо дослідження та визначення психологічних характеристик цільової аудиторії з метою максимальної ефективності психологічного впливу. Окрім цього необхідно визначити соціально-демографічну структуру цільової аудиторії, зони проживання та отримання соціальних послуг, провести загальний соціально-психологічний аналіз із визначенням конкретних «больових точок» свідомості та підсвідомості цільової аудиторії для отримання очікуваного результату СІО. Важливу роль відіграє

коректне та чітке визначення всіх елементів психологічної характеристики цільової аудиторії, без якої ймовірність досягнення кінцевої мети СІО зводиться до мінімуму аж до провалу операції чи отримання зворотної негативної реакції із викриттям та (або) дискредитацією джерел поширення інформації у середовищі цільової аудиторії.

З огляду на необхідність реагування на агресивну політику Російської Федерації, неможливість надання симетричної відповіді з боку України, кризову ситуацію в економіці РФ, варто перейти до тактики асиметричних відповідей на агресію зі сторони північно-східного сусіда. Створення та розвиток джерела напруги та невдоволення соціальною політикою окупаційної влади на території півострову здатне створити розкол як у російському суспільстві (наприклад, через збільшення об'єму дотацій з федерального бюджету), так і серед кримської спільноти (когнітивний дисонанс між очікуваннями та реаліями), що, у свою чергу, викличе одночасно ланцюгову та циклічну реакцію – більше дотацій, більше незадоволення, ще більше дотацій, ще більше незадоволення тощо. Разом із неофіційним фінансуванням так званих ДНР та ЛНР, скороченням надходжень до бюджетів усіх рівнів, веденням бойових дій у Сирії, створенням додаткового навантаження на фінансову та соціальну системи Росії можна поглибити фінансову кризу та посилити соціальну напругу у російському суспільстві. У якості інструментарію можуть бути задіяні різні державні та неурядові структури як в Російській Федерації так і за її межами, засоби масової інформації, громадські, націоналістичні, право-радикальні, гуманітарні, релігійні організації (у тому числі релігійні культи, течії та окремі представники церкви), партії та рухи, об'єднання громадян (ультрас, байкери), представники народної (публічної) дипломатії, вразливі, незахищені верстви населення (молодь, біженці, переселенці з тимчасово окупованих територій), діячі культури та мистецтв, науковці, громадські активісти, а також інші суб'єкти так званої «м'якої сили» («soft power»). Втім на напрямах вдосконалення інформаційно-правового забезпечення СІО детальніше буде доцільно зосередитись у наступному підрозділі дисертаційного дослідження.

3.3. Напрями вдосконалення правового забезпечення спеціальних інформаційних операцій

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.

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.

У свою чергу, як вже зазначалося, визначення спектру методів проведення СІО залежатиме від обраної моделі СІО. У попередньому підрозділі цього дослідження 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) [139]. Піддаючи аналітичному розгляду кожну з них (в нашому випадку – виокремлені Г.Почепцовим традиційні моделі СІО [193]), надалі можемо одержати загальний висновок за допомогою операції інтегрування [180, 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» [27], пов'язаної з трансформацією поглядів на характер загроз у новому столітті. Сутність нового усвідомлення загроз полягає в тому, що наразі основна загроза виходить не від регулярних армій різних країн, а від усіляких терористичних, кримінальних і інших організацій, учасники яких об'єднані у мережні структури. Подібні організації не мають чіткої ієрархічної підпорядкованості, найчастіше в них немає єдиного керівництва, вони координують свою діяльність із використанням засобів глобальних комунікацій. Відмінною рисою таких структур є наявність єдиної стратегічної мети й відсутність чіткого планування на тактичному рівні. Для позначення подібних структур з'явився спеціальний термін «сегментована, поліцентрична, ідеологізована мережа» («Segmented, Polycentric, Ideologically integrated Network» - SPIN). В умовах впливу подібних загроз змінюються роль і місце СІО у системі забезпечення національної безпеки, адже більшою мірою акцент робиться на проведення невоєнних операцій (Operation Other Then War), що вимагає тісної взаємодії з недержавними організаціями й структурами. Фактично, мережна/контрмережна боротьба переводить інформаційну перевагу в «бойову міць», ефективно пов'язуючи інтелектуальні об'єкти в єдиний інформаційний простір забезпечення національної безпеки або, якщо мова йде про військові дії, у бойовий простір. До нього, крім традиційних цілей для ураження звичайними видами озброєнь, включені також і цілі, що лежать у віртуальній сфері: емоції, сприйняття й психіка супротивника. Вплив на нові класи цілей досягається за рахунок тісної інтеграції мережних структур сектору безпеки і оборони й мережних структур громадянського суспільства (як сукупності суспільних об'єднань, відповідальних за вироблення «суспільної думки»). 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 [65-66, 86, 94, 254, 257]. Зауважимо, що в даному випадку з урахуванням змісту підрозділу 3.1 цього дослідження 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 іноземними 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 суспільно-політичної 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 [80, 183] (Таб.1):

Таблиця 1. Огляд безпекового середовища проведення СІО з використанням SWOT-аналізу

Аналіз внутрішніх факторів		*Аналіз зовнішніх факторів*	
Сильні сторони	**Слабкі сторони**	**Можливості**	**Загрози**
Strengths	**Weaknesses**	**Opportunities**	**Threats**
S	**W**	**O**	**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 інформаційно-аналітичних 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 числа журналістів, громадських діячів, політиків, державних службовців, представників правоохоронних органів та фінансово-промислових груп; підконтрольні іноземним державам або кримінальним структурам медіа-холдинги, 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. На цьому ж етапі необхідно ретельно дослідити цільову аудиторію СІО (Додаток В).

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.

Теоретично пошук або створення інформаційного приводу для проведення СІО може розглядатися як стадія підготовчого етапу, адже ця стадія характеризує процес підготовки до безпосереднього проведення СІО, втім пропонуємо розглядати це як самостійний етап алгоритму проведення СІО - інформаційний,- якому притаманне не лише самостійне змістовне навантаження, але й активні дії, що виходять за межі обробки та аналізу інформації.

Отже, під час пошуку або створення інформаційного приводу для проведення СІО необхідно з'ясувати передумови для проведення інформаційних впливів, зокрема, визначити вразливі місця у без пековому 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 пощо, - 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 тригеру залежить 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. Зокрема, у теорії нейро-лінгвістичного програмування передбачається можливість керування настроями цільової аудиторії залежно від емоцій та переходу від одного емоційного стану до іншого разом з використанням емоційного настрою з метою спонукання аудиторії до дії чи бездіяльності відповідно до задуму організаторів інформаційно-психологічного впливу. Так, існує матриця референтних станів соціальних мас, яка складається з чотирьох частин, а саме: пасивний негатив, пасивний позитив, активний негатив, активний позитив. Активний емоційний стан штовхає аудиторію до дій чи бездіяльності, тоді як пасивний емоційний стан лише виражає емоційне відношення. Завдання організаторів СІО – визначити в ході підготовчого етапу домінантний тип емоційного стану цільової аудиторії, а у випадку відсутності можливості - під час інформаційного етапу здійснити комплекс інформаційних акцій, які створять необхідний емоційний стан або підсилять наявний емоційний стан, необхідний для подальшого проведення СІО.

У свою чергу, 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.

Безпосередній зміст заходів, які планується здійснити в ході проведення СІО, залежатиме від її типу й спрямування.

Так, первісно О. Литвиненко у своїй роботі 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 диксредитуючих 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) [148-151].

В сучасних умовах доречно 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, спрямована 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 протесних 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» [31]. 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 [166]. 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 опертивно-

прикладного характеру [194]. 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 умовиводів і заключень 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 характеру 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 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 (ці методи детально розглядалися у підрозділі 3.1. цього дослідження). 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 (Додаток Д).

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 (Додаток Е) 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 (Додаток Ж).

ВИСНОВКИ ЗА РОЗДІЛОМ

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

Основною проблемою інформаційно-правового забезпечення СІО в умовах

сьогодення є відсутність достатнього законодавчого унормування їх проведення. Відповідно, відсутнє й достатнє законодавче підґрунтя для розробки методологічних засад інформаційного забезпечення СІО. Це передусім зумовлює потребу у законодавчому визначенні заборон при здійсненні інформаційного впливу, в тому числі в ході проведення СІО, які визначатимуть межі їх проведення, адже в Україні, як у демократичній правовій державі, діяльність державних органів влади, відповідальних за забезпечення національної безпеки має організовуватись на нормах закону, які забезпечують реалізацію конституційних прав та свобод громадян.

Оскільки спеціальні операції в цілому, в т.ч. СІО, наразі розглядаються за законодавством України як форма воєнних дій, фактично унеможливлюється проведення 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 - хоча цими категоріями не вичерпується коло осіб, причетних до протиправних дій; так, як потенційна «аудиторія» СІО можуть розглядатися, наприклад, також учасники організованих злочинних угруповань), а також проведення СІО на території України поза межами території, на якій введено правовий режим воєнного стану, поза межами району проведення антитерористичної операції або інших місць (районів) підготовки та застосування Збройних Сил. Втім як розвідувальний, так і контррозвідувальний аспект СІО проявляється на всіх етапах СІО незалежно від їх спрямування, «наступального» (розвідувального) або «оборонного» (контррозвідувального) характеру. Тож питанням нагальної необхідності 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 не лише в інтересах оборони, але в інтересах антитерористичної, антикримінальної, інформаційної та інших складових 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, що надалі надасть можливість розробити ефективну модель та алгоритм 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 сладової 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 підґрунтя для інформаційно-правового забезпечення проведення СІО. Необхідно зауважити, що інформаційно-правове забезпечення СІО обов’язково має здійснюватись з дотриманням основоположних принципів права – справедливості, пропорційності і гуманізму (що відповідає принципам міжнародного гуманітарного права, яке застосовується у регулюванні

військових конфліктів), а також таких загальних принципів інформаційного права, як: законність; забезпечення інформаційної безпеки; рівність громадян перед законом; комплексність відносин в інформаційній сфері. Щодо інших загальних принципів інформаційного права – принципу свободи доступу до інформації та свободи висловлення думок та переконань, підкреслимо, що їх реалізація має співвідноситись з дотриманням принципу конфіденційності, реалізація якого є необхідною у правовідносинах щодо забезпечення національної, в т.ч. інформаційної безпеки, а також підпорядковуватись реалізації вже згаданого принципу забезпечення інформаційної безпеки [123]. На нашу думку, має обов'язково дотримуватись також принцип правової визначеності.

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.

В сучасних умовах СІО доречно типологізувати наступним чином: СІО, об'єктом (ціллю) яких є конкретна особа або визначене коло осіб (суб'єкти прийняття рішень або інші особи, які мають певний авторитет); СІО, спрямована на ініціювання, зміну напрямку розвитку, припинення чи «розмиття» певного процесу, явища чи події; «Спін-операції», які спрямовуються на формування дискурсу та створення «вікон Овертона». Така 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: 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. Запропонована класифікація СІО за типом і видом, а також системний підхід до планування та підготовки СІО на базі відповідного

алгоритму, слугує підґрунтям для побудови матриці інформаційно-правового забезпечення синергетичної моделі СІО, застосування якої складовими сектору безпеки і оборони України дозволить підвищити ефективність інформаційно-правового забезпечення СІО та сприятиме підвищенню їх результативності.

ВИСНОВКИ

За результатами проведеного дослідження, на підставі аналізу здобутків науки адміністративного, інформаційного, воєнного тощо права, законодавства України, зарубіжного досвіду напрацювання інформаційно-правових засад забезпечення проведення СІО, здійснено теоретичне узагальнення та запропоновано нове вирішення наукового завдання щодо теоретичного визначення, обґрунтування й розкриття сутності правового забезпечення СІО, а також напрацьовані теоретичні засади інформаційно-правового забезпечення СІО відповідно до потреб сектору безпеки і оборони України.

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

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

2. Визначено, що понятійно-категоріальний апарат дослідження питань правового забезпечення СІО характеризують такі категорії інформаційного права:

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

стану захищеності;

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

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

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

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

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

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

3. З’ясовано, що методологія дослідження правового забезпечення СІО, як головний орієнтир наукового пошуку, становить систему методів (способів і прийомів), а також сукупність принципів, застосування яких уможливлює одержання нових знань щодо організації та проведення СІО. Особливу роль у дослідженні відіграє тензорна методологія, яка дозволяє обґрунтовано пов’язувати

процес і структуру, що набуває особливого значення для організації та проведення СІО як складової системи стратегічних комунікацій. Застосування тензорної методології дозволяє поширити на СІО закономірності здійснення стратегічних комунікацій.

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

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

6. Розкрито, що теоретико-методологічні засади інформаційного забезпечення СІО характеризуються розгалуженим інструментарієм, який може використовуватись як у військовий, так і у мирний час для різної цільової аудиторії. Взяття сектором безпеки і оборони України «на озброєння»

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

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

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

- у проекті Закону України Про внесення змін до Закону України "Про Службу безпеки України" та у проекті Закону України «Про розвідку» визначити серед функцій Служби безпеки України та розвідувальних органів «участь у забезпеченні загальнодержавної системи стратегічних комунікацій», передбачити серед повноважень Служби безпеки України наступне: «проводити спеціальні інформаційні операції; протидіяти проведенню проти

України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій», а серед повноважень розвідувальних органів України - «проводити спеціальні інформаційні операції з метою сприяння реалізації національних інтересів України та протидії зовнішнім загрозам національній безпеці України у визначених законом сферах»;

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

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

Також результати проведеного дисертаційного дослідження дозволяють

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Air Force Doctrine Document: 2-5.Information operations, 2005. URL: http://www.iwar.org.uk/iwar/resources/usaf/afdd2-5-2005.pdf (дата звернення 02.02.2019)

2. AJP-3.10 Allied Joint Doctrine for Information Operations, Sept.2014. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (дата звернення 02.06.2019)

3. AJP-3.4.4 Allied Joint Doctrine for Counterinsurgency (COIN), Jul.2016. URL: https://www.gov.uk/government/publications/allied-joint-doctrine-for-counter-insurgency-coin-ajp-344a (дата звернення 02.06.2019)

4. AJP-3.9 Allied Joint Doctrine for Joint Targeting, Apr.2016. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/628215/20160505-nato_targeting_ajp_3_9.pdf (дата звернення 02.06.2019)

5. AJP-5 Allied Joint Doctrine for Operational-Level Planning, Jun.2013 URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/393699/20141208-AJP_5_Operational_level_planning_with_UK_ elements.pdf (дата звернення 03.06.2019)

6. Alberts D., Garstka J., Hayes R., Signori D. Understanding Information Age Warfare. *CCRP Publication Series.* Aug.2001

7. An Assessment of International Legal Issues in Information Operations. - Department of Defense, Office of General Counsel. May,1999. URL: http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf (дата звернення 03.01.2019).

8. Andreas F. Lowenfeld. Trade Controls for Political Ends. 1983. p. 313

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

10. Arquilla J., Ronfeldt D., The Advent of Netwar, 1996. p. 15

11. BS 7799-2: аудит и сертификация. URL: https://www.osp.ru/ os/2007/

03/4158303/ (дата звернення 27.01.2019).

12. Clinton E. Cameron. Developing a Standard for Economically Related State Economic Action II Michigan Journal of International Law.Vol. 13, 1991. p. 230

13. Consultation, command and control board, AC/322-D(2016)0017, 14 March 2016. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_ 08/ 20180801_180801-ac322-d_2016_0017-c3t.pdf (дата звернення 05.05.2019)

14. Control Objectives for Information and related Technology, v. 4.1. URL: https://www.itexpert.ru/rus/biblio/cobit/ (дата звернення 27.01.2019)

15. Cyber defence / Офіційний сайт Організації Північноатлантичного договору / Організація Північноатлантичного договору. URL: http://www.nato. int/cps/en/natohq/topics_78170.htm. (дата звернення 29.01.2019)

16. Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO). URL: www.statewatch.org/ news/2006/sep/nato-sec-classifications.pdf (дата звернення 28.12.2018)

17. Douglas Waller, Onward Cyber Soldiers II Time, Aug. 21, 1995. p. 37

18. Fadok D. S, Boyd J., Warden J.: Air Power Quest for Strategic Paralysis. *A Thesis presented to the faculty of the School of Advanced Airpower Studies.* Air University. Maxwell Air Force Base, Alabama, June 1994. p.28-43

19. Garigue R. Information Warfare. Developing a Conceptual Framework. *Management Analytics and Others.* 1995. p. 18

20. Goldgeier, J. The Future of NATO. *NATO Science for Peace and Security Series, E: Human and Societal Dynamics.* Amsterdam : IOS Press, 2011. Vol. 76. p. 1–12

21. Harold Lasswell. Propaganda Technique In The World War. New York, 1938. p.10-12

22. ICJ Reports 1949, p. 34-35

23. Iran’s Cyber Warfare. URL: https://www.slideshare.net/HackRead/irans-cyber-war-skills (дата звернення 19.04.2019)

24. J. Lee Thompson. Fleet Street Colossus: The Rise and Fall of Northcliffe, 1896–1922. p. 116

25. Joint publication: 3-13. Information operation, 2006. URL: http://www.

acqnotes.com/Attachments/Joint%20Publication%203-13%20Information%20Operations%2013%20Feb%2006.pdf (дата звернення 02.02.2019)

26. Joint publication: 3-13. Information operation, 2012. URL: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (дата звернення 02.02.2019)

27. Joint Vision 2020. URL: http://pentagonus.ru/doc/JV2020.pdf (дата звернення 12.05.2019)

28. Keeton, Pamela & McCann, Mark. (2005). Information Operations, STRATCOM, and Public Affairs. Military Review. URL: www.au.af.mil/au/awc/awcgate/milreview/keeton.pdf (дата звернення 05.02.2019)

29. Kempf, A. Considerations for NATO Strategy on Collective Cyber Defense. URL: http://csis.org/blog /considerations-nato-strategy-collective-cyberdefense (дата звернення 02.02.2019)

30. Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, Information Warfare and International Law. National Defense University, Institute for National Strategic Studies. Wash.: CCRP, 1997. XIX. p. 41-45

31. Nathan J. Russell An Introduction to the Overton Window of Political Possibilities. URL: https://www.mackinac.org/7504 (дата звернення 12.05.2019)

32. NATO Bucharest Summit Declaration, 3 April 2008. URL: http://www.nato.int/docu/pr/2008/p08-049e.html (дата звернення 28.12.2018).

33. NATO Lisbon Summit Declaration, 20 Nowember 2010. URL: http://www.nato.int/docu/pr/2010/p10-049e.html (дата звернення 28.12.2018).

34. NATO Strategic Communications Policy (2009). URL: http://info.publicintelligence.net/ NATO-STRATCOM-Policy.pdf (дата звернення 03.02.2019)

35. NATO Warsaw Summit Communiqué, 9 July 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата звернення 03.01.2019)

36. Norman Menachem Feder, Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack. *NYU, Journal of International Law and Politics*. Vol. 19. p. 410

37. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. URL: http://www.nato.int/ lisbon2010/strategic–

concept–2010–eng.pdf (дата звернення 28.12.2018)

38. Ralf Bedrath. Die Informations revolution und ihre Rezeption im strategischen Denken der USA. URL: http://www.infowar.de (дата звернення 08.11.2018)

39. Richard Szafranski. A Theory of Information Warfare: *Preparing for 2020 II Airpower Journal*. Spring 1995. p. 27

40. Richard W Aldrich. The International Legal Implications of Information Warfare. *INSS Occasional paper 9, Information warfare series*. April 1996. p. 34.

41. Robert L. Heath. Encyclopedia of Public Relations. 2005. p. 1067

42. STANAG 4586 – Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability. URL:https://www.sto.nato.int/publications/ STO% 20Educational%20Notes/STO-EN-SCI-271/EN-SCI-271-03.pdf

43. Strategy for operations in the information environment. Department of Defense, 2016. 20 p.

44. Telecommunications Act of 1996. URL: https://transition.fcc.gov/ Reports/ tcom1996.pdf (дата звернення 22.01.2019).

45. The Digital Millennium Copyright Act (DMCA). URL: https://www.copyright.gov/legislation/dmca.pdf (дата звернення 18.01.2019)

46. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. URL: https:// it.ojp.gov/privacyliberty/authorities/statutes/1281 (дата звернення 22.01.2019)

47. US Department of Defense: Memorandum for secretaries of the military departments. Strategic Communication and Information Operations in the DoD. URL: https://pdnetworks.files.wordpress.com/2011/01/2011-strategic-communication-io-memo-25-jan2011.pdf (дата звернення 02.02.2019)

48. IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі. URL: https://zakon.rada.gov.ua/laws/show/995_222 (дата звернення 18.01.2019)

49. Академічний тлумачний словник української мови (1970-1980). URL: http://sum.in.ua (дата звернення 03.08.2018)

50. Араньев А.С. Анализ развивающегося понятия. Наука, 1965. 444 с.

51. Арутюнян Г. Информационные операции: история и современность. URL:

http://www.noravank.am/rus/issues/detail.php?ELEMENT_ID=13489 (дата звернення 03.12.2018)

52. Арутюнян Г. Распад «системы» и формирование будущего. URL:http://docplayer.ru/42681829-Gagik-arutyunyan-raspad-sistemy-i-formirovanie-budushchego-na-osnove-lekciy-prochitannyh-v-letnih-shkolah-fonda-noravank.html (дата звернення 28.11.2018)

53. Арутюнян Г., Гриняев С., Арзуманян Р. Информационные войны новой формации. URL: http://www.noravank.am/rus/issues/ detail.php? ELEMENT_ ID=15064 (дата звернення 29.11.2018).

54. Ахмадуллин В.Р. США больше не намерены «давить на психику» противника. Пентагон официально объявил об отказе от устоявшегося термина. *Независимое военное обозрение.* 2011. 28 янв.

55. Баранов О. Віртуальність і правове регулювання. *Публічне право.* № 1 (25). 2017. С. 210-218.

56. Барт Р. Миф сегодня. *Мифологии.* М.: Изд-во Сабашниковых, 1996. 312 с.

57. Бернейс Э. Пропаганда. Москва: Hippo Publishing LTD, 2010. 176 с.

58. Більш ніж третина жителів Південного Сходу України розчарувалася в російських ЗМІ – опитування. URL: http://ua.interfax.com.ua/ news/political/ 256212.html (дата звернення 12.03.2019)

59. Бондар І.Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation.* 2014. № 1. С. 68-75

60. Брусницин НА. Информационная война и безопасность. М.: Вита-Пресс, 2001. С. 9

61. Будылин К.Ю. Информационное противоборство в военной сфере (политологический анализ): дисс. … канд. полит. наук. М., 2009. 169 с.

62. Букреев И.Н. Социальные аспекты информационной безопасности. *Информационное общество*. 1998. № 1. С. 42.

63. Буркин А.И., Возженников А.В., Синеок Н.В. Национальная безопасность России в контексте современных политических процессов. Издание второе, дополненное / Под общ. ред. А.В. Возженикова. М.: Изд-во РАГС, 2008. 480 с.

64. Быстрицкий А. Возрождение вида: «Гражданская журналистика против

«профессиональной»: кто и как влияет на самосознание общества. *Власть*. № 19(1124), 2015. С.26

65. Василенко И.А. Геополитика современного мира. URL: https://studme.org/158407205825/politologiya/ geopolitika_sovremennogo_mira (дата звернення 10.04.2019)

66. 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)

67. Вилко В. М. Інформаційно-психологічне забезпечення ЗС США в локальних війнах і збройних конфліктах 1950–2000 рр. (історичний аспект): дис. … канд. іст. наук. К., 2005. 284 с.

68. Военная доктрина Российской Федерации. URL: https://rg.ru/ 2014/ 12/30/doktrina-dok.html (дата звернення 28.01.2019).

69. Военный энциклопедический словарь. М.: Оникс 21 век, 2002. 1432 с.

70. Вопросы Министерства обороны Российской Федерации: Указ Президента РФ от 16.08.2004 № 1082 (в ред. от 26.01.2019). URL: http://www.consultant.ru/document/cons_doc_LAW_48879/ (дата звернення 29.01.2019)

71. Гаазька конвенція про захист культурних цінностей у випадку збройного конфлікту. URL: https://zakon.rada.gov.ua/laws/show/995_157 дата звернення 18.01.2019)

72. Гавра Д.П. Социально-коммуникативные технологии: сущность, структура, функции. URL: http://www.studmed.ru/download/gavra-dp-socialno-kommunikativnye-tehnologii-suschnost-struktura-funkcii-statya_197c941406e.html (дата звернення 13.02.2019)

73. Гаптєєва О. Міжнародна інформаційна безпека – ключовий напрям діяльності Шанхайської організації співробітництва: 2006-2017 рр. URL: https://doi.org/10.24919/2519-058x.4.111226 (дата звернення 18.01.2019)

74. Гарев В.А. Информационная борьба с международным терроризмом: теоретические и практические аспекты: дисс. … канд. полит. наук. М., 2007.

293 с.

75. Гаспаров М. Занимательная Греция. Рассказы о древнегреческой культуре. М.: Новое литературное обозрение, 1995. 382 с.

76. Гафуров В.Р. Анализ методов ведения информационной войны по Донскому М.В. URL: elar.urfu.ru/bitstream/10995/50786/1/978-5-8019-0294-4_2012_310.pdf (дата звернення 23.01.2019).

77. Горбенко А. Н. Информационное противоборство в политике современных государств: автореф. дис. ... канд.полит.наук.. М., 2008. 19 с.

78. Горбенко І.Д., Долгов В.І., Гріненко Т.О. Інформаційна війна – сутність, методи та засоби ведення. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Матеріали ювілейної науково-технічної конференції.* К., 1998. С. 36-40.

79. Горбулін В .П., Качинський А.Б. Системно-концептуальні засади стратегії національної безпеки України: монографія. К., 2007. 592 с.

80. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки: монографія. К.: НІСД, 2010. 288 с.

81. Горбулін В.П., Качинський А.П. Засади національної безпеки України: підручник. К.: Інтертехнологія, 2009. 272 с.

82. Гордиенко Д.В. Информационное противоборство в военном конфликте. *Право и политика*. 2000. №10. С. 74-82.

83. Грешневиков А. Информационная война. М.: Русскій міръ, Рыбинск: Рыбынское подворье, 1999. 400 с.

84. Гриняев С.Н. Война в четвёртой сфере. *НВО.* 2000. № 42. С. 7

85. Гриняев С.Н. Поле битвы – киберпространство. *Теория, приемы, средства, методы и системы ведения информационной войны*. М., 2004. 428 с.

86. Гриняев С. “Сетевая война» по-американски. URL: nvo.ng.ru/wars/2002-02-16/10_americanwar.html (дата звернення 13.04.2019)

87. Губарев А.Б. Информационные войны как объект политологического исследования: дис. ... канд. полит. наук. Уссурийск, 2005. 170 с.

88. Дебор Ги Э. Общество спектакля. М.: Логос, 1999. 224 с.

89. Декларация о недопустимости интервенции и вмешательства во

внутренние дела государств. URL: https://undocs.org/ru/A/RES/36/103 (дата звернення 13.01.2019).

90. Декларація ООН про неприпустимість втручання у внутрішні справи держав, про захист їх незалежності та суверенітету. URL: https://zakon.rada.gov.ua/laws/show/ru/995_818 (дата звернення 13.01.2019).

91. Декларація про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй. URL: https://zakon.rada.gov.ua/laws/show/995_569 (дата звернення 07.01.2019)

92. Декларація про свободу комунікацій в Інтернеті. URL: https://cedem.org.ua/library/deklaratsiya-pro-svobodu-komunikatsij-v-internet/ (дата звернення 18.01.2019)

93. 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 14.04.2019)

94. Деньщиков А. Л. Информационная стратегия США (анализ, стратегия, перспективы): дисс. ... канд. педаг. наук. М, 2008. 186 с.

95. Дерюжинский В. Ф. Полицейское право: пособие для студентов. СПб: Сенатская типография, 1908. 524 с.

96. Директива 2000/31/ЄС Європейського парламенту та Ради "Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку" (Директива про електронну комерцію). URL: https://zakon.rada.gov.ua/laws/show/994_224 (дата звернення 22.01.2019).

97. Директива 97/66/ЄС Європейського Парламенту і Ради "Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі". URL: https://zakon.rada.gov.ua/laws/ show/ 994_243 (дата звернення 22.01.2019)

98. Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла. URL: https://zakon.rada.gov.ua/laws/show/995_480. (дата звернення 15.01.2019).

99. Додонов А.Г. Распознавание информационных операций/ А.Г. Додонов, Д.В. Ландэ, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Грайворонская. К.: ООО «Инжиниринг», 2017. 282 с.

100. Донсков Ю.Е., Никитин О.Г. Место и роль специальных информационных операций при разрешении военных конфликтов. URL: http://militaryarticle.ru/voennaya-mysl/2005-vm/9555-mesto-i-rol-specialnyh-informacionnyh-operacij-pri (дата звернення 20.11.2018)

101. Егорова-Гантман Е. В тумане войны. Наступательные военные коммуникативные технологии. М.: «Никколо М», 2010. 432 с.

102. Егорова-Гантман Е., Плешаков Н. Политическая реклама. М.,1999. 240 с.

103. Жабчик С.В., Токарев К.К. Информационная война как катализатор геополитических изменений. URL: https://elibrary.ru/download/ elibrary_ 35236659_69242074.pdf (дата звернення 30.11.2018)

104. Жарков Я.М. Інформаційно-психологічний вплив на війська та населення противника (1939- 2000рр.) : дис... канд. іст. наук. К., 2007. 211с.

105. Женевська конвенція про захист цивільного населення під час війни. URL: https://zakon.rada.gov.ua/laws/show/995_154 дата звернення 18.01.2019).

106. Женевська конвенція про поводження з військовополоненими. URL: https://zakon.rada.gov.ua/laws/show/995_153 дата звернення 18.01.2019).

107. Завальний А.М. Юридичні факти в сфері здійснення правоохоронної діяльності: дис. … канд. юрид. наук. К., 2007. 167 с.

108. Законы Ману: Манав-дхармашастра. Ману-Самхита. М.: ЭКСМО-Пресс, 2002. 497 с.

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

110. Золотухін Д. Ю. Біла книга спеціальних операцій проти України, 2014 – 2018. К., 2018. 384 с.

111. Иванов Д.В. Общество как виртуальная реальность. *Информационное общество: Сборник материалов.* М.: ООО Издательство АСТ, 2004. С. 355-363

112. Интервью А.Венедиктова с К.Пауэллом на радиостанции «Эхо Москвы», 15.05.2003. URL: http://www.echo.msk.ru/programs/ beseda /

22183.phtml (дата звернення 08.02.2019)

113. Информационная война против Российской Федерации: институализация информационного противоборства. *Материалы круглого стола (30 ноября 2010 г.).* М.: Науч. эксперт, 2011. 109 с.

114. Информационные вызовы национальной и международной безопасности. URL: www/pricentr.org|media/content/files/9/13464042510/pdf

115. Информационные технологии – практические правила управления информационной безопасностью. Международный стандарт (ISO/IEC 17799): . URL: http://www.kmgep.kz/data/filedat/default/ISO_IEC_17799_2000_rus.pdf (дата звернення 27.01.2019)

116. Казаковцев А.В. НАТО и кибербезопасность. *Вестн. Волгогр. гос. ун-та. Сер. 4, Ист.* 2012. № 2 (22). С.109-114

117. Калюжний Р. Питання концепції реформування інформаційного законодавства України. *Правове, нормативне та метрологічне забезпечення системи інформації в Україні: Тематичний збірник праць учасників Другої науково-технічної конференції.* - К., 2000. - С.17-21

118. Караяни А. Г. Слухи как средство информационно-психологического противодействия. *Психологический журнал.* 2003. С.47-55

119. Кассирер Э. Техника современных политических мифов. *Вестник МГУ. Сер. 7. Философия.* 1990. № 2. С. 58-65

120. Клаузевиц К. О войне. URL:http://militera.lib.ru/science/clausewitz/index.html (дата звернення 05.10.2018)

121. Климчук А. Информационная и кибербезопасность в современном мире: опыт СБУ. URL: https://www.liga.net/politics/opinion/informatsionnaya-i-kiberbezopasnost-v-sovremennom-mire-opyt-sbu (дата звернення 27.11.2018)

122. Коваленко Л.П. Принципи інформаційного права. *Державне будівництво та місцеве самоврядування.* № 23. 2012. С. 185-195

123. Ковтун Н.А., Мухин В.И., Набока Ю.И., Чумаров И.С. Основные категории информационной борьбы. *Вопросы защиты информации.* 2001. №2. С. 2-7

124. Кожен владний гравець розмовляв зі «своїм» Донбасом. URL:

https://detector.media/infospace/article/ 137267/2018-05-07-kozhen-vladnii-gravets-rozmovlyav-zi-svoim-donbasom/ (дата звернення 10.03.2019)

125. Комов С.А. О способах и формах ведения информационной борьбы. *Военная мысль.* 1997. № 4. С.18-22

126. Комунікація з Донбасом: боротьбя «яструбів» та «голубів» у владі. URL: https://detector.media/monitoring/ article/128073/2017-07-18-komunikatsiya-z-donbasom-borotba-yastrubiv-ta-golubiv-u-vladi/ / (дата звернення 10.03.2019)

127. Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію. URL: https://zakon.rada.gov.ua/ laws/ show/995_266 дата звернення 18.01.2019)

128. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/ show/994_575 (дата звернення 20.01.2019)

129. Конвенція про міжнародну організацію морського супутникового зв'язку (ІНМАРСАТ). URL: https://zakon.rada.gov.ua/laws/show/995_017 (дата звернення 15.01.2019)

130. Конвенція про поліпшення долі поранених і хворих у діючих арміях. URL: https://zakon.rada.gov.ua/laws/show/995_151 дата звернення 18.01.2019)

131. Конвенція про поліпшення долі поранених, хворих та осіб, які зазнали корабельної аварії, зі складу збройних сил на морі. URL: https://zakon.rada. gov.ua/laws/show/995_152 дата звернення 18.01.2019).

132. Конвенція, що засновує Європейську Організацію Супутникового Зв'язку "EUTELSAT». URL:https://zakon.rada.gov.ua/laws/show/994_578 (дата звернення 15.01.2019)

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

134. Концепція (основи державної політики) національної безпеки України: схвалена Постанової Верховної Ради України від 16.01.1997 № 3/97-ВР. URL: http://zakon.rada.gov.ua/laws/ show/3/97-%D0%B2%D1%80 (дата звернення 10.11.2018)

135. Коротченко Е.Г. Информационное противоборство в операциях

общевойсковых объединений: лекция. М.: ВАГШ, 1999. 41 с.

136. Костин Н.А. Теория информационной борьбы. М., ВАГШ, 1996. 380 с.

137. Коцюбинская Л.В. Понятие «информационная война» в современной лингвистике: новые подходы. URL: https://cyberleninka.ru/article/n/ponyatie-informatsionnaya-voyna-v-sovremennoy-lingvistike-novye-podhody(дата звернення 13.11.2018)

138. Красноступ М.Д. Інформаційна війна – міфи чи реальність? *Інформаційні технології та захист інформації*. 1999. №1. С. 111-136

139. Крон Г. Исследование сложных систем по частям - диакоптика. М.: Наука, 1972. 544с.

140. Крылов Г.О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации: дисс. ... канд. юрид. наук . М, 2007. 327 с.

141. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт)/ под общ. ред. А.Е. Тараса. Мн.: Харвест. 1999. 448 с.

142. Кубышкин А.В. Международно-правовые проблемы обеспечения информационной безопасности государства: дисс. ... канд. юрид. наук. URL: http://diss.rsl.ru/diss/03/0509/030509026.pdf (дата звернення 10.11.2018)

143. Кузнецов П.А. Информационная война и бизнес. *Конфидент.* 1996. № 4. С. 21-23

144. Кусова Е.А. Информационно-правовое обеспечение государственного управления. *Вестник ТГУ*. выпуск 4 (96), 2011. С.292-295

145. Кушнір О.В. Поняття та сутність стратегічних комунікацій у сучасному українському державотворенні. URL: http://goal-int.org/ponyattya-ta-sutnist-strategichnix-komunikacii-u-suchasnomu-ukrainskomu-derzhavotvorenni/ (дата звернення 04.12.2018)

146. Лебедев С.Д. Мифотворчество как социокультурный фактор функционирования со временного технического знания: автореф. дисс. … канд. соц. наук. Белгород, 1996. 22 с.

147. Липпманн У. Общественное мнение. М.: Ин-т Фонда «Общественное мнение», 2004. 384 с.

148. Литвиненко О. В. Спеціальні інформаційні операції: монографія. К.: НІСД, 1999. 163 с.

149. Литвиненко О. В. Інформаційна безпека Європи: Конспект лекцій до курсу лекцій для студ. спец. «Між-нар. інформація» спеціалізації «Європ. комунікації». К., 1999. 61 с.

150. Литвиненко О. В. Інформаційні впливи та операції: теорет.-аналіт. нариси. К.: Нац. ін-т стратегічних досліджень, 2003. 239 с.

151. Литвиненко О. Інформаційні впливи та інформаційні операції: механізми самоорганізації. *Людина і політика.* 1999. № 6. С. 32–36

152. Ліпкан В. А. Роль стратегічних комунікацій в протидії гібридній війні проти України. URL: http://goal-int.org/rol-strategichnix-komunikacij-v-protidii-gibridnij-vijni-proti-ukraini/ (дата звернення 30.11.2018)

153. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник/ В. Ліпкан, Ю. Максименко, В. Желіховський. К.: КНТ, 2006. 280 с.

154. Ліпкан В.А. Сутність гібридної війни проти України. *Імперативи розвитку цивілізації*. 2015. № 2. С. 13-16.

155. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України. К.: Видавництво Національної академії внутрішніх справ України, 2005. 350 с.

156. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба. URL: csef.ru/madia/articles/7976/9298/pdf (дата звернення 29.12.2018)

157. Макаренко С. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. URL: https://psyfactor.org/t/Makarenko_InfPro_2017.pdf (дата звернення 03.12.2018)

158. Макаров В. Е., Ступин С. А. Политические и социальные аспекты информационной безопасности: монография. Москва, Таганрог, 2015. 351 с

159. Малявин В. Б. Шэнь. Искусство управления. М.: АСТ, 2004. 430 с.

160. Мальковская И.А. Знак коммуникации. Дискурсивные матрицы. М., 2005. 240 с.

161. Манойло А.В., Петренко Л. И., Фролов Д. Б. Государственная

информационная политика в условиях информационно-психологической войны. М., 2003. С. 208.

162. Манойло А.В. Государственная информационная политика в особых условиях. М.: МИФИ, 2003. 388 с.

163. Маркоменко В. Информационное общество и проблемы его безопасности. *Федерализм.* 1997. № 4. С.18-24

164. Марущак А.І. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика*. 2010. № 3(27). С. 17-21

165. Международное публичное право. *Сборник документов.* Т. 2. М.: БЕК, 1996. 539 с.

166. 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)

167. Методологія наукових досліджень з державного управління: хрестоматія/ за заг. ред. д-ра політ. наук К.О. Ващенка. К.: НАДУ, 2014. 180 с.

168. Мина Ж., Яновська А., Матвійчук О. Інформаційна зброя як інструмент впливу на сучасне суспільство. URL: http://ena.lp.edu.ua/bitstream/ntb/33315/1/34-84-85.pdf (дата звернення 25.11.2018).

169. Моль А. Социодинамика культуры. М., 1973. 407 с.

170. Моніторинг медіа-власності в Україні. URL: http://ukraine.mom-rsf.org/ua/ukraine/ (дата звернення 04.05.2019)

171. Надійний щит для захисту інформації. URL: www.nbuv.gov.ua (дата звернення 10.11.2018)

172. Неформальная интернет-библиотека мемов Луркоморье. URL: http://lurkmore.ru/ (дата звернення 13.02.2019)

173. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України: монографія. К.: Інтертехнологія, 2008. 496 с.

174. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017 (дата звернення 27.01.2019)

175. Окінавська Хартія глобального інформаційного суспільства від 22.07.2000. URL: http://zakon.rada.gov.ua/laws/show/998_163 (дата звернення 02.12.2018).

176. Панарин И. СМИ, пропаганда и информационные войны. М.: Поколение, 2012. 411 с.

177. Панарин И.Н. Информационная война, PR и мировая политика: курс лекций. М.: Огни, 2014. 352 с.

178. Панченко В.М. Інформаційні операції в системі стратегічних комунікацій. *Стратегічні пріоритети*. № 4 (41), 2016. С.72-79

179. Петрик В.М. Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN= UJRN& P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/sitsbo_ 2009_3_15.pdf. (дата звернення 23.12.2018)

Петрик В.М. Соціально-правові основи інформаційної безпеки. URL: pidruchniki.com/18430605/politologya/sotsialno-pravovi_osnovi_informatsionoyui_bezpeki

180. Петров А.Е. Тензорная методология в теории систем. М., 1985. 152 с.

181. Петрова Г.О. Норма и правоотношения – средтсва уголовно-правового регулирования. Н. Новгород: Из-во Нижегородского университета, 1999. 192 с.

182. Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах. *Военная мысль.* 1997. № 5. С.24-27

183. Подольчак Н. Ю. Стратегічний менеджмент: навч. посібник. Львів: Видавництво Львівської Політехніки, 2012. 400 с.

184. Полевой устав СВ США FM 3-05.30 (FM 33-1-1) «Психологические операции». URL: http://issuu.com/kdavies/docs/us_army__ psychological _operations__psyops___tacti (дата звернення 18.01.2019).

185. Політика щодо прифронтових звільнених та окупованих територій донбасу з метою їх реінтеграції. URL: https://dif.org.ua/article/politika-shchodo-prifrontovikh-zvilnenikh-ta-okupovanikh-teritoriy-donbasu-z-metoyu-ikh-reintegratsii?fbclid=IwAR0sKX-9EqQL3g8zDY6aBTi0O9gIPuf5Mjke7IF15KPrjj33nTIvyB5VJr4 (дата звернення

02.05.2019)

186. Попов И.М. Война будущего: взгляд из-за океана: Военные теории и концепции современных США. М., 2004. 448 с.

187. Попов И.М. Сетецентрическая война. URL:http://www.milresource.ru/ NCW.html (дата звернення 28.10.2018)

188. Поправко К.В., Сыров В.Н. Генезис массового сознания. *Социологический журнал.* 1998. № 1-2. С. 66–78.

189. Потемкин А. В. Выявление информационных операций в средствах массовой информации сети Интернет: дисс. … канд. техн. наук. Брянск, 2015. 144 с.

190. Почепцов Г.Г. Информационные войны. Новый инструмент политики. М.: Алгоритм, 2015. 256 с.

191. Почепцов Г.Г. Информационные войны/ Г.Почепцов. М.: «Рефл-бук», К.: «Ваклер», 2000. 567 с.

192. Почепцов Г.Г. Пропаганда и контрпропаганда. М.: Центр, 2004. 210 с.

193. Почепцов Г. Три модели построения информационных операций. URL: https://ms.detector.media/ ethics/manipulation/tri_modeli_postroeniya _informatsionnykh_operatsiy/ (дата звернення 29.04.2019)

194. 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

195. 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 08.02.2019)

196. Про концепцію військово-технічного співробітництва з іноземними державами на період до 2010 року: Указ Президента України від 27.08.2003 № 913/2003. URL: http://zakon.rada.gov.ua/laws/show/913/2003 (дата звернення 12.11.2018)

197. Про інформацію: Закон України від 02.10.1992 (в редакції від

13.01.2011). URL: http://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 24.12.2018)

198. 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)

199. Про оборону України: Закон України від 06.12.1991. URL: https://zakon.rada.gov.ua/laws/show/1932-12 (дата звернення 08.02.2019)

200. Про основи національної безпеки України: Закон України від 19.06.2003. URL: http://zakon.rada.gov.ua/laws/show/964-15 (дата звернення 15.11.2018)

201. Про основні засади розвитку інформаційного суспільства на 2007-2015 роки: Закон України від 06.02.2007. URL: http://zakon.rada.gov.ua/laws/show/537-16 (дата звернення 10.12.2018)

202. Про ратифікацію Статуту і Конвенції Міжнародного союзу електрозв'язку: Закон України від 15.07.1994. URL: https://zakon.rada.gov.ua/laws/show/116/94-%D0%B2%D1%80 (дата звернення 12.01.2019).

203. 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)

204. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України: Указ Президента України від 24.09.2015 № 555/2015. URL: http://www.president.gov.ua/documents/5552015-19443 (дата звернення 30.11.2018)

205. 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)

206. Проект Закона Республики Беларусь (18.10.2000) «Об информационной безопасности».URL: http://jurfak.spb.ru/conference/2001.htm (дата звернення 23.07.2018)

207. Прокоф‘єва Д.М. Інформаційна війна та інформаційна злочинність. *Вісник Запорізького юридичного інституту*. 2000. №1. С. 288-307.

208. Прохожев А.А. Теоретико-методологические основы безопасности России. *Безопасность России в XXI веке*. М.: РИЦ ИСПИ РАН, 2006. С. 129 – 140.

209. Прохожев А.А., Турко Н.И. Основы информационной войны. *Анализ систем на пороге XXI века: теория и практика.* М., 1996. С. 252-253

210. Радиков И. В. Национальная безопасность: типичные проблемы реализации. URL: www.pilitex.info/content/view/327 (дата звернення 10.12.2018)

211. Разуваев В.Э. Правовые средства противостояния информационным войнам: дис. ... канд. юрид. наук. М., 2007. 174 с.

212. Расторгуев С.П. Информационная война. М.: Радио и связь, 1998. 415 с.

213. Расторгуев С. П. Информационная война. Проблемы и модели. Экзистенциальная математика. М: Гелиос АРВ, 2006. 237 с.

214. Расторгуев С.П. Принципы целостности и изменчивости в решении задачи обеспечения безопасности. *Конфидент*. 1998. № 3. С. 11-15

215. Расторгуев С.П., Литвиненко М.В. Информационные операции в сети Интернет/ Под общ. ред.А.Б. Михайловского. М.: АНО ЦСОиП, 2014. 128 с.

216. Расторгуев СП. Философия информационной войны. М.: Изда-во МПСИ, 2003. 496 с.

217. Рашкофф Д. Медиавирус. Как поп-культура тайно воздействует на ваше сознание. М.: Ультракультура, 2011. 394 с.

218. Резолюция 60/45, принятая Генеральной Ассамблеей Организации Объединенных Наций "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности". URL: https://zakon.rada.gov.ua/laws/show/995_e45 (дата звернення 27.01.2019)

219. Решение № 1106 «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» от 03.12.2013. URL: https://www.osce.org/ru/pc/109648?download=true (дата звернення 31.01.2019)

220. Руководство ООН по предотвращению и контролю за компьютерными преступлениями. UN, New- York, 1993. 32 с.

221. Сацута А.А. Национальная безопасность как социальное явление: современная парадигма// Вестник Военного университета. 2007. № 3 (11). С.36–43

222. Ситнова И.В., Поляков А.А. Информационно-психодогическое воздействие как практика ведения войн четвертого поколения. URL: https://cyberleninka.ru/article/n/informatsionno-psihologicheskoe-vozdeystvie-kak-praktika-vedeniya-voyn-chetvertogo-pokoleniya (дата звернення 12.12.2018)

223. Скакун О.Ф. Теория государства и права: учебник. Х.: Консум, 2000. 704 с.

224. Снытников А.А., Туманова Л.В. Обеспечение и защита права на информацию. М.: Городец-издат., 2001. 344 с.

225. Соловьева Е. А. Информационное противоборство в сети Интернет: политологический анализ: дисс. … канд. полит. наук. Пятигорск, 2011. 215 с.

226. Спецоперация «Гюльчатай, открой личку!» или сказ о том, как мы «разводили» вату, пользуясь методами российских пропагандистских СМИ. (Часть 1). URL: https://psb4ukr.org/189342-specoperaciya-gyulchataj-ili-skaz-o-tom-kak-my-razvodili-vatu/(дата звернення 04.12.2018)

227. Спецоперация «Гюльчатай, открой личку!» или сказ о том, как мы «разводили» вату, пользуясь методами российских пропагандистских СМИ. (Часть 2). URL: https://psb4ukr.org/190529-specoperaciya-gyulchataj2/(дата звернення 04.12.2018)

228. Столтенберг: статья 5 Вашингтонского договора будет распространена и на гибридные атаки. URL: https://topwar.ru/87197-stoltenberg-statya-5-vashingtonskogo-dogovora-budet-rasprostranena-i-na-gibridnye-ataki.html (дата звернення 31.01.2019)

229. Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору від 19.11.2010 р. URL: https://www.nato.int/ cps/uk/natohq/ official_texts_68580.htm (дата звернення 29.01.2019)

230. Сунь-Цзы. Искусство войны. URL:http://masters.donntu.org/2014/ fknt/kebikov/library/article9.pdf (дата звернення 02.11.2018)

231. Т. Бережна Стратегічна Концепція НАТО "активне залучення, сучасна

оборона". URL: http://www.niss.gov.ua/articles/358/ (дата звернення 27.01.2019)

232. Т. Попова Правове поле для спецназу. URL: https://www. radiosvoboda. org/a/28373318.html (дата звернення 12.02.2019)

233. Тамодлин А.А, Государственно-правовой механизм обеспечения информационной безопасности личности: дисс. ... канд. юрид. наук. URL: http://diss.rsl.ru/diss/06/0268/060268047.pdf (дата звернення 18.12.2018).

234. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … докт. юрид. наук. URL: https://www.uzhnu. edu.ua/uk/infocentre/get/19617

235. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 411 с.

236. Угода про діяльність держав на Місяці та інших небесних тілах. URL: https://zakon.rada.gov.ua/laws/show/995_482 (дата звернення 15.01.2019).

237. Устав Организации Объединённых Наций и Устав Международного Суда. URL:https://zakon.rada.gov.ua/laws/show/995_010 (дата звернення 05.01.2019)

238. Уэбстер Ф. Теории информационного общества. М.: Аспект Пресс, 2004. 400 с.

239. Фаренік С.А. Логіка і методологія наукового дослідження : наук.-метод. посібник. К. : Вид-во УАДУ, 2000. 340 с.

240. Фомин А.А. Юридическая безопасность субъектов российского права (вопросы теории и практики): дисс. … докт.юрид.наук: 12.00.01. Пенза, 2007.466 с.

241. Фролов Д.Б. Информационная война: эволюция форм, средств и методов. URL: cyberleninka.ru/article/n/informatsionnaya-voyna-evolyutsia-form-sredstv-i-metodov (дата звернення 12.12.2018)

242. Фролов Д.Б. Информационное противоборство в сфере геополитических отношений: дис. ... докт. полит. наук. URL: http://diss.rsl.nj/diss/07 /0233 /070233 048.pdf (дата звернення 18.12.2018)

243. Фролов Д.Б., Старостина Е.В. Информационные войны: проблемы

терминологии. *Адвокат*, № 1, январь 2005 года. С.82-84

244. Хаба Р.С. Деструктивні інформаційні впливи в сучасних умовах. *Інформаційна безпека людини, суспільства, держави*. № 1(21) 2017. С.216-224

245. Хананашвили М.М. Информационные неврозы. М.: Медицина, 1986. 310 с.

246. Хантингтон С. Столкновение цивилизаций. URL: https://www.litres.ru/ semuel-hantington/stolknovenie-civilizaciy/chitat-onlayn/ (дата звернення 21.04.2019)

247. Цымбал В.И. О концепции информационной войны. *Информационный сборник «Безопасность»*. М., 1995. № 9. С. 35

248. Черкасов А. Оружие, которое не убивает, но побеждает. *Ориентир*. 1997. № 1. С. 13–19

249. Черных С.Н., Зуева Н.А. Информационная война: традиционные методы, новые тенденции. *Контекст и рефлексия: философия о мире и человеке.* 2017. Том 6. № 6А. С. 191-199

250. Четырехлетний обзор оборонной политики. URL: http://archive.defense. gov/qdr/formatted%20Exec%20Summ%20_RUSSIAN_.pdf (дата звернення 27.01.2019)

251. Чи принесла війна “мову ворожнечі” в українські медіа? URL: http://ua.ejo-online.eu/2481 (дата звернення 09.03.2019)

252. Шейко В.М. Організація та методика науково-дослідницької діяльності: підручник. К.: Знання-Прес, 2002. 295 с.

253. Широканов Д.И., Буслаева М.К. Информационные войны и новая парадигма безопасности. URL: https://ibn.idsi.md/sites/default/ files/imag_file/ Informationie%20voini%20i%20novaia%20paradigma%20bezopasnosti_0.pdf (дата звернення 28.11.2018)

254. Шишкина Л.Р. Особенности информационно-психологических воздействий в современной информационно-психологической борьбе: дисс. … канд. полит. наук. М., 2005. 214 с.

255. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. URL: http://www.economy.nayka.com.ua/ ?op=1&z=5514 (дата

звернення 03.12.2018)

256. Шутов Р. Дискурс українських каналів окреслив чітку лінію між «своїми» і «чужими». URL: https://ms. detector.media/go_detector_media/diyalnist/zvity/mediyniy_diskurs_ukrainskikh_telekanaliv_okresliv_chitku_liniyu_mizh_svoimi_i_chuzhimi_roman_shutov/ (дата звернення 07.03.2019)

257. Щербина Д.Н. Военные информационно-коммуникативные операции как явление современного общества: дисс. … канд. филос. наук. М., 2016. 227 с.

258. Эко У. Осмысляя войну. *Пять эссе на темы Этики*. URL: http://www.niworld.ru/Statei/umberto_ako/war.htm (дата звернення 13.02.2019)

259. Юнг К.Г. Психология бессознательного. М., 1994. 400 с.

260. Як писати правду під час війни. URL: http://osvita.mediasapiens.ua/ethics/standards/yak_pisati_pravdu_pid _chas_viyni/ (дата звернення 09.03.2019).

261. Якунин В., Багдасарян В., Сулакшин С. Новые технологии борьбы с российской государственностью: монография. М.: Научный эксперт, 2009. 424с.

262. Ярмиш Н. Проблема інформаційної причинності у науці кримінального права. *Право України*. 2003. № 7. С. 28-30.

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

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

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

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

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

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

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

Наукові праці, які засвідчують апробацію матеріалів дисертації:

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

8. Верголяс О.О. Стандарти НАТО у сфері проведення спеціальних інформаційних операцій. *Матеріали Міжнародної науково-практичної конференції «Юридична наука: виклики і сьогодення*». 2018. С. 72-76.

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

Додаток Б

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОЇ ОКУПАЦІЇ АВТОНОМНОЇ РЕСПУБЛІКИ КРИМ РОСІЙСЬКОЮ ФЕДЕРАЦІЄЮ

Технологія інформаційної блокади, що активно застосовувалась під час анексії Криму, була спрямована на формування інформаційного вакууму для українських засобів масової інформації в АРК з метою безальтернативного подання фактів про події в Україні та Криму, забезпечуючи єдину інтерпретацію подій. При цьому Росія ставила на меті здобути інформаційне домінування в регіоні, не гребуючи забороненими засобами. Серед поширених заходів – позбавлення кримських радіокомпаній можливості брати участь у конкурсі отримання права на наземне ефірне мовлення, нормативно-правові обмеження ЗМК, невмотивована відмова у реєстрації (перереєстрації) кримських ЗМК, а також використання «самооборони» для впливу на ЗМІ.

Окрім того журналісти піддавалися силовому тиску – стеження і профілактичні бесіди з боку спецслужб, прослуховування їх розмов і читання листування, погрози фізичної розправи з подальшим викликом спецслужб, звинувачення в іноземному фінансуванні тощо. Як результат – на півострові не залишилося вільних медіа, інформаційний простір Криму повністю було зачищено під «нові російські реалії». Технологія інформаційної блокади включає також **контекстуальне блокування**. Відповідний блокувальний контроль інформаційного простору передбачав: контроль вербальних позначень («повернення Криму»), які прибирають зі свідомості агресивний характер; контроль візуальної складової – на телеекранах відсутні зображення невдоволених анексією Криму місцевих мешканців півострову; контроль єдності інтерпретації подій (більшість матеріалів представляють собою суб’єктивні коментарі російських кореспондентів або редакцій (у кращому випадку все обмежується окремими фразами, вирваними з контексту), що по суті, є одним з варіантів цензури).

Інформаційна блокада завжди тісно зв'язана з інформаційним

домінуванням. Це дві сторони однієї медалі. До них вдаються як у випадку воєнних дій, так і в мирний час (наприклад, під час виборів). Має місце створення інформаційного вакууму з якогось

Інформаційна блокада сьогодні супроводжує практично усі військово-політичні конфлікти. Так, війна з Іраком у 1991 р. зображувалася як «чиста» і справедлива. Західні ЗМІ всіляко розхвалювали чесноти «хірургічно точних ударів». При цьому старанно замовчувалися будь-які свідчення протилежного характеру (ті ж випадки, що неможливо було сховати, називалися прикрими «помилками», щоб згладити негативну реакцію громадськості).

Г.Почепцов на прикладі війни в Чечні класифікує контроль інформаційного простору, що блокує, у такий спосіб:

1. Контроль вербальних позначень. Прикладом служать такі обтічні фрази як «Килимові/крапкові бомбометання», «Зачищення території» і т.п., що забирають зі свідомості смертоносний характер цих військових операцій.
2. Контроль візуальної картинки, відповідно до якого на телеекрані відсутні зображення поранених та убитих, понівеченої техніки своїх та союзницьких військ.
3. Контроль єдності інтерпретації подій. Наочним прикладом є спеціальна вказівка російської влади, що заборонила показ на телеекрані інтерв'ю з чеченськими бойовиками.

У російських ЗМІ прикладом інформаційної блокади може служити не тільки висвітлення подій у Чечні, але й у країнах ближнього зарубіжжя: Бєларусі, Україні, Грузії, Молдові. Російська преса практично не дозволяє представникам цих країн самостійно висловлювати свою позицію. У кращому випадку усе обмежується їхніми окремими фразами, вирваними з контексту.

Використання медіаторів – «лідерів думки» – стало одним з найбільш популярних прийомів кремлівських ЗМК. В якості медіаторів у різних ситуаціях і для різних соціальних груп і прошарків виступали неформальні лідери, політичні діячі, представники релігійних конфесій, діячі культури, науки, мистецтва, спортсмени, військові – для кожної категорії населення обирався свій авторитет. У психології впливу це називається **«фіксацією на**

авторитеті»: *«Лукашенко считает Крым частью России»*, *«Лидер французского Национального фронта Марин Ле Пен заявила, что признает референдум, состоявшийся в Крыму, вполне законным»*, *«Кустурица о Майдане: западные политики – лучшие режиссеры, чем я»*, *«Бесспорной исторической справедливостью считают возвращение Крыма в Россию представители дома Романовых»*.

Дана техніка ґрунтується на двох постулатах. По-перше найбільший ефект справляють, як не дивно, міфи, чутки і плітки, що циркулюють у суспільстві Другий постулат випливає з першого: ефективний інформаційний вплив на людину здійснюється не безпосередньо засобами масової комунікації, а через значимих для нього, знайомих йому авторитетних людей («лідерів думки») - трансляторів думок і чуток. Неофіційні особистісні комунікації для людей більш значимі, ніж «офіційні» повідомлення ЗМІ. У більшості випадків думки людей із приводу чого-небудь складаються в процесі спілкування в родині, у колективі і т.д. У бесідах між собою родичі, друзі, товариші по службі осмислюють події і факти, виробляють спільний підхід відповідно до звичних для них цінностей і норм. Думки з кожного питання (від простого - який пральний порошок купувати, до складного - за кого голосувати) складаються і утверджуються під впливом певних авторитетів. Це люди, що або займають формально (батьки, чоловіки, старші брати/сестри, начальник, лідер серед однодумців) центральне становище в групі (лідери групи), або визнані експертами в даній сфері (лідери думки). Іншими словами, пропагандистський вплив ЗМІ завжди має опосередкований характер.

Розглянемо докладніше механізм сприйняття подібної інформації. Після одержання інформаційного повідомлення реципієнт не відразу приймає рішення прийняти чи відкинути його. Свідомо чи на підсвідомому рівні він шукає ради серед оточуючих, насамперед у так званих «лідерів думки» своєї групи. Лідери думки - це високоавторитетні члени групи, думки і поради яких з певних питань мають особливу цінність для інших. Саме вони відіграють вирішальну роль у формуванні ставлення основної маси реципієнтів до проблеми, відображеної в пропагандистському повідомленні. Дане явище

знайшло відображення в моделі двоступінчастого потоку комунікації, розробленої в середині 50-х років у США П.Лазарсфельдом. У запропонованій ним моделі двоступеневого пропагандистського процесу враховується, по-перше, взаємодія між джерелом і авторитетами мікросоціального рівня, що позначаються як лідери думки чи «медіатори» (посередники), по-друге, взаємодія лідерів думок чи медіаторів з окремими членами мікросоціальних груп. У практиці інформаційно-психологічного впливу ЗМІ це, зокрема, призвело з одного боку до того, що пропагандистські і рекламні повідомлення стали більш орієнтованими на лідерів мікросоціальних груп, а з іншого боку - у них стали використовуватися особи, думки яких значимі для інших.

Американські фахівці вважають: щоб сформувати думку широкої аудиторії з якогось питання, досить обробити усього лише 10% її членів - лідерів думки (медіаторів), які й протранслюють повідомлення на масовий рівень. Як медіатори в різних ситуаціях і для різних соціальних груп та прошарків можуть виступати неформальні лідери, політичні діячі, представники релігійних конфесій, діячі культури, науки, мистецтва, спортсмени, військові, секс-бомби і т.д. - для кожної категорії населення знаходиться свій авторитет.

У психології впливу це називається «фіксацією на авторитетах». Більшість людей схильні до наслідувальної поведінки, орієнтуючись у своїх учинках на дії авторитетних для них лідерів думки. Їм властиво брати приклад з тих, кого вони поважають і хто для них є лідером. Тому вибір естрадних і спортивних «зірок», інших популярних осіб для передач рекламно-пропагандистського характеру й участі у виборчих кампаніях обумовлений насамперед тим, що вони мають досить широку аудиторію шанувальників, багато з яких не схильні оцінювати рівень компетентності своїх кумирів не тільки в політичних, але й інших питаннях, з яких вони дають свої оцінки чи здійснюють рекламне просування (наприклад, товарів, якими особисто можуть і не користатися і т.п.).

З іншого боку, у рекламних роликах і пропагандистських сюжетах широко використовуються і «прості люди з народу», «такі як ми». Усе залежить

від специфіки товару чи ідеї, що просуваються. Наприклад, переконати нас в тому, що рекламовані ліки дійсно дієві, скоріше зможе професійний лікар (а точніше - той набір ознак, що ми сприймаємо як «авторитетні» показники професіоналізму: білий халат, лікарський кабінет, використання медичних термінів у розмові). У крайньому випадку з цією задачею справиться популярний артист. А от товари повсякденного попиту ми купуємо, ґрунтуючись, у першу чергу, на думці «таких як ми», нашого найближчого оточення - друзів, родичів, сусідів.

Одним з найефективніших прийомів введення в оману була **технологія анонімного авторитету**. В таких випадках російськими ЗМІ цитувалися документи, оцінки експертів, свідків, звіти та інші матеріали, які необхідні для більшої переконливості, однак ім'я відповідного авторитету не повідомляється: *«Турчинов признал полный провал так называемой антитеррористической операции и приказывает любой ценой восстановить контроль над бунтующим юго-востоком непременно до 3 мая. Об этом на условиях анонимности журналистам рассказал источник в украинском Генштабе»***.**

Авторитет, до якого звертаються, може бути релігійним, це може бути вагома політична фігура, діяч науки або іншої професії. Ім'я авторитету не повідомляється. При цьому може здійснюватися цитування документів, оцінок експертів, свідків звітів та інших матеріалів, які необхідні для більшої переконливості. Приклади: «Вчені на підставі багаторічних досліджень встановили ...», «Доктора рекомендують ...», «Джерело з найближчого президентського оточення, який побажав залишитися невідомим, повідомляє ...». Посилання на неіснуючий авторитет додають їй солідність і вагу в очах обивателів. При цьому джерело не ідентифікований і ніякої відповідальності за неправдиве повідомлення журналісти не несуть.

Прийом «тримай злодія» використовувався російськими мас-медіа для дискредитації української влади, коли держава-агресор першою піднімає ґвалт і спрямовує суспільне невдоволення в бік України: *«Именно радикализация действий Киева заставила и Крым принимать решения быстрее и четче. Референдум уже через неделю, и вопросы на нем конкретнее: широкая*

автономия или воссоединение с Россией. И это редкий политический результат, которого блестяще добились самозванцы в Киеве».

Неодноразове застосування техніки «**ефект ореолу**», що передбачало візити російських авторитетних діячів культури, спорту та політики до Криму сприяло підвищенню статусу зусиль РФ в напрямку повернення Криму та «легалізації» так званого «референдуму» кримчан. Так 26 лютого 2014 до Криму прибула делегація РФ, до якої входили відомі російські діячі такі як Ірина Родніна, Микола Валуєв, Валентина Терешкова, Дмитро Савельєв та лідер «Справедливої Росії» Сергій Миронов. 14 березня 2014 року м. Сімферополь відвідали відомий російський хокеїст Вячеслав Фетісов, російський борець класичного (греко-римського) стилю Олександр Карелін і російський тенісист Марат Сафін. Однією з характерних ознак російських ЗМК є їх оперативність та миттєва реакція на події.

Ефект ореолу базується на підступній психологічній властивості – людській схильності мислити помилковими аналогіями. Найчастіше він ґрунтується на двох розповсюджених стереотипах-оманах.

1. «Поруч - значить разом». Унаслідок цього феномена перебування поруч зі знаменитою чи високопоставленою людиною трохи підвищує статус тих, хто знаходиться поруч, в очах оточуючих.

2. Другий стереотип полягає в наступному. Людину, яка домоглася вагомих успіхів у якійсь конкретній галузі і якій, відповідно, приписуються певні якості, оточуючі вважають здатною на більше й в інших справах, а також приписують цілий букет інших якостей..

Граючи на випередження завдяки ефекту першості росіянам успішно вдавалося першими донести необхідну інформацію до реципієнта та сформувати бажане уявлення про події: *«Сколь громко бы ни звучали заявления из Киева о единой и неделимой Украине, граница по перешейку, де-факто, уже пролегла… Но Крым с каждым днем все больше напоминает государственное образование»*. В даному випадку спрацьовує один з ефектів сприйняття: при надходженні суперечливої інформації (перевірити яку неможливо) люди схильні віддавати перевагу тій, що надійшла першою. А змінити вже

сформовану думку дуже важко.

Досить активно та ще задовго до анексії Криму РФ використовувала такий маніпулятивний прийом як **переписування історії**. Це прийом є ефективним в довготривалій перспективі, коли потрібно поступово сформувати потрібний світогляд. Він діє завдяки руйнуванню історичної пам'яті через канали радіо і телебачення, пресу, театральні вистави, кінофільми, книги, лекції і т.д. Таким чином будується ілюзорний світ, який сприймається як справжній. Сформована картина історичної дійсності «стирається» зі свідомості людини шляхом підміни фейковими даними: *«После развала СССР россияне не переставали считать Крым своим»*, *«Развал СССР превратил фарс в трагедию: сотни тысяч русских жителей полуострова оказались оторваны от своей исторической родины. Украинское руководство безапелляционно заявило о принадлежности Крыма (вместе с Севастополем) Украине, российские лидеры молчаливо согласились с утратой региона, имеющего стратегическое значение»*, *«События 1991 года превратили русскую нацию, крупнейшую в Европе, в национальное меньшинство в бывших союзных республиках, где русские по численности мало уступают титульным нациям. С приходом к власти в республиках националистических правительств русские испытывают все возрастающее давление, проявившееся в различных формах. В данном случае это – нарастающий с каждым годом процесс украинизации, который в русском – и в языковом, и в этническом плане – в Крыму проходит наиболее болезненно»*.

Метод ефективний у тривалій перспективі, коли потрібно поступово сформувати потрібний світогляд. Щоб «промити мозки» цілому суспільству, зробити над ним велику програму маніпуляції і відключити здоровий глузд декількох поколінь, треба в першу чергу зруйнувати історичну пам'ять. Сучасні технології маніпуляції свідомістю здатні зруйнувати в людині знання, отримана від реального історичного досвіду, замінити його штучно сконструйованим «режисером» знанням. Штучно сформована картина історичної дійсності передається окремим індивідам за допомогою книг, лекцій, радіо і телебачення, преси, театральних вистав, кінофільмів і т.д. У такий спосіб

будується ілюзорний світ, що сприймається як дійсний. У результаті все реальне життя людина може сприймати як неприємний сон, а ті химери, що йому нав'язує пропаганда, реклама і масова культура, увівши її в транс, сприймає як реальність.

У цій справі особливо ефективний кінематограф. Кіно, як спосіб пропаганди, здатне справляти надзвичайно високий емоційний вплив (див. Емоційний резонанс). Воно активно генерує в уяві глядача ілюзорну картину світу в дуже ідеалізованому вигляді. Відповідно до авторського задуму кіно може довільно створювати в глядача відчуття «справедливості» і моральної правоти того чи іншого персонажа, незалежно від його дійсної ролі в історії. При цьому пропагандистський вплив на людину відбувається приховано, на емоційному рівні, поза його свідомим контролем. Ніякі раціональні контраргументи в цьому випадку не спрацьовують.

Техніка ефекту присутності часто використовувалася мас-медіа Росії під час «репортажів з місця події», спотворюючи реальність та транслюючи змонтовані відповідним чином сюжети: *«Горят пассажирские автобусы, направлявшиеся в Крым. Людей, мужчин и женщин, выволокли на улицу, избили палками. Заставили лежать на земле друг на друге, ходить на корточках, петь гимн Украины. Издевались над безоружными так называемые герои Майдана. Автобусы с разбитыми окнами и фарами привезли в Симферополь раненых, словно с войны. Очевидцы заявили об убийстве семи крымчан в ту ночь»*. Ілюзія достовірності здійснювала потужний емоційний вплив і створювала відчуття справжності подій.

Систематичне повторення одних і тих самих визначень та фраз є прикладом **техніки класифікації**. За допомогою класифікаторів, що описують об'єкти або події, інформація форматується таким чином, що одержувач повідомлення несвідомо сприймає нав'язане йому визначення ситуації. По-перше, це слова і поєднання, що описують **власну «позитивну і конструктивну позицію**»: *«восстановление мира и стабильности»*, *«наши русскоязычные братья»*, *«великий славянский народ»*. По-друге, це **«контрастуючі слова»,** що мають на меті охарактеризувати супротивника в

негативному ключі: *«фашистский переворот»*, *«бандеровское государство»*, *«украинские политики-эстремисты»*, *«украинские националисты»*.

Домінуючі у ЗМІ класифікатори звичайно відбивають загальний напрямок поточної політики владних структур, насамперед інформаційної. Досить згадати, як у державних (а в останні роки й у недержавних) ЗМІ висвітлюються різні політичні акції. Типовий варіант повідомлення в новинах: «учасники акції»... (варіанти: «люди похилого віку, особи без певних занять, серед яких є злочинні елементи, алкоголіки і наркомани; радикально налаштовані молоді люди, що сповідують екстремістські погляди...»; «акція проводиться на гроші»... (варіанти: Б. Березовського; кримінальних структур; іноземних спецслужб; міжнародних терористичних центрів...); «метою акції є»... (варіанти: дестабілізація ситуації в країні; створення негативного іміджу нашої держави у світі; перешкоджання роботі органів влади...); «державні органи»... (варіанти: пропонують вирішити питання цивілізованим способом; демонструють готовність до конструктивного діалогу; займають позитивну і прагматичную позицію; не приймають ультиматумів...); «правоохоронні структури»... (варіанти: неухильно дотримують вимоги закону; діють адекватно ситуації; застосовують відповідні сили і засоби; мужньо протистоять деструктивним силам і антидержавним елементам...); «прості громадяни»... (варіанти: не підтримують акцію; засуджують ініціаторів безладь; виявляють розуміння дій правоохоронних органів; схвалюють дії глави держави під час кризової ситуації...). Як правило, для посилення значеннєвого й емоційного ефекту класифікатори супроводжуються відповідним відеорядом.

Прийом зворотного зв'язку, що передбачає реакцію реципієнтів інформації на певні події також був вельми поширений у російських меседжах. ЗМІ РФ активно повідомляло про штучно інсценовані масові акції на підтримку відторгнення Криму від України: *«…народные сходы – в поддержку Украины и соотечественников, живущих в этой стране, начались в России в воскресенье. Тогда на шествия и митинги, инициированные патриотическими молодежными и ветеранскими организациями, собрались десятки тысяч*

человек в Москве, Санкт-Петербурге и Краснодаре. В столице также состоялись мото- и автопробег. В течение всей недели мероприятия под девизами «За братский народ!», *«Своих не сдаем!»прошли в крупнейших российских городах, в том числе пограничных с Украиной российских регионах, – Белгороде, Брянске, Новочеркасске, Ростове-на-Дону и многих других».*

Люди, що виступають у якому-небудь дійстві як учасники, більшою мірою схильні змінювати свої погляди на користь думки, що рекомендується його сценарієм, ніж пасивні спостерігачі тих подій, що відбуваються. Ілюзія участі в дискусії з якої-небудь актуальної проблеми призводить до більшої зміни думок та настанов, ніж просто пасивне сприйняття інформації. Для того, щоб в аудиторії не виникало відчуття однобічного впливу і комплексу «байдужості адресата», сучасними ЗМІ широко практикуються способи, так званого, «зворотного зв'язку» у різних формах: дзвоники в студію під час прямого ефіру, вибір по телефону варіанта відповіді на поставлене питання й ін. Подібний прийом маніпуляції покликаний створити в масової аудиторії ілюзію участі в інформаційному процесі.

У тих випадках, коли невигідна комунікатору думка є домінуючою, задача «зворотного зв'язку» зводиться до корекції, зміні умонастроїв мас. Демонстрація підтасованих результатів телефонних опитувань, «фільтрація» дзвоників у студію, організація «думки громадськості» через підставних людей «з вулиці» і т.п. спрямовані на те, щоб у людини, яка має іншу думку, сформувати психологічну установку «білої ворони» - адже інші, а їх більшість, думають інакше. Часом незгода й інакомислення свідоме чи випадково допускається, наприклад, озвучується обурений телефонний дзвоник чи оприлюднюється протест. Цей момент всіляко використовується, підкреслюються чесноти даного джерела інформації, що «об'єктивно» показує весь спектр думок і точок зору по різних питаннях.

Різновидом зворотного зв'язку є так звана **техніка інсценованих заходів**. Насамперед до неї відносяться різноманітні варіанти спілкування високопоставлених персон з «простим народом». «Спілкування» може бути

прямим (відповіді на питання, задані громадянами по телефону, розмови з «випадковими перехожими» на вулиці і т.д.) і опосередкованим (прес-конференції, брифінги для мас-медіа, відповіді на питання журналістів і т.п.). Найчастіше т.зв. спілкування з народом є усього лише добре зрежисованим спектаклем. Відповідні телепрограми організовуються таким чином, нібито голова держави (або інша високопоставлена персона) спонтанно відповідає на питання, задані громадянами по телефону чи через Інтернет. Питання звичайно підбираються виходячи з результатів соціологічних досліджень. Вони повинні відбивати актуальні соціальні проблеми, що хвилюють широкі маси людей, або формувати сприятливий імідж даної посадової особи. Далі народ спостерігає чергове телешоу за назвою «Глава держави відповідає на питання простих громадян у прямому ефірі» з наступною демонстрацією схвальних відгуків «простих людей з вулиці» («Ах, я навіть і не припускав, який демократичний у нас президент - простий і доступний, відкритий для діалогу, поспілкуватися з ним може кожен!» тощо).

Яскравим прикладом цієї техніки є спілкування народу з Президентом В.В. Путіним в режимі он-лайн – т.зв. «прямі лінії», – що є лише добре відрепетованою виставою. Різновидом даної техніки «зворотного зв'язку» є «псевдосоціологічні опитування», що як правило є лише способом формування громадської думки, а не його реальним відображенням, тобто різновидом звичайної пропагандистської маніпуляції.

Питання формулюються таким чином, щоб створити у аудиторії «правильний» погляд на ту чи іншу проблему: «*более 90 процентов граждан считают, что Россия должна защищать интересы русских и представителей других национальностей, проживающих в Крыму. При этом около 83 % россиян полагают, что Россия «должна это делать, даж*е если эта позиция осложнит наши отношения с некоторыми государствами».

Техніка констатації факту здобула неабияке поширення у медіа-повідомленнях країни-агресора. Бажане демонструвалось як факт. Такого роду пропаганда зазвичай подається під виглядом новин або результатів соціологічних досліджень, що в свою чергу знижує критичність сприйняття:

*«Крым – один из самых известных в мире исторических регионов России», «Воссоединени*е с Россией: крымчане хотят восстановить историческую справедливость». Прийом використовується для створення відповідних настроїв у суспільстві. Розрахунок тут простий, адже більшість людей мислять стереотипами: «Диму без вогню не буває», «Раз про це усі говорять - значить так воно і є». У людини штучно створюється відчуття себе в меншості. У результаті вона стає безініціативною, віддаючи пріоритет тому, кого вона вважає представником «більшості».

Такого роду пропаганда звичайно подається під виглядом новин чи результатів соціологічних досліджень. Для додання авторитетності подібним повідомленням широко використовуються «лідери думки»: популярні журналісти, відомі політологи, соціологи і т. ін. Скинути тягар авторитету - психологічно важкий процес. Він вимагає мужності та вільної волі. Адже ті, хто при владі, та грошові мішки завжди мають можливість найняти приємного ведучого, улюбленого артиста, шановного академіка, непідкупного чи правозахисника секс-бомбу - для кожної категорії населення знайдеться свій авторитет.

Надзвичайно поширеним методом навіювання була техніка **«свідки подій»**, що подекуди використовувалась для створення емоційного резонансу. ЗМІ формували сюжет на основі опитування випадкових людей, із слів яких конструювали необхідний смисловий і емоційний ряд. Особливо сильний ефект створювався завдяки використанню **коментарів «простого населення»**: *«Пять автобусов доставили в столицу региона шахтеров соседних горняцких поселков. «Да мы на все готовы. Шахтеры – это такая специальность, нация, люди в душе такие, что будут до последнего стоять, чтобы отстоять свое. Нас ничем не испугать», – убежден звеньевой проходческой бригады Александр Сезонов. Здесь готовы стоять и днем, и ночью, чтобы дать отпор боевикам. На митинг собираются и шахтеры, и бывшие афганцы. «Я категорически против того, что они хотят вообще сотворить. Чего они хотят? Войны? Они не понимают, что такое война!» – говорит ветеран войны в Афганистане из*

Донецка Олег Кудинов. Обычно тихий Донбасс тоже вышел на митинг».

Класичним став приклад часів війни в Перській затоці. У жовтні 1990 р. світові ЗМІ облетіла розповідь п'ятнадцятирічної дівчинки про те, що вона бачила, як іракські солдати витягли п'ятнадцять дитин з роддома і поклали їх на холодну підлогу вмирати. Ім'я дівчинки демонстративно ховалося з причин безпеки її родини. Президент США Дж. Буш використовував розповідь про мертвих дітей десять разів протягом сорока днів перед початком вторгнення в Ірак. Сенатське обговорення по схваленню військової акції так само неодноразово поверталося до цього факту. Пізніше з'ясувалося, що цією дівчинкою виявилася дочка посла Кувейту в США, члена кувейтської правлячої родини. Ще пізніше стало відомо, що більшість інших «свідків» були підготовлені і виставлені відомою фірмою з паблік рілейшнз Hill & Knowlton.

Прийом хибної аналогії, що базується на схильності людини мислити аналогіями, будувати у своєму мисленні т.зв. псевдологічні послідовності, також не пройшов поза увагою російських журналістів. В основі даного методу – звичка більшості людей мислити, використовуючи логічні зв’язки «причина – наслідок», під час якого люди схильні екстраполювати події з минулого на інші події, що не мають жодного відношення до первинних: *«Право о самоопределении никто не отменял, — пояснила Валентина Матвиенко. – Почему-то никто не заявил, что референдум о независимости Шотландии, который должен состояться в сентябре, априори незаконный». Техніку емоційного резонансу як спосіб створення у широкої аудиторії антиукраїнського настрою також активно використовували російські медіа: «Споры, угрозы, обвинения все громче. В ход идут кулаки. Жертв нет. Но побоище в Симферополе – это то, о чем сегодня говорил, пожалуй, весь Крым, которому неофашисты из Киева и Западной Украины уже пригрозили своим десантом».* Щоб підсилити емоційну дієвість повідомлення нерідко його насичували конкретними подробицями, які краще запам’ятовуються і краще засвоюються. Особливо ефективна тут є **техніка «свідок подій»,** оскільки вона спирається на елементи особистого досвіду людини. Для створення емоційного резонансу використовуються і різноманітні «класифікатори».

Однією із самих небезпечних психологічних пасток є схильність людини мислити аналогіями, будувати у своєму розумі так звані псевдологичні послідовності. Звичним для більшості людей стилем мислення є той стиль, що використовує логічні зв'язки «причина - наслідок». Ці зв'язки здаються цілком доступними контролю свідомості і відповідають сфері «здорового глузду». Зв'язки «конкретна причина - конкретний наслідок», що коли-небудь мали місце, ми схильні екстраполювати і на інші об'єкти, які не мають ніякого відношення до первісних - отут і криється підступ.

Особливо помітна техніка «**емоційного резонансу**» під час телевізійних новин за участю зокрема Д. Кисельова, який використовуючи необхідні інтонації коментує діяльність українських державних посадовців, свідомо викликаючи обурення у населення на їх адресу завдяки «емоційному налаштуванню». Та навпаки, описуючи дії російської провладної еліти та особисто Президента РФ В.В. Путіна в його голосі відчуваються ознаки «конструктивного оптимізму» і впевненість в успішних перспективах російської нації. Таким способом формувалося емоційне ставлення масової аудиторії до «справедливого повернення Криму до Росії». Застосовуючи техніку психологічного шоку, російські медіа демонструючи «насильницькі» дії кримських татар проти проросійських громадян Криму мали на меті здійснити сильний вплив на підсвідомість та налаштувати російськомовних мешканців Криму проти кримськотатарської меншини: *«Медики подвели итоги противостояния между русскоязычными жителями и крымскими татарами 26 февраля. И итоги эти печальны. Два человека погибли в давке, 35 получили ранения»*. Але ж насправді агресивна пропагандистська кампанія з нагнітання антиісламських настроїв у Криму активно велась російськими ЗМК щодо Духовного управління мусульман Криму (ДУМК) і Меджлісу кримськотатарського народу з метою дискредитації місцевих мусульманських громад, а також заміни незручних лідерів мусульман на проросійськи налаштованих**.** Численні спроби дестабілізувати ситуацію на півострові шляхом нагнітання антиісламських настроїв передбачали звинувачення на адресу ДУМК, Меджлісу кримськотатарського народу, інших організацій щодо їх

фінансових та ідеологічних зв’язків з «радикальними ісламістськими організаціями».

Техніку емоційного резонансу можна визначити як спосіб створення у широкої аудиторії певного настрою з одночасною передачею пропагандистської інформації. Емоційний резонанс дозволяє зняти психологічний захист, що на усвідомлюваному рівні створює людина, намагаючись відгородитися від пропагандистського чи рекламного «промивання мозків». Одне з основних правил пропаганди говорить: у першу чергу потрібно звертатися не до розуму, а до почуттів людини. Захищаючись від пропагандистських повідомлень, на раціональному рівні людина завжди здатна вибудувати систему контраргументації і звести всі зусилля із «спецобробки» до нуля. Якщо ж пропагандистський вплив на людину відбувається на емоційному рівні, поза її свідомим контролем, ніякі раціональні контраргументи в цьому випадку не спрацьовують.

Відповідні прийоми відомі з древніх часів. У їхній основі лежить феномен соціальної індукції (емоційного зараження). Справа в тім, що ті емоції і почуття, які ми зазвичай переживаємо, багато в чому являють собою соціальні явища. Вони можуть поширюватися подібно до епідемії, заражаючи часом десятки і сотні тисяч людей і змушуючи маси «резонувати» в унісон. Ми істоти соціальні і легко сприймаємо почуття, що виникають в інших. Це добре помітно на рівні міжособистісних відносин - коли справа стосується близьких людей. Усім відомо, що значить «зіпсувати настрій» близькій людині і як часом легко це можна зробити. Так, мати, якою володіють негативні почуття, завжди передає їх своїй маленькій дитині; поганий настрій однієї людини може миттєво передаються іншій і т.д. Особливо сильно ефект емоційного зараження виявляється у натовпі - ситуативній людській спільноті, не зв'язаних усвідомлюваною метою. Натовп - це властивість соціальної спільності, що характеризується подібністю емоційного стану її членів. У юрбі відбувається взаємне зараження емоціями і як наслідок - їхня інтенсифікація. Природа масового емоційного зараження майже не вивчена. Одна з цікавих гіпотез стверджує, що головну роль у цьому грає виникнення резонансних коливань у

структурі електромагнітних полів, утворених людським організмом.

Механізм поведінки людини в юрбі описаний у багатьох джерелах, усі вони збігаються в тому, що людина, стаючи частиною маси, потрапляє під владу пристрастей. Типові ознаки поведінки людини в юрбі - домінування ситуативних почуттів (настроїв), втрата інтелекту, відповідальності, гіпертрофована сугестивність, легка керованість. Ці стани можна підсилити за допомогою різних засобів. Необхідні настрої викликаються за допомогою відповідного зовнішнього оточення, певного часу доби, освітлення, легких збудливих засобів, різних театралізованих форм, музики, пісень, і т.д. У психології існує спеціальний термін - фасцинація, яким позначають умови підвищення ефективності сприйманого матеріалу завдяки використанню супутніх фонових впливів. Найбільш часто фасцинація використовується в театралізованих виставах, ігрових і шоу-програмах, політичних і релігійних (культових) заходах тощо. - для зараження людей у юрбі особливим емоційним станом. На цьому тлі передається відповідна інформація, причому потрібно прагнути до того, щоб її не було занадто багато.

У сучасному світі ті емоції, що ми їх переживаємо, значною мірою є результат індукції, яку викликають засоби масової комунікації. Створення емоційного резонансу — одне з головних завдань більшості інформаційних повідомлень і розважальних шоу. ЗМІ завжди намагаються викликати в широкої аудиторії сильні емоції, і якщо необхідно, то ці емоції вони доводять до судоми. Простий приклад: зверніть увагу на ті інтонації, з якими радіо- чи телеведучі зачитують нам інформацію про події в країні й у світі. Коли мова йде про трагічні події (катастрофа, війна, терористичний акт) інтонації звичайно сповнені шляхетної скорботи чи обурення на адресу винуватців. Якщо ж, приміром, слідом за цим йде повідомлення про чергову зустріч глави держави із шахтарями (льотчиками, учителями, лікарями), ви помітите, як екранна телефізіономія миттєво перетвориться й у її голосі почнуть виразно проступати «конструктивний оптимізм» і впевненість у щасливому майбутньому нації. Цей прийом називається «емоційне підстроювання під ситуацію». Таким нехитрим способом можна формувати емоційне ставлення

масової аудиторії до тієї чи іншої події. Крім емоційного підстроювання існують і інші методи, що змушують емоційно реагувати аудиторію з потрібним ступенем інтенсивності. Один з них - риторичний прийом градація: коментатор повторює доводи з усезростаючою напругою: «Наш народ терпів, довго терпів, дуже довго терпів! Ми терпіли голод, бідність, приниження, ганьбу! Ми страждали, довго страждали, дуже довго страждали! До яких пір...» Такий прийом емоційно «заводить» слухачів. Щоб підсилити емоційну дієвість повідомлення нерідко його насичують конкретними подробицями, які краще запам'ятовуються і краще засвоюються. Особливо ефективні «свідчення очевидців», оскільки вони несуть опору на елементи особистісного досвіду людини.

Нерідкістю стало і використання російськими медіа **техніки коментування подій**, мета якої полягає у створенні необхідного контексту. Повідомлення про факт супроводжувалось інтерпретацією коментатора, який пропонував читачеві або глядачеві «розумний» варіант пояснення: *«Тем не менее, та взвешенная политика, которую проводит российское руководство в отношении происходящих на Украине событий, по признанию политологов, в настоящее время является единственно правильной…»*. При цьому здійснювався підбір фактів посилення або послаблення висловлювань та оперування порівняльними матеріалами для посилення важливості, демонстрації тенденцій і масштабності подій, явищ.

Ціль - створення такого контексту, у якому думки людини йдуть у потрібному напрямку. Повідомлення про факт супроводжується інтерпретацією коментатора, який пропонує читачу чи глядачу кілька розумних варіантів пояснення. Від спритності коментатора залежить зробити необхідний варіант найбільш правдоподібним. Американський фахівець О'Хара в книзі «Засоби інформації для мільйонів» пише про диктора: «Його повідомлення може виглядати об'єктивним у тому сенсі, що воно не містить схвалення чи несхвалення, але його вокальне доповнення, інтонація і багатозначні паузи, а також вираз обличчя часто мають той самий ефект, що і редакторська думка».

Для цього звичайно використовується кілька додаткових прийомів. Їх

активно використовують усі досвідчені коментатори. По-перше, включення в пропагандистські матеріали так званих «двосторонніх повідомлень», що містять аргументи за і проти певної позиції. «Двостороннє повідомлення» ніби випереджають аргументи опонента і при вмілій їхній критиці сприяють створенню певного імунітету проти них.

По-друге, дозуються позитивні і негативні елементи. Для того, щоб позитивна оцінка виглядала більш правдоподібною, до характеристики описуваної точки зору потрібно додати трошки критики, а ефективність осудливої позиції збільшується у випадку присутності елементів похвали. Усі використовувані критичні зауваження, фактичні дані, порівняльні матеріали при цьому добираються таким чином, щоб необхідний висновок був досить очевидним.

По-третє, здійснюється підбір фактів, які здатні посилити чи послабити враження від певних висловлювань. Висновки не входять у текст оприлюднюваних повідомлень. Їх повинні зробити ті, для кого призначена інформація.

По-четверте, відбувається оперування порівняльними матеріалами для посилення важливості, демонстрації тенденцій і масштабності подій, явищ. Необхідний ефект також можна отримати шляхом структурування подачі повідомлень.

Завдяки прийому «**обхід з флангу**» створювалось враження об'єктивності і неупередженості через включення в тексти пропагандистських матеріалів фактів, які на перший погляд несприятливі для місцевої аудиторії: *«Меня впечатлило, что там (Симферополь) ездят автомобили, на которых водители сами клеят наклейки «Я за Таможенный союз». Особенно приятно, что это не какие-то активисты, а простые граждане, которые ориентированы на интеграцию с Россией. Они не видят Украины без России, не видят Крыма без России. Поэтому именно оттуда должна быть точка кристаллизации и развития «Славянского антифашисткого фронта».* Тут розрахунок робився на поступове, неквапливе, еволюційне залучення до орбіти ідеологічних і політичних поглядів. Таке повільне, приховане залучення до сфери

пропагандистських впливів нерідко виявляється досить ефективним для людей з слабкими поглядами, які не визначили для себе прихильності до певного кола людей, образу думки і способу життя і т.п.

Головне місце в тактиці «обходу з флангу» займає пропаганда інформацією (т.зв. фактографічна пропаганда) Вона полягає в дозованої передачі достовірних відомостей, точність яких заздалегідь відома слухачам або читачам і може бути легко ними перевірена. До категорії такої «переконливою інформації» відносяться, зокрема, фактичні дані. Наприклад, імена, назви вулиць, номери будинків, величезна кількість деталей, які є достовірними і, в які як би «упаковуються» пропагандистські повідомлення.

Технологія **«буденна розповідь»** використовувалась для адаптації людини до інформації відверто негативного змісту. Такий прийом дозволяє ЗМК зберегти ілюзію об'єктивного висвітлення подій, але, в той же час, девальвує значущість певної «незручної» події, створює у масової аудиторії уявлення про дану подію як про щось малозначуще, не варте особливої уваги і, тим більше, суспільної оцінки. Через кілька тижнів такої обробки населення перестає реагувати на самі жахливі злочини і масові вбивства, які чиняться в суспільстві, настає психологічний ефект звикання: *«Нам не нужен Майдан! Нам нужен Таможенный союз с Россией, Белоруссией и Казахстаном», – говорят на предприятии. «Вы посмотрите вокруг – завод работает, значит, работает город, есть достаток в семье. Кто захочет этот достаток поломать? Можно все сломать, а потом что?» – задается вопросом сотрудник «Турбоатома» Владислав Олейник…. «У нас нет баррикад – мы работаем. Нам некогда на баррикады идти. Это на Майдане бездельники сидят…», – сказала бригадир фермерского хозяйства Валентина Резюкина…»*.

Даний прийом застосовувався, зокрема, під час державного перевороту в Чилі (1973), коли було необхідно викликати індиферентність населення до дій піночетівського спецслужб. На пострадянських просторах його активно застосовують при висвітленні масових акцій протесту, дій політичної опозиції, страйків і т.д. Наприклад, відбувається багатотисячна демонстрація противників чинного режиму, яка розганяється Беркутом (чи його аналогом) за

допомогою кийків і сльозогінного газу. Жорстоко б'ються беруть участь в ній жінки і люди похилого віку, лідери політичної опозиції заарештовують. На наступний день журналісти буденним і діловим тоном, без емоцій, мимохідь розповідають нам, що, мовляв, напередодні була проведена чергова акція протесту, органи правопорядку змушені були застосувати силу, заарештовано стільки-то порушників громадського спокою, проти яких порушено кримінальні справи «у відповідності до чинного законодавства »і т.д. Такий прийом дозволяє ЗМІ зберегти ілюзію об'єктивного висвітлення подій, але, в той же час, девальвує значимість події, створює у масової аудиторії уявлення про дану подію як про щось незначному, не вартим особливої уваги і, тим більше, громадської оцінки.

Ще одним з маніпулятивних прийомів російських ЗМІ було **відволікання уваги**. Ефективність впливу пропаганди зростає коли вона комбінується з розважальним компонентом. Пропагандистські сюжети РФ транслювались і в розважальних передачах для домогосподарок і в радіопрограмах для таксистів в різних країнах світу, де постійно повторювався міф про «неукраїнський Крим». Окрім того описуючи ситуацію в Криму систематично повторювалась теза про загрозу Заходу для РФ: «*Главные вопросы, которые обсуждают в кулуарах НАТО – насколько далеко готов пойти североатлантический альянс в поддержке Украины, что значит в контексте этой военной организации «поддержка территориальной целостности страны» и насколько вероятен сценарий открытого вооруженного противостояния НАТО с Россией»*.

Для пропаганди, як і будь-якого іншого виду маніпуляції, важливою задачею є придушення психологічного опору людини проникненню в її свідомість нав’язуваної інформації. Тому, на думку більшості фахівців, будь-яка пропаганда повинна бути комбінацією розважального, інформаційного і переконуючого компонентів. Під розвагою розуміється будь-який засіб, що збуджує інтерес до повідомлення й у той же час маскує його справжній смисл, блокує критичність сприйняття.

У 1960-і роки було виявлено, що повідомлення, спрямовані проти якої-небудь думки чи настанови, виявляються більш ефективними, якщо в момент

їхньої передачі відвернути увагу одержувача від змісту повідомлення (наприклад, програючи популярну музичну мелодію). У цьому випадку утруднюється осмислення інформації одержувачем і вироблення ним контрдоводів, які є основою опору інформаційному впливові. Дослідження 60-х років підвищили ефективність маніпуляції в пресі і на телебаченні. Газети стали застосовувати «калейдоскопічне» розташування матеріалу, розведення важливих повідомлень плітками, суперечливими чутками, сенсаціями, барвистими фотографіями і рекламою. Телебачення стало по новому компонувати відеоряд, точно підбираючи відволікаючі увагу образи. Сьогодні практично всі новинні телепередачі являють собою калейдоскопічний набір привабливих візуальних образів і інформаційних повідомлень про ніяк не пов'язані між собою події.

Завдяки **техніці перспективи** засоби масової комунікації Російської Федерації надають слово тільки одній стороні конфлікту, створюючи таким чином односторонню перспективу. Так, під час анексії Криму практично всі повідомлення російських ЗМК щодо української сторони мали негативний контекст, тоді як щодо росіян та «зеленых человечков» негатив практично був відсутній: *«События, произошедшие в феврале 2014 года в городе Киеве, резко обострили общественно-политическую ситуацию в Украине... Экстремистские группировки предприняли ряд попыток проникновения в Крым в целях обострения ситуации, эскалации напряженности и незаконного захвата власти»*.

Висвітлюючи який-небудь конфлікт, «незалежні» ЗМІ дають слово тільки одному учаснику і фактично грають на його стороні, створюючи однобічну перспективу. Зокрема, цей прийом використовується при висвітленні воєнних дій. Один з найефективніших способів пропаганди, що була застосована в процесі інформаційного супроводу анексії Криму, – невпинне повторення одних і тих же тверджень, що поступово формує звичку у населення та сприймається ним як єдине правильне. При цьому інформаційний вплив спрямовувався **не на ідеологічні установки, а на буденну свідомість громадян**: «бандеровщина», «экстремисты» «радикалы», «провокации

неофашистов в Киеве», «антиконституционный переворот», «правоэкстремистская организация «Правый сектор».

Людині завжди здається переконливим те, що вона запам'ятала, навіть якщо запам'ятовування відбулося в ході чисто механічного повторення рекламного ролика чи настирливої пісеньки. При цьому треба впливати не на ідеї і теорії супротивника, а на повсякденну свідомість, повсякденні «маленькі» думки, бажання і вчинки середньої людини. Відповідно, кваліфіковані редактори телепередач доводять текст до примітива, часто викидаючи з нього логіку і зв'язний зміст, заміняючи їх асоціаціями і грою слів. Повторення - головний засіб пропаганди. Тому воно служить гарною ознакою її наявності. Якщо раптом починають щодня мусолити ту саму тему і вживати ті самі словесні конструкції - справа нечиста. Наприклад, щорічно під час збирання врожаю організовується плач преси з приводу високих податків на дизпаливо; періодично виникають кампанії проти скасування пільг монополістам, проти заборони реклами алкоголю і тютюну; незадовго до виборів всі урядові ЗМІ, як на підбір, починають хвалити одних діячів і лаяти інших і т.д. Тут йде відома ставка на проникнення, оскільки ніяких розумних доводів звичайно не існує - просто має місце звичайне тіньове замовлення, оплачений певною кількістю банкнот із зображеннями «не наших» президентів.

Пропагандистами Кремля широко використовувалась **технологія підміни (варіант «подвійних стандартів»)**, що передбачає використання позитивних визначень (евфемізмів) для позначення негативних дій і навпаки. Цей метод переважно застосувався для створення сприятливого іміджу акту анексії. Так, анексія називалася «воссоединением», «исторической справдливостью», квазіреферендум – «демократическим актом» та «народным волеизъявлением».

Технологія полягає у використанні сприятливих визначень (евфемізмів) для позначення несприятливих дій і навпаки. Основною метою застосування прийому є створення сприятливого іміджу насильницьких дій. Так, погроми називаються «демонстраціями протесту», бандитські формування - «борцями за волю», найманці - добровольцями.

Сьогодні в західній пропаганді використовуються такі ж прийоми. У висвітленні «антитерористичних операцій» і «миротворчих акцій» уживаються вислови «захисна реакція», «обмежений повітряний удар», використовуються позначення: «моральний борг США», «програма об'єднаних сил демократії». Підривні організації, що створюються західними спецслужбами для скинення небажаних політичних режимів, отримують красиві назви типу «Національний фонд підтримки демократії», «Міжнародний демократичний форум», «Інститут відкритого суспільства», «Вільний будинок» і т.п. Коли убивають американців чи євреїв де-небудь на Близькому Сході - це тероризм; коли убивають російських солдатів у Чечні - це боротьба за незалежність і право народу на самовизначення... Узагалі, метод вербальної підміни використовується дуже широко. Якщо ви летите бомбити військові об'єкти в іншій державі... ні, ви не агресор, ви - учасник миротворчої операції. Це в нас ловлять шпигунів, у них же - наших розвідників.

Коли наші спецслужби ліквідують державних злочинців - це змушена самооборона, коли їх - це брудні політичні убивства. Коли тубільці воюють проти нас - вони «душмани» (бандити), коли на нашій стороні - «моджахеди» (борці за віру). Друга чеченська війна в Росії привела до виникнення цілого сонму вербальних підмін, покликаних «правильно» описувати ситуацію: «Це не війна, а антитерористична операція...», «Йде зачищення територій...», «Федеральні війська зайняли, федералы просунулися...». Г. Почепцов наводить цікавий приклад із уживанням/невживанням слова «кордон» стосовно Чечні. Оскільки перетинання кордону припускає акт агресії, це слово швидке зникло з лексікона російських ЗМІ.

Об’єктивна ситуація на півострові подекуди приховувалась за тезами напівправди: *«Что касается территориальной целостности, то, с одной стороны, статья 157 гласит, что основной закон Украины не может быть изменен, если изменения предусматривают отмену или ограничение прав и свобод или направлены на нарушение территориальной целостности. С другой стороны, есть статья 73 – о том, что «исключительно референдумом решаются вопросы об изменении территории Украины».…на региональный*

референдум в Конституции запрета нет. Тогда почему бы и не провести в Крыму референдум». Завдяки принципу контрасту російським ЗМК вдавалось натякнути на «несхожість» Криму з рештою України: *«Мирный Крым стабилен, многонационален, в котором все люди живут нормально. Если Украина не будет выступать угнетателем русских, как на сегодняшний день, и не будут вносить дурацкие русофобские законы, то у нас будет все нормально, все спокойно»*. Цей прийом у непрямий спосіб наводив одержувача інформації на цілком однозначні висновки, а саме – термінової необхідності від'єднатися від «нестабільної» України та стати частиною «безпечної» РФ.

Метод напівправди активно використовувався в часи розпаду СРСР. Наприкінці 1980-х років у союзних республіках виникли центробіжні тенденції. Для їхнього посилення республіканські еліти, які прагнули влади і повної незалежності від Москви, активно формували образ ворога. Впроваджувалася ідея: Росія нас грабує. Естонці були глибоко переконані, що саме вони годують весь СРСР. Та ж ідея була дуже популярна в Україні, де дуже любили підраховувати кількість областей, «працюючих» на забезпечення Москви продовольством.

Схожі міфи розроблялися в республіках Середньої Азії і на Кавказі. Вони активно використовувалися для формування і керування національними рухами, що охопили на початку 90-х років більшість союзних республік. Дійсно, республіки віддавали велику частину свого валового продукту в союзне користування. Цей факт активно використовувався для розпалення невдоволення Союзом взагалі і Москвою - зокрема. Але при цьому була зовсім «забута» та обставина, що союзні республіки одержували «з центра» нікель, олово, кадмій, нафту, газ і інші ресурси, необхідні для функціонування національних економік. Це - класичний приклад застосування напівправди. Сьогодні багатьох у Росії дратує та швидкість, з яким колишні «брати по соцтабору» зі Східної Європи зближаються в НАТО. Психологічно це не важко пояснити. У прибалтів, поляків, болгар і інших народів ще дуже свіжа пам'ять про васальну залежність від СРСР, твердий ідеологічний диктат «старшого брата».

Прийом рейтингування, що являє собою один з різновидів методу констатації факту, використовувався кремлівськими ЗМК для виправдання агресивних дій російської влади: *«Еще до начала крымского подъема более 70 процентов россиян считали, что Москва должна активнее отстаивать свои интересы на полуострове. То есть за 23 года после развала СССР мы в большинстве так и не перестали считать Крым своим».* Такі квазісоцопитування формували ілюзію «обуреного російського народу», який прагнув повернути Кримський півострів під свій контроль. Російські ЗМК застосовували схожий на прийом рейтингування і такий інструмент як соціальне схвалення (або несхвалення): *«Администрация парка имени Горького согласовала проведение первого марта публичной акции в поддержку жителей Крыма», «Крымчане не признают киевскую власть»*.

Від 10 до 25% виборців при виборі кандидатів, за яких вони будуть голосувати, керуються соціологічними рейтингами. Багато людей хочуть голосувати за сильного, але мало хто - за слабкого. Тут спрацьовує психологічний феномен, властивий середньостатистичному обивателю - бажання бути «як усі». Тому, оголосивши напередодні виборів більш високий рейтинг кандидата, можна реально збільшити кількість поданих за нього голосів. У зв'язку з цим багато соціологічних фірм у період виборчої кампанії уподібнюються представницям найдавнішої професії і починають працювати за принципом «Будь-яка забаганка за ваші гроші». «Призначаючи» лідера рейтингу вони тим самим і створюють почасти цього лідера.

У ЗМІ псевдорейтинги звичайно подаються під науковим соусом: «Опитування проводилося у всіх регіонах нашої країни. Обсяг статистичної вибірки склав 3562 чоловік. Враховано всі соціальні категорії і вікові групи. Гранична величина середньостатистичної помилки не перевищує 1,5% і т.д.» Розумні слова і наукові терміни покликані зробити вплив, що гіпнотизує, на обивателя.

Маніпулювання свідомістю завдяки **техніці сенсаційності** було спрямовано на підвищення рівня нервозності і підрив психологічного захисту громадян Криму. Базуючись на принципі про те, що відчуття безперервної

кризи різко підвищує сугестивність людей і знижує здатність до критичного сприйняття, практично всі новинні блоки в російських ЗМК щодо України мали сенсаційне забарвлення: *«Ситуация в Крыму продолжает накаляться», «У крымского парламента прогремел взрыв», «Последняя экономическая надежда Крыма рухнула», «Аэропорт Симферополя захвачен вооруженными людьми», «Крым оставили без правительства», «А ведь кризис только нарастает. В частности, самый нескрываемый – долговой»*.

Прийом швидкої дії, що забезпечує необхідний рівень нервозності і підриває психологічний захист. Ця нервозність, відчуття безупинної кризи, різко підвищує сугестивність людей і знижує здатність до критичного сприйняття. Справа в тім, що будь-яка маніпуляція досягає успіху, коли вона випереджає процес мобілізації психологічного захисту аудиторії, коли їй удається нав'язати свій темп нашій свідомості. Саме тому сьогодні практично всі новинні блоки в ЗМІ починаються з т.зв. «сенсаційних повідомлень»: серійних убивств, авіаційних катастроф, терористичних актів, скандалів з життя політиків чи шоу-зірок. Насправді терміновість повідомлень майже завжди буває помилковою, штучно створеною. Іноді сенсаційність служить для відволікання уваги. Звичайно така «сенсація» не коштує виїденого яйця, - то слониха в зоопарку народила, то в тунелі автобус з вантажівкою зштовхнувся, то підліток зґвалтував і убив свою бабусю. Наступного дня про це усі забувають. Під прикриттям сенсації можна або замовчати важливу подію, про яку публіка знати не повинна, або припинити скандал, якщо вже настав час припинити - але так, щоб про нього більше ніхто не згадував. Тому сенсаційність тісно зв'язана з прийомом «Відволікання уваги»

З метою прикриття окупаційних заходів кремлівські медіа вдавалися до **прийому зміщення акцентів** *«…ни один участник брюссельских мероприятий не произнес слов осуждения действий радикальных элементов, непрекращающегося давления и запугивания представителей оппозиционных партий, журналистов, наступления на русский язык, вмешательства в дела церкви, осквернения православных храмов и мемориалов. Ожидали также, что западные представители поддержат соглашение от 21 февраля, под которым*

стоят подписи трех министров иностранных дел трех ведущих стран-членов НАТО», а також **техніки створення проблеми**: «*Выжидательная автономия: возможен ли переход Крыма к России. В Крыму не без оснований опасаются, что в случае, если националисты придут к власти, они уничтожат автономный статус полуострова»*.

Завдяки цим прийомам досягався, зокрема, високий рівень значущості вигаданих проблем для населення, оскільки як правило найбільш актуальними люди вважають саме ті проблеми, які найдокладніше висвітлюються в засобах масової комунікації. Створюючи тематичне домінування в інформаційному просторі, нав'язується певне бачення ситуації, а реальні проблеми суспільства, як злочинність, соціальна нерівність, відсутність свободи слова, безробіття залишаються поза увагою. Близьким за сутністю до прийому створення проблеми, що активно експлуатувався Москвою, є **прийом створення загрози**. ЗМК нагнітали істерію з приводу, наприклад «фашистської загрози», прагнучи деморалізувати населення та викликати масовий страх з метою створення сприятливої атмосфери для маніпуляції масовою свідомістю*: «Это только кажется, что после освобождения Украины от фашизма прошло 70 лет… Фашисты для жителей юго-востока Украины – это те самые необандеровцы, оккупировавшие киевский Майдан, швырявшие в милицейские кордоны коктейли Молотова. …».*

Його головна задача - будь-яким способом змусити нас боятися. Деморалізовані і залякані люди роблять чи хоча б схвалюють дії, що цим людям зовсім не вигідні. Найчастіше технологія наступна. Ілюзорна чи реально існуюча небезпека якого-небудь явища (наприклад, тероризму) багаторазово підсилюється і доводиться до абсурду. ЗМІ влаштовують істерію з приводу чергової «глобальної погрози», викликаючи в людей масовий страх з метою створення сприятливої обставини для маніпуляції масовою свідомістю - насамперед, у політичних цілях.

Міняються часи і люди, але пропагандистська технологія «створення глобальної погрози» залишається незмінною. Віртуальний світ (наприклад, війна у Чечні чи Афганістані), створений ЗМІ, стає обивателю набагато

ближчим і важливішим, ніж безробіття чи корупція правлячої верхівки у власній країні. У цьому дана технологія співзвучна з пропагандистським прийомом Відволікання уваги. Створення погрози - один з найдужчих засобів маніпуляції свідомістю і відволікання уваги громадськості від махінацій верхівки.

«Переорієнтування агресії - це найпростіший і самий надійний спосіб знешкодити її. Вона задовольняється ерзац-об'єктами легше, ніж більшість інших інстинктів, і знаходить у них повне задоволення» (Конрад Лоренц, «Агресія») Ще це - ефективний засіб акумулювати негативну енергію суспільного невдоволення і переключати її на «безпечні» чи вигідні цілі. У соціальній психології метаморфози подібного роду нерідко позначаються як «пошук козла відбувала".

Нав'язування необхідної позиції мешканцям Криму здійснювалось Кремлем також завдяки **технології упереджувального удару**: *«Ситуация в Крыму продолжает накаляться… Впервые в истории Крым имеет возможность самоопределиться… Это не только русские, но и крымские татары. Все они считают, что судьбу полуострова нужно решать на референдуме», «Крымчане не хотят жить в бандеровском государстве... Речь может идти о расширении прав республики и разграничении полномочий между Крымом и Украиной, независимости или присоединении к России».* Таким чином міф про гостру необхідність проведення референдуму щодо самовизначення Криму був свідомо «вкинутий» в медіапростір півострову.

Найчастіше являє собою упереджувальний викид негативної інформації. Його задача - викликати реагування супротивника заздалегідь і в більш вигідному для себе контексті. Цей прийом нерідко використовують владні структури, щоб нейтралізувати критику майбутніх непопулярних рішень. У даному випадку влади самі організовують «випадковий» витік негативної інформації, щоб стимулювати прояви суспільного обурення. Це робиться для того, щоб заздалегідь «випустити пару» у всіх незадоволених. Якщо це зроблено вчасно, то на момент настання «Дня Х» багаття народного гніву уже встигає згаснути. До моменту ухвалення відповідного рішення люди

утомляться протестувати і сприймуть дії влади індиферентно.

У випадку використання інструментарію «отруйного сендвічу» комунікатор (Росія) надавав позитивну інформацію поміж негативною, приховуючи, наприклад, супутні деструктивні фактори діяльності проросійських «захисників» на території АРК: «И все это на фоне уже привычных угроз о каком-то военном походе на автономию из Киева. В Крыму говорят, что готовы ко всему и надеются на помощь России. На полуострове сейчас все спокойно. И спокойно в первую очередь потому, что люди, готовые к борьбе, теперь точно знают, за что идет вся эта борьба. …Это все – колыбель русского православия. Здесь не может быть двух мнений о том, кто здесь должен быть».

Цей пропагандистський прийом активно використовує можливості психологічного впливу за рахунок структуризації тексту. Завжди краще не брехати, а домогтися, щоб людина не помітила «непотрібної» правди.

Комунікатор дає позитивне повідомлення між негативною передмовою і негативним висновком. При наявності у комунікатору певних здібностей і досвіду позитивне повідомлення може лишатися непоміченим аудиторією. Це дуже гарний прийом, активно використовуваний тими ЗМІ, що претендують на «об'єктивне висвітлення подій» і прагнуть створити собі імідж у стилі «тільки факти, нічого крім фактів». При такому структуруванні подій об'єктивність формально дотримана, але ефект «непотрібних» повідомлень девальвований.

Додаток В

ДОСЛІДЖЕННЯ ХАРАТАЕРИСТИК ЦІЛЬОВОЇ АУДИТОРІЇ СІО

Дослідженню підлягають передусім наступні характеристики аудиторії:

1. **Соціальний статус кінцевого споживача інформації**. Ця характеристика є ключовою, базовою для проведення подальшого аналізу цільової аудиторії. Оскільки в залежності від того, хто є кінцевим споживачем інформації (студент, пенсіонер, військовослужбовець, науковець, підприємець, безробітний, хворий тощо), різняться й механізми та прийоми ІПВ;

2. **Статевий склад цільової аудиторій**. З еволюційним розвитком людства склалися певні відмінності сприйняття та поширення інформації чоловіками та жінками. Тому, в залежності від статевої належності об'єкта, мають розроблятися окремо і засоби поширення інформації, і прийоми впливу на підсвідомість та свідомість цільової аудиторії.

3. **Середній вік цільової аудиторії**. Вік споживачів інформації також відіграє важливу роль при здійсненні ІПВ. Через вікові відмінності люди по-різному сприймають та інтерпретують інформацію. Тому на етапі планування СІО необхідно враховувати, що люди старшого віку користуються відмінними від молоді джерелами отримання та поширення інформації тощо.

4. **Рівень освіти**. При дослідженні об'єктів ІПВ варто враховувати рівень освіти та загальний рівень ерудиції й обізнаності. Окрім рівня освіти необхідно враховувати й час його отримання. Оскільки база та ідеологічна направленість освіти Радянського союзу беззаперечно відрізняється від освіти незалежної України, виникають відмінності у сприйнятті та реакції на інформацію людей зазначених освітніх систем.

5. **Фахова підготовка цільової аудиторії**. Знання фахової підготовки цільової аудиторії дозволить точніше та ефективніше здійснити ІПВ на визначений об'єкт впливу.

Окрім психологічної характеристики цільової аудиторії необхідно визначити зональність проведення спеціальної інформаційної операції, а саме

виокремити **територію її проведення**. Важливо також установити такі характеристики, як місця проживання, роботи та отримання соціальних послуг, найбільш усталені маршрути пересування, а також місця скупчення людей у певний момент часу. Зазначені характеристики відносяться до **інформаційної логістики, інформаційної структури цільової аудиторії** та **територіальності** СІО.

У розрізі інформаційної логістики доцільно знати джерела отримання інформації цільовою аудиторією та поширення цієї інформації серед її представників.

1. **Джерела отримання інформації**. Телебачення, радіо, газети, журнали, сайти, групи та сторінки у соціальних мережах. Важливо не тільки визначити пропорції співвідношення споживання інформації з тих чи інших джерел, але й визначити конкретний перелік найбільш популярних серед представників цільової аудиторії засобів масової інформації, лідерів суспільної думки, інтернет-сайтів, сторінок та груп у соціальних мережах. Окрім зазначеного варто детально проаналізувати не тільки наявність чи відсутність тих чи інших джерел в «інформаційному раціоні» споживача, але й дати характеристику джерелам, а саме тематиці джерел (політика, спорт, мода), ідеологічному забарвленню (ліберальні, нейтральні, центристські тощо), формату інформації (комікси, випуски новин на телебаченні чи радіо, записи у соціальних мережах лідерів суспільної думки тощо).

Визначивши перелік джерел отримання інформації цільовою аудиторією, організатори можуть виокремити вибір інформаційних ресурсів, лідерів суспільної думки, адміністраторів сайтів, сторінок та груп у соціальних мережах, які необхідно взяти під контроль чи (та) залучити до СІО. Відбір найбільш авторитетних та найбільш відвідуваних джерел інформації збільшить ефективність ІПВ через охоплення ширшої аудиторії та довіри до інформаційних матеріалів, що розроблені відповідними органами СБУ.

2. **Джерела поширення інформації в середині цільової аудиторії**. Означає визначення кола осіб, які є «генераторами», «передавачами» та безпосередньо «споживачами» інформації, а також основні майданчики, де

циркулює інформація (сторінки та групи в соцмережах і на форумах, місця громадського харчування, паління, тощо).

Використовуючи зазначені місця можна поширювати інформацію фактично оминаючи лідерів і передавачів та додатково охопити нецільову аудиторію.

Джерела отримання та поширення інформації всередині цільової аудиторії можуть перетинатись між собою та дублювати один одного. Завдання підготовчого етапу СІО полягає у визначенні таких джерел для оптимізації використання сил та ресурсів при здійсненні ІПВ на цільову аудиторію. Окрім цього, це дозволить автономізувати поширення інформації серед споживачів інформації, тим самим мінімізуючи як витрати сил та ресурсів, так і ризики викриття спроб ІПВ з боку СБУ.

Наступним кроком підготовчого етапу СІО є дослідження **інформаційної структури цільової аудиторії** за такими характеристиками:

1. **«Генератори» інформації чи лідери суспільної думки**. Ця категорія людей генерує інформаційні потоки, які проходять через цільову аудиторію. До них відносяться експерти, політологи, окремі блогери, науковці та використання медійних майданчиків (сайтів, форумів), що мають значний попит серед представників цільової аудиторії. Зазначена категорія є найменшою за чисельністю, проте вона є найбільш впливовою. Відповідно, залучення такого роду осіб та майданчиків до проведення СІО збільшить ефективність ІПВ на цільову аудиторію.

2. **«Передавачі» інформації**. Це люди, що виконують функцію мультиплікаторів інформації. До них відноситься основна маса журналістів, користувачів соціальних мереж, другорядних та маловідомих ЗМІ тощо. Ця група людей є більшою від попередньої і не менш цінною для СБУ, оскільки саме вони здійснюють розповсюдження інформації. Контроль та (або) моніторинг зазначених осіб дає можливість не тільки фіксувати динаміку та тенденцію поширення тієї чи іншої інформації, але й створювати своїх власних, по відношенню до СБУ, лідерів суспільної думки з можливістю впливати на наступну категорію людей.

3. **«Споживачі» інформації**. Найбільш чисельна група. Фактично, саме вона є цільовою аудиторією СІО, на яку має бути направлений ІПВ і саме ця група підпадає під найретельніший аналіз з метою визначення найбільш доцільних інформаційних джерел передачі інформації до кінцевого споживача.

Варто зазначити, що соціальні мережі є динамічними та багатогранними структурами і будь яка особа, мережеве ЗМІ, група чи сторінка у соціальних мережах може бути водночас і лідером суспільної думки, і «передавачем», і «споживачем». Відповідно, при підготовці до проведення СІО організатори мають чітко визначити інформаційну структуру цільової аудиторії, роль та місце кожного із учасників СІО та об'єктів ІПВ.

Наступним кроком підготовчого етапу є визначення зональності СІО:

1. Територіальні, коли цільова аудиторія значну частину часу знаходиться в межах певної території, розміщена відносно рівномірно по площі, групи цільової аудиторії не розірвані між собою або знаходяться на відносно незначній відстані між собою, мають спільні джерела отримання та передачі інформації, або ці джерела між собою пересікаються тощо. Прикладом такої цільової аудиторії можуть бути військовослужбовці та членів їх сімей у визначеному місті. Відповідно, ІПВ здійснюється на аудиторію, що компактно розташована у кварталах міста, де проживають військовослужбовці та військові пенсіонери. Відповідно, всі зусилля ІПВ мають бути зосереджені саме на цій ділянці компактного проживання без розпорошення сил та засобів по всій території населеного пункту.

2. **Екстериторіальні**, коли цільова аудиторія розміщена неоднорідно в межах великої площі, групи її представників розірвані між собою, можуть не мати спільних джерел отримання та передачі інформації, або ці джерела між собою не пересікаються. Прикладом такої цільової аудиторії є така категорія населення, як молодь, що проживає, навчається та працює в різних місцях визначеного населеного пункту та отримує інформацію з різних джерел. У такому випадку зусилля ІПВ щодо донесення інформації мають бути зосереджені з урахуванням певних факторів та моделей поведінки цільової аудиторії. Представники цієї цільової аудиторії можуть знаходитися в різних

місцях в залежності від **дня та часу доби** (робота, ВНЗ, дім, нічний клуб тощо), **погодних та кліматичних умов** (в сезон дощів молодь проводить більше часу в приміщеннях, у ясну погоду – на вулиці), **маршрутів пересування та точок скупчення** (дорога до ВНЗ, метрополітен та інший громадський транспорт), де у них є можливість отримати інформацію як у друкованому вигляді так і в усному). Враховуючи викладене, оптимізацію ІПВ на визначену аудиторію можливо здійснити через звуження кола можливих джерел поширення інформації та збереженням кількості її споживачів.

3. **Змішані**, коли представники цільової аудиторії мають певні спільні ознаки (місце проживання, отримання соціальних послуг, робота, маршрути пересування). Наприклад, якщо представники цільової аудиторії компактно проживають в одному мікрорайоні, але працюють в різних місцях, чи навпаки. У такому випадку пропонується сфокусувати увагу на місцях максимальної концентрації представників цільової аудиторії у певний період часу, як то вихід з метрополітену, де можна організувати роздачу друкованих інформаційних матеріалів.

Запропонований набір характеристик цільової аудиторії є рамковим і може бути змінений у залежності від завдань та умов проведення СІО.

Додаток Д

ПРОТИДІЯ ІНФОРМАЦІЙНІЙ БЛОКАДІ АВТОНОМНОЇ РЕСПУБЛІКИ КРИМ ТА ПРОНИКНЕННЯ ДО ІНФОРМАЦІЙНОГО ПРОСТОРУ АНЕКСОВАНОГО ПІВОСТРОВУ

Стан інформаційного поля України 2013-14 років сприяв виникненню такого явища як **інформаційна бульбашка** або **бульбашка фільтрів** у майже всього населення нашої держави. Відповідно до політичних вподобань а також інформаційно-психологічних прийомів керівництва Російської Федерації, яке попередньо впродовж довгого періоду часу проводило інформаційну та суспільно-політичну експансію у відповідні сфери суспільного життя півострову, населення АР Крим так чи інакше потрапило до інформаційного простору нашого північно-східного сусіда.

Разом із бульбашкою фільтрів, яка сформувалась самостійно на тлі кризових явищ та процесів в українському суспільстві, російською окупаційною владою у інформаційному просторі Криму було створено інформаційне гетто, відповідно чого мешканці анексованого півострову отримують інформацію переважно з місцевих проросійських джерел та федеральних російських інформаційних каналів.

В той же час можна твердо стверджувати, що Крим живе українською порядком денним, значна кількість новин в інформаційному просторі півострову стосується стану речей континентальної України. Однак ці новини подаються у певному, найчастіше негативному, ключі із відповідним контекстом.

Ще до моменту підступної анексії Автономної республіки Крим (далі – АРК, Крим) Російська Федерація (далі – Росія, РФ) активно нарощувала присвою присутність у інформаційному просторі Криму, здійснюючи мовлення через супутниковий зв'язок, кабель та відкриваючи філіали своїх центральних федеральних ЗМІ. А вже 9 березня 2014 року, за тиждень до т.зв. референдуму

про приєднання Криму до Росії, який відбувся 16 березня того ж року, було припинено мовлення українських телеканалів із їхньою заміною на російські. З прийняття нового закону, що розширив права Роскомнагляду (рос. Роскомнадзор, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) по блокуванню сайтів які містять екстремістську (з точки зору влади) інформації як, наприклад, заклик до несанкціонованих мітингів. На практиці, в розрізі гібридної агресії Росії проти України, це рішення вилилось у блокування доступу російським користувачам до ряду українських сайтів. Так російською владою було додано до Єдиного реєстру заборонених сайтів такі інформаційні ресурси як Liga.net, Цензор.net, События Крыма. Окрім блокування інформаційних ресурсів, російська влада заблокувала доступ до ряду груп та пабліків у соціальній мережу «Вконтакте», серед яких Євромайдан, Правий сектор (сама організація була визнана екстремістською), Українська революція та інші.

Для відновлення доступу мешканців Криму до об'єктивної та неупередженої інформації українська влада почала зведення радіовеж уздовж адміністративного кордону з тимчасово анексованим півостровом. У березні 2017 року було зведено вежу у Чонгарі з якого розпочато радіомовлення а згодом буде розпочато і трансляція українських телеканалів у бік анексованого кримського півострову.

Отже, внаслідок створення окупаційною владою інформаційного гетто в Криму склалась такі умови:

- обмежено мовлення українських теле- та радіоканалів;
- обмежено доступ до українських Інтернет видань та інформаційних джерел у соціальних мережах;
- інформаційна монополія російських ЗМІ, що поширюють лише заангажовану та спеціально підготовлену інформацію

В той же час відзначається інтерес мешканців анексованого Криму до подій на території континентальної України, інформацію про які отримують через супутникову трансляцію.

В рамках загальної мети відновлення територіальної цілісності України, а

саме повернення АР Крим до складу України в т.ч. через проведення СІО перед СБ України стоїть завдання проникнення до інформаційного простору півострову та поширення спеціально підготовленої інформації, відповідно до цілей та завдань СІО.

Відтак, на прикладі інформаційних заходів волонтерів, під умовною назвою «Рука помощи» можна запропонувати наступні можливі організаційні заходи проникнення до інформаційного простору Криму.

Так, волонтерами було створено розгалужену мережу акаунтів у всіх соціальних мережах («Фейсбук», «Вконтакте», «Одноклассники») а також сайтах і форумах проросійського та сепаратистського направлення. Впродовж певного періоду часу через зазначені акаунти проводились бесіди та зав'язувались контакти з представниками проросійські налаштованих громадян а також осіб, що співчувають сепаратистам та терористам. Разом з цим проводились регулярні «посіви» (масове поширення спеціально підготовленої інформації із широким охопленням аудиторії). В результаті було встановлено контакти з представниками російського телеканалу «Лайфньюз», яким передали нібито копії документів про початок програми «Рука помощи», яка фінансуватиметься Агентством США з міжнародного розвитку (United States Agency for International Development, USAID), в рамках якої буде створена мережа інфільтраційних таборів. У якості реабілітаційних заходів, згідно з програмою, нібито було передбачена повна амністія учасників незаконних збройних формувань, надання місць роботи, молоді (до 30 років) організація безкоштовного навчання у країнах Східної Європи тощо (див.мал.1-3).

Окрім публікації вищезазначених документів, для розвитку та посилення ефекту публікації було розроблено та поширено нібито відповідь на вказані документи від імені очільника Луганської обласної військово-цивільної адміністрації Павла Жебрівського (див.мал.4).

Такий комплект документів, створений достатньо якісно, хоча і не позбавлений певних фактологічних та інших дрібних помилок, став своєрідною інформаційною бомбою для російської аудиторії. Сюжет про таку програму був показаний у ефірі телеканалу а також розміщений на його сайті. Сенсаційність

та скандальність інформації відіграла позитивну роль, що відбилось у статистиці передруків (більше 90) та охоплення надзвичайно широкої аудиторії (більше 70 мільйонів осіб).

У якості фінального акорду було записано нібито звернення представника терористичної організації до Президента України Петра Порошенка з вимогою надання гарантій реалізації зазначеної програми та надання вичерпного переліку документів та кроків які необхідно здійснити йому та його товаришам для включення у програму. Таке відео також було широко поширене мережею Інтернет (див. мал. 5-7.)

Зазначений волонтерський захід є не тільки чудовим прикладом проникнення у інформаційний простір Російської Федерації але й прикладом спонукання до реакції представників. Так, у відповідь на поширення спеціально підготовленої інформації серед російської аудиторії стосовно програми реабілітації членів НЗФ колишній української політик Олег Царьов заявив про неможливість підкупу «ополченців». Інший одіозний, псевдоопозиційний політик Едуард Лімонов також відерагував на вкид інформації, заперечивши будь-яку можливість до підкупу бойовиків.

мал 1.

Національної програми «Рука допомоги». Координацію і формування та керівництво робочою групою залишаю за собою.

Прошу попередньо опрацювати та підготувати пропозиції щодо формалізації базових положень Програми (відповідно до профілю кожного відомства), яка передбачатиме:

- повну амністію усім хто складає зброю та перейде на територію контрольовану українською владою;
- надання гарантованого соціального пакету (житло, грошова допомога, робота);
- надання іноземцям, як біженцям, громадянства України з можливістю надання громадянства та притулку в Україні також членам їх родин;
- надання молоді (до 30 років) можливості безоплатного навчання в українських ВНЗ або у ВНЗ деяких країн Східного партнерства (Польща та Чехія);
- можливість перейти (в тому числі діючим військовослужбовцям ВС РФ) до лав ВСУ або Національної гвардії із збереженням військового звання і можливістю навчання на курсах НАТО з отриманням нової військової спеціальності;
- отримання кредитів на створення в Україні власного бізнесу.

Робоча група з розробки Програми має підготувати документ до 07.09.2015 р. Перше засідання робочої групи призначається на 22.07.2015 р. Початок реалізації Програми передбачається з 01.10.2015 р.

Головам Донецької та Луганської обласних адміністрацій підготувати пропозиції з організації таборів тимчасової інфільтрації осіб що підпадають під дію Програми. Термін виконання – 15.07.2015 р.

Головам Міністерства внутрішніх справ України та Служби безпеки України підготувати пропозиції щодо створення комісій з перевірки осіб що підпадають під дію Програми. Термін виконання – 15.07.2015 р.

мал.2.

Голові Служби безпеки України, підготувати пропозиції щодо організації окремої лінії для видачі та повторного оформлення осіб що відповідають під дію Програми. Термін виконання – 15.07.2015 р.

А також Міністру внутрішніх справ України та Голові Служби безпеки України підготувати пропозиції з створення механізмів безпечного переходу бажаючих скористатися Програмою по території контрольованій українською владою. Термін виконання – 31.07.2015 р.

Контроль за виконанням даного доручення залишаю за собою.

Міністр Кабінету Міністрів

мал.3.

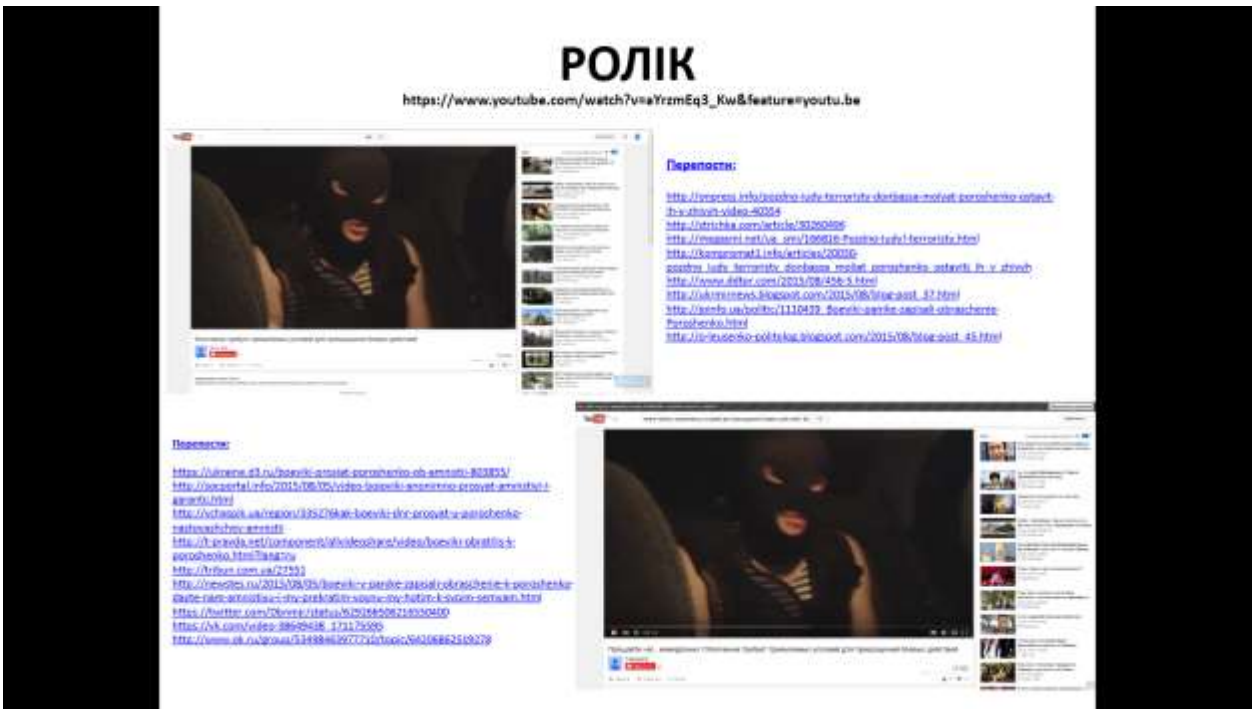
УКРАЇНА
ДОНЕЦЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ДОНЕЦЬКА ОБЛАСНА ВІЙСЬКОВО-ЦИВІЛЬНА АДМІНІСТРАЦІЯ

Міністру кабінету міністрів України

Голова
обласної державної адміністрації,
керівник обласної
військово-цивільної
адміністрації

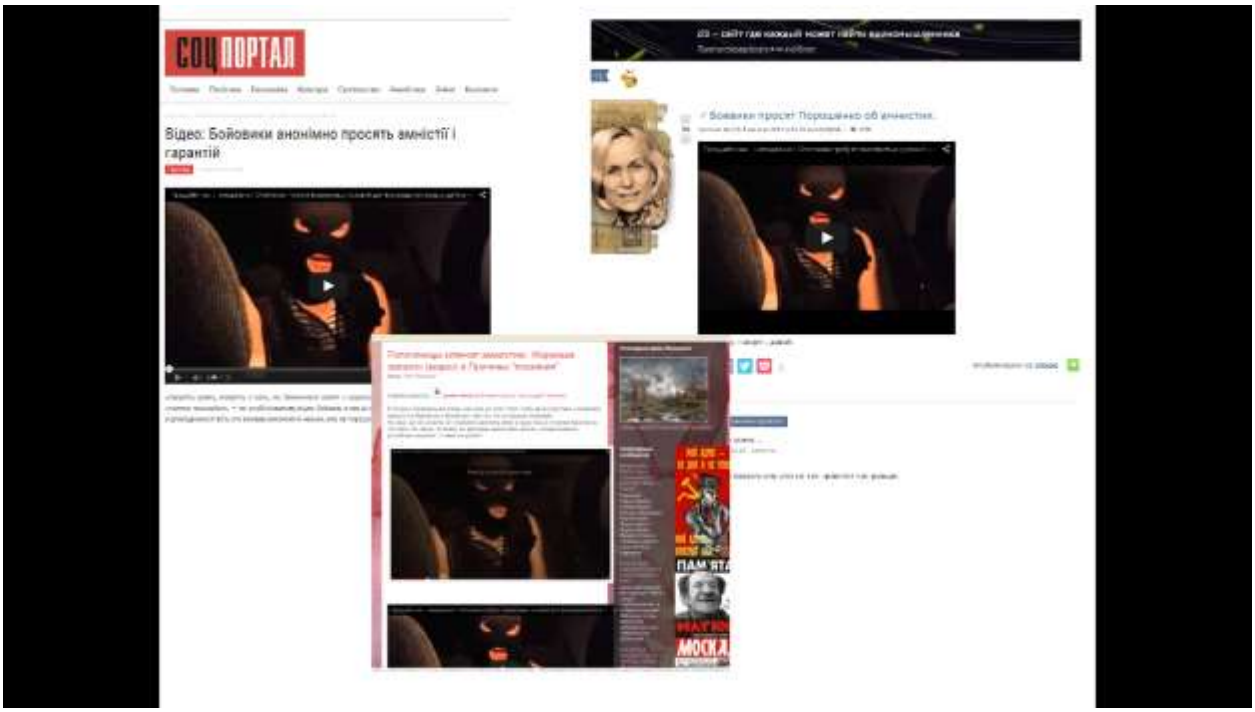
О.І. Жебрівський

мал. 4.



мал 5.

мал.6



мал. 7.

Створення фейкових осіб, які можуть представлятись співробітниками українських міністерств або відомств, що мають прихильність до Росії та підтримують анексію Криму. Впродовж певного часу ця персона чи коло осіб мають «популяризуватись» та входити у довіру до цільової аудиторі. Для цього має бути створена відповідна «**легенда**» та дотримуватись **необхідна лінія поведінки**.

Із отриманням достатнього рівні довіри стає можливим організація передачі інформації а також спроби виведення необхідних осіб на континентальну Україну.

У випадку необхідності поширення спеціально підготовленої інформації з мінімізацією ризиків блокування доступу до джерела можна розглянути варіант створення **груп та пабліків у соціальних мережах та (або) сайту проросійського напрямку** і використовуючи **технологію «бутерброд»** вносити до інформаційного простору анексованого півострову зазначену вище інформацію. Технологія «бутерброд» полягає у наступному: між інформаційними блоками «істина» розмішається блок «брехня». В результаті сприйняття блоків інформації у такій структурі блок «брехня» сприймається як «істина» і вкорінюється у інформаційний простір.

Створення власних інформаційних ресурсів у інформаційному просторі Криму дозволить обійти негативні асоціації з вже наявними українськими медіа, які вже мають певну впізнаваність або характеристики, які можуть підірвати довіру до інформації, яку вони транслюють. Серед таких, наприклад, українська назва, український домен (net.ua, com.ua, .ua, ukr), українська мова ведення сайту тощо. У випадку реєстрації сайту у російському сегменті мережі Інтернет, формування проросійської позиції інформаційного ресурсу можна без зайвих ризиків викриття

Створення, розвиток та просування таких інформаційних джерел у інформаційному просторі АРК дозволить вирішити питання поширення спеціальної підготовленої інформації та розширення аудиторії. В той же час функціонування таких джерел потребує досконалого знання всіх аспектів місцевої політики, соціально-економічного становища, внутрішньополітичних відносин між різними групами впливу та образу мислення місцевого населення.

У випадку вдалої та ефективної реалізації задуму створення такого джерела або системи джерел можливо досягти завдання просування, поширення та вкорінення необхідної інформації в умовах активної інформаційної та контррозвідувальної протидії з боку спеціальних служб Російської Федерації

Окрім створення сайту чи (та) групи (пабліку) у соціальних мережах можна розглянути можливість **створення окремого фейкового персонажу** для розкрутки його як блогера (журналіста) з метою поширення спеціально підготовленої інформації. У сучасних умовах популярності соціальних мереж, блогосфери, популяризувати акаунт у соціальній мережі завдання відносно не складне, єдине питання, яке виникає під час реалізації такого задуму – наявність достатньої кількості часу та навичок правильної поведінки у соціальних мережах та мережі Інтернет у осіб, які залучені та виконують функцію популяризацію таких персонажів.

Як видно із вищенаведеного, найкращий варіант проникнення до інформаційного простору, який знаходиться у під прискіпливим контролем спеціальних служб Російської Федерації, який фактично перетворений у інформаційне гетто – створення джерела безпосередньо у цьому гетто. Сучасні технології створення web-сторінок, поширення матеріалів у соціальних мережах, відносна дешевизна замовлення рекламних кампаній значно спрощують завдання входження, розвитку та поширення інформації у інформаційному просторі.

З точки зору оптимального майданчику для початку популяризації «персони» чи (та) сайту є соціальна мережа «Вконтакте», як така, що є найпопулярнішою соцмережею як на території тимчасово анексованого півострову так і в Російській Федерації. Разом з цією мережею варто взяти до уваги місцеві кримські форуми, як то, наприклад, «Крымский форум» (Crimea-Board), «Крым». «Крымский форум», «Симферопольский форум», «Форум Крыма на Перекопе - Крым на Перекоп.Инфо» тощо.

Специфіка діяльності будь-яких форумів полягає у тому, що при розміщені покликань на таких майданчиках відбуваються наступні речі:

- пошукові «роботи» систем Гугл та Яндекс індексують ці покликання і додають рейтинг сайту чи (та) сторінці
- на форумах користувачі частіше переходять за лінками, ніж у звичайних соціальних мережах;
- на форумах більш активні користувачі на предмет реакцій та

встановлення контактів ніж у соціальних мережах.

На нашу думку, комбінація група чи/та сайту а також інших ресурсів, таких як канал у соціальній мережі «Твітер», пабілк (група) у мережі «Фейсбук», група (паблік) у мережі «Однокласники», комплексне використання яких дозволить досягти наступних завдань:

- індексація пошуковими роботами пошукових систем;
- широке охоплення аудиторії;
- диверсифікація джерел поширення інформації.

Протидія інформаційному захисту та жорсткий контррозвідувальний режим, який встановлено окупаційною владою на території Автономної республіки Крим вимагає нестандартних дій для проникнення, поширення та вкорінення спеціально підготовленої інформації у інформаційний простір кримського півострову. Для цього можна створити фейкових персон, які будуть видавати себе за державних службовців, що симпатизують країні агресору через які можна здійснювати вкиди у інформаційний простір Криму або створювати умови для виводу на підконтрольну територію цікавих для СБ України осіб. Також перспективним вважається можливість створення Інтернет-медіа, яке загалом буде притримуватись проросійської позиції однак час від часу буде здійснювати поширення спеціально підготовленої інформації. Окремо стоїть можливість створення персони «блогера» чи «журналіста», який може здійснювати аналогічні до ЗМІ поширення інформації.

Додаток Е

МАТРИЦЯ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ СИНЕРГЕТИЧНОЇ МОДЕЛІ СІО

Синергетична модель СІО					
Проблема, яка потребує вирішення					
Законодавчі засади проведення СІО					
Правові обмеження у проведенні СІО					
підмережі	підмережа збору інформації				
	підмережа комунікацій				
	підмережа аналізу інформації				
	підмережа прийняття рішень				
	підмережа виконаня рішень				
спрямування		Наступнальні СІО		Оборонні СІО	
аспект		розвідувальний	контррозвідувальний	розвідувальний	контррозвідувальний
характер	технічні				
	психологічні				
вид	новинарні				
	комунікативні				
	наукові/ культурні				
тактика	зміна ставлення до предмету, явища, події				
	зміна поведінки об’єкта				
	зміна світогляду				
суб’єкт	сили сектору безпеки і				

	оборони				
	допоміжні суб'єкти (ЗМІ, лідери громадської думки тощо)				
об'єкт	конкретна особа або коло осіб, суспільство, держава				
	процес				
	дискурс				
цільова аудиторія	стать				
	вік				
	освітній рівень				
	соціальний статус				
	фахова підготовка				
	регіон проживання				
	джерело отримання інформації				
	джерело поширення інформації				
	Інформаційна структура цільової аудиторії				
	«генератори»				
	передавачі				
	споживачі				
територія	територіальні				
	екс-територіальні				
	змішані				

Ефективність		Критичність наслідків		Зменшення вразливості	
	збройні сили				
	спецслужби				
	правоохоронні органи				
	критична інфраструктура				

	населення				
	терористичні, кримінальні або інші протиправні утворення				
Безпекове середовище	сильні сторни				
	слабкі сторони				
	загрози				
	можливості				
Можлива протидія	спецслужби іноземних держав				
	міжнародні організації				
	іноземні неурядові установи, громадські організації, ЗМІ				
	українські неурядові установи, громадські організації, ЗМІ				
	населення іноземних держав				
	населення України				
	терористичні, кримінальні або інші протиправні утворення				
ризики	високий				
	низький				
	середній				

Алгоритм СІО

Етап	Час	Учасники	Зміст	Очікуваний

				результат
підготовчий етап				
інформаційний етап				
етап планування				
етап реалізації				
етап виходу				
Форми і способи зворотного зв’язку між учасниками, а також між етапами з метою аналізу ефективності їх виконання та внесення необхідних коректив.				

* графи таблиці, позначені сірим кольором, заповнюються у текстовому форматі конкретними відомостями, необхідними для проведення СІО.

* графи таблиці, позначені зеленим кольором, заповнюються опціонально, з використанням шкали якісної оцінки від 0 до 3 (використання відповідної шкали дозволяє визначити, якою мірою задіюється в ході проведення СІО той чи інший напрямок, передбачений синергетичною моделлю).

Додаток Ж

ПРОБЛЕМИ ІНФОРМАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

(на прикладі операції «Гюльчатай» центру «Миротворець»)

У якості прикладу СІО пропонуємо розглянути операцію «Гюльчатай» (далі – Операція), яка була проведена міжнародним центром «Миротворець» (далі – Миротворець)[2].

Навесні 2015 року невідомими (на той момент) було вбито проросійського журналіста та публіциста Олеся Бузину (16.04.2015) та колишнього народного депутата від Партії регіонів, Олега Калашнікова (15.04.2015). Адміністраторами однойменного сайту центру «Миротворець» «заднім числом» було розміщено на сайті профілі вбитих з місцями проживання, фотографіями, контактними даними тощо, а опісля — розміщено статтю про нагороду «агента 404» (*прим. авт – 404 — це код помилки, що міститься у відповіді сервера на запит користувача та свідчить про відсутність запитуваної інформації на сервері*) за успішну ліквідацію зазначених осіб. Інформація про це (стосовно розміщення профілю, подальшого вбивства та «нагородження агента») була широко поширена серед проросійськи налаштованих користувачів мережі Інтернет та дійшла до потенційних і чинних на той момент членів терористичних організацій «Луганська народна республіка», «Донецька народна республіка» та інших афільованих до них бандитських угруповань та злочинців.

Оскільки доступ пересічному користувачу мережі Інтернет до бази даних терористів та осіб, що підозрюються у співпраці з терористичними

---

[2] Спецоперация «Гюльчатай, открой личку!» или сказ о том, как мы «разводили» вату, пользуясь методами российских пропагандистских СМИ. (Часть 1): [Електронний ресурс]. – Режим доступу: https://psb4ukr.org/189342-specoperaciya-gyulchataj-ili-skaz-o-tom-kak-my-razvodili-vatu/(дата звернення 04.12.2018).
Спецоперация «Гюльчатай, открой личку!» или сказ о том, как мы «разводили» вату, пользуясь методами российских пропагандистских СМИ. (Часть 2): [Електронний ресурс]. – Режим доступу: https://psb4ukr.org/190529-specoperaciya-gyulchataj2/(дата звернення 04.12.2018).

організаціями та з країною-агресором (Російська Федерація), що розміщена на сервері центру «Миротворець», можливий лише через форму пошуку, особи, що потенційно можуть бути у зазначеній базі та переймались за свою безпеку (підозрювані у вбивстві О. Бузини А. Медведько та Д. Поліщук були затримані значно пізніше) могли пересвідчитись про наявність чи відсутність своїх даних у зазначеній базі лише після того, як власноруч введуть свої ім'я та прізвище. У свою чергу, адміністратори сайту «Миротворець» мають можливість фіксувати всі дані, що вводяться користувачами у форму пошуку (ім'я, по-батькові, прізвище, позивний тощо) та, користуючись технологією OSINT (одна з розвідувальних дисциплін, що включає в себе пошук, вибір і збір інформації, отриманої із загальнодоступних джерел і її аналіз), проводити подальше наповнення бази новими підозрюваними у тероризмі та співпраці з терористичними організаціями.

Таким чином, операція публічно складалась з наступних етапів:

1. ***Підготовчий етап.***

Фактично, підготовчий етап у даній конкретній операції був відсутній, оскільки організатори використали наявний інформаційний привід та наявні адміністративні та оперативні ресурси, напрацьовані попередніми операціями.

2. Інформаційний привід.

Як інформаційний привід було використано наявну подію, гучне вбивство.

В даному випадку у плануванні СІО було задіяно схему, яку використовують засоби масової інформації (далі – ЗМІ) з метою «зачепити» користувача та утримати його увагу. Найбільш активно сучасні ЗМІ використовують схему «СССССГ», де відповідно: Скандали, Сенсації, Страх, Секс, Смерть, Сміх та Гроші: (6 С + Г). Кожна із зазначених тем викликає 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. Тож завдання організаторів СІО – у підготовчому етапі визначити

домінантний тип емоційного стану цільової аудиторії, а у випадку відсутності можливості (під час інформаційного етапу, перед проведенням інформаційного приводу) – здійснити комплекс інформаційних акцій, які створять необхідний емоційний стан або підсилять наявний емоційний стан, необхідний для подальшого ефективного інформаційного етапу.

Повертаючись до вищенаведеної схеми, використана в ході СІО «Гюльчатай» тема підпадає під ознаки **«сенсація»** (смерть проросійськи налаштованих широковідомих осіб). Варто зазначити, що така ситуація (майже одночасна смерть відомих опозиційних, радикально проросійських медійних особистостей) виникла вперше у новітній історії України. Представники центру «Миротворець» додали елемент **«страх»,** увівши неіснуючого агента «404» із натяком на те, що будь-яка особа, яка перебуває в базі центру «Миротворець», є під загрозою фізичної ліквідації. Завдяки комплексу дій з боку центру «Миротворець» інформацію стосовно наявності профілів зазначених осіб було широко поширено серед проросійської аудиторії, в тому числі така інформація була поширена центральними ЗМІ РФ та популярними проросійськими й російськими блогерами і журналістами, тим самим посіявши панічні настрої серед потенційних учасників бази центру «Миротворець» та спровокувавши їх на наступну дію — пошук самих себе на сайті центру «Миротворець», що стало наступним етапом операції «Гюльчатай».

*3. **Закріплювальний етап.***

Особи, які відносили себе до тих, хто може бути у базі центру «Миротворець» та переймались за власну безпеку й маючи доступ до бази виключно через форму пошуку на сайті, почали активно шукати себе у зазначеній базі, тим самим власноруч вносили свої дані (прізвище, ім’я, по-батькові, позивний) у цю базу, мимовільно надаючи команді центру «Миротворець» інформацію про себе. Це розширення бази і було ціллю операції. Побічним та корисним результатом операції було поширення страху, демонізація центру «Миротворець» в очах терористів та їхніх поплічників, що розширило можливості та цінність центру «Миротворець».

4. Вихід з операції.

Після того, як командою центру «Миротворець» було зібрано достатньо інформації, на сайті проекту було розміщено інформацію про операцію, її цілі завдання та перебіг із саркастичною подякою всім її учасникам з числа терористів та їх прибічників.

З використанням НЛП-теорії про референтний стан мас можна зробити такий висновок, що в даному випадку цільова аудиторія гучною подією була введена в стан пасивного негативу (жах від інформації про смерть О. Бузини та О. Калашнікова) а представниками центру «Миротворець» доведена до стану активного негативу – страх за власне життя, що штовхнуло потенційних (на їхню власну думку) жертв «агента 404» на пошук самих себе у базі центру «Миротворець».

Отже, фактично перед організаторами СІО стоїть завдання започаткування контрольованого поширення та направлення психічної енергії в руслі, відповідно до задуму організаторів операції. Варто зазначити, що у суспільстві одночасно обертається велика кількість інформації, адже відбувається політична боротьба, протидія гібридній агресії РФ, країна переживає економічну кризу тощо, відповідно населення постійно перебуває під постійним зовнішнім психологічним тиском. Більше того, цей тиск на суспільство відбувається масовано і комплексно, з різних джерел (ЗМІ, соціальні мережі, чутки тощо) та цілодобово отже як для інформаційних операцій, так і для інформаційних приводів виникають чи можуть виникнути будь-які обставини, які у свою чергу можуть вилитися у будь-які ситуації, і не тільки спецслужби, але й треті сторони можуть їх використати у своїх цілях.

До проблемних аспектів операції «Гюльчатай» при цьому можемо віднести недостатнє дослідження безпекового середовища проведення СІО, а також неврахування ризиків проведення СІО. Зокрема, не врахована можливість випадків, за яких користувачі мережі Інтернет з цікавості вводять до пошуку у базі «Миротворець» відомості про своїх знайомих незалежно від того, чи вони дійсно причетні або підозрюються у причетності до діяльності на шкоду Україні.

Додаток З

«ЗАТВЕРДЖУЮ»
Т.в.о. директора Науково-дослідного інституту інформатики і права Національної академії правових наук України,
доктор юридичних наук, с.н.с
О. Д. Довгань
«4» липня 2019 року

АКТ

впровадження результатів дисертаційного дослідження Верголяса О.О. на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право на тему: ***«Правове забезпечення спеціальних інформаційних операцій»***

Комісія у складі: завідувача наукової лабораторії, доктора юридичних наук, старшого наукового співробітника Коржа І.Ф.; ученого секретаря кандидата юридичних наук Беланюк М.В.; завідувача наукової лабораторії, кандидата юридичних наук, доцента Дороніна І.М. склала цей акт про те, що результати дослідження на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право Верголяса Олександра Олександровича на тему: «Правове забезпечення спеціальних інформаційних операцій», використані у науковій діяльності Інституту, а саме в рамках планових дослідницьких тем Науково-дослідного інституту інформатики і права Національної академії правових наук України "Теоретичні та організаційно-правові основи забезпечення кібербезпеки в Україні" (№ державної реєстрації 0116U007745) та «Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері» (№ державної реєстрації 0117U007745) у частині надання пропозицій з проблематики інформаційно-правового забезпечення спеціальних інформаційних операцій, а також розробленні рекомендації щодо його вдосконалення, виявлення специфіки спеціальних інформаційних операцій як інструменту ведення інформаційної війни та засобу забезпечення національної безпеки, визначення їх місця в системі засобів протидії загрозам національній безпеці України тощо, а також частково при підготовці пропозицій щодо удосконалення законодавства в сфері національної безпеки та інформаційній сфері.

Члени комісії:

доктор юридичних наук, с.н.с. *І.Ф.Корж*
кандидат юридичних наук *М.В.Беланюк*
кандидат юридичних наук, доцент *І. М. Доронін*

Додаток К

ДОВІДКА

про апробацію та впровадження результатів дисертаційного дослідження Верголяса О.О. на тему: «Інформаційно-правове забезпечення спеціальних інформаційних операцій» на здобуття наукового ступеня кандидата юридичних наук

Результати дисертаційного дослідження Верголяса О.О. на тему «Інформаційно-правове забезпечення спеціальних інформаційних операцій» апробовано та впроваджено в діяльності Служби безпеки України в ході нормативно-правового супроводження процесу реформування Служби.

Зокрема, пропозиції дисертанта щодо включення до повноважень Служби безпеки України права «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» враховано при підготовці на виконання п.6 Прикінцевих і перехідних положень Закону України «Про національну безпеку України» нової редакції Закону України «Про Службу безпеку України» (відповідний законопроект 12 грудня 2018 року скеровано до Адміністрації Президента України за № 99/884).

Помічник Голови СБ України
доктор юридичних наук,
заслужений юрист України **Д.Прокоф'єва-Янчиленко**
«20» червня 2019 р.

Підпис засвідчую

Т.в.о. начальника РСВ
Апарату Голови СБ України **С.Синельниченко**
«20» червня 2019 р.