УДК 340+681.3

ВЕРГОЛЯС О.О., аспірант НДІІП НАПрН України

ІНФОРМАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Анотація. *В цій статті проаналізовано роль та місце інформаційного етапу спеціальних інформаційних операцій (на прикладі операції "Гюльчатай" центру "Миротворець") у загальному алгоритмі проведення спеціальних інформаційних операцій, а також розглянуто актуальний стан та проблеми правової регламентації спеціальних інформаційних операцій на сучасному етапі.*

Ключові слова*: інформаційні операції, спеціальні інформаційні операції, інформаційні війни, інформаційний привід, стратегічні комунікації.*

Summary. *This article analyzes the role and place of the information phase of the special information operations (on the example of Operation "Gulchatay" of the "Peacemaker" Center) in the general algorithm for carrying out special information operations, as well as the current state and problems of legal regulation of special information operations at the present stage.*

Keywords: *information operations, special information operations, information wars, information retrieval, strategic communications.*

Аннотация. *В этой статье проанализированы роль и место информационного этапа специальных информационных операций (на примере операции "Гюльчатай" центра "Миротворец") в общем алгоритме проведения специальных информационных операций, а также рассмотрены актуальное состояние и проблемы правовой регламентации специальных информационных операций на современном этапе.*

Ключевые слова: *информационные операции, специальные информационные операции, информационные войны, информационный повод, стратегические коммуникации.*

Постановка проблеми. Поняття "ноосфери", запропоноване французьким ученим Едуардом Леруа та розвинене його сучасниками Пьером Тейяр де Шарденом та В.І. Вернадським, наприкінці минулого століття набуло нового значення. У 1990-х роках експерти аналітичного центру RAND адміністрації США Дж. Аркилла 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 [1]. Інформаційна війна являє собою 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. [2, с. 204, 108-109].

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 [3, с. 191-193].

На сьогоднішній день жодними нормативно-правовими актами України не врегульований та не закріплений алгоритм проведення спеціальних інформаційних операцій (далі – СІО), що відбивається на ефективності й результативності зазначених заходів. Прогалина у законодавстві частково компенсується сталою практикою владних структур, на які покладені функції з проведення СІО, що, однак, повністю не вирішує питання проведення ефективних операцій з вигідного впливу на цільову аудиторію СІО.

Вдосконаленню нормативно-правової бази, яка регулює діяльність вітчизняних спецслужб та правоохоронних органів в частині правової регламентації проведення СІО може сприяти належне теоретичне підґрунтя, зокрема, розроблений науковцями загальний алгоритм проведення СІО [4], оптимізації якого, у свою чергу, має сприяти комплексне дослідження інформаційного етапу СІО, яке має на меті збільшити ефективність як інформаційно-психологічного впливу на цільову аудиторію, так і оптимізувати використання людських та матеріально-технічних ресурсів в ході проведення СІО.

Результати аналізу наукових публікацій. Питання організації та планування СІО при забезпеченні національної безпеки та у правоохоронній діяльності розглядались такими вченими як Богданова Ю., Голубев С., Гриняев С., Зуева Н., Иванов И., Козирацкий Ю., Кушнір О., Ланде Д., Ліпкан В., Лизанчук В., Литвиненко О., Макаренко С., Панченко В., Прохоров Д., Резепов И., Чадов И., Черных С., Фурашев В.

У той же час слід констатувати, що наразі залишаються недостатньо вивченими проблеми, пов’язані із дослідженням інформаційно-правового забезпечення СІО.

Метою статті є визначення ролі та місця інформаційного етапу СІО у загальному алгоритмі проведення СІО, а також актуального стану правової регламентації проведення СІО на сучасному етапі, вироблення на цій основі певних рекомендацій щодо вдосконалення інформаційно-правового забезпечення СІО.

Виклад основного матеріалу. Розпочинаючи дослідження проблематики СІО, передусім слід визначитись з категорією більш загального порядку – інформаційними операціями, котрі є складовою інформаційної війни. 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 [5].

У сучасних умовах не викликає сумніву також і той факт, що інформаційні операції можуть проводитись не лише у воєнній, але й в інших сферах забезпечення національної безпеки, зокрема, у правоохоронній, що додатково підсилює роль та значення інформаційних операцій в умовах ведення гібридної війни.

За характером завдань, які вирішують інформаційні операції, вони класифікуються на оборонні і наступальні. Метою оборонних інформаційних операцій – забезпечення виконання цільових завдань інформаційними й керуючими системами в умовах ведення інформаційної війни, а також забезпечення схоронності інформаційних ресурсів і запобігання витоку, викривлення, втрати або викрадення інформації в результаті несанкціонованого доступу до неї з боку супротивника. Метою наступальних інформаційних операцій є досягнення й утримання інформаційної переваги в інформаційній війні. Наступальні інформаційні операції являють собою комплексне проведення за єдиним задумом і планом заходів щодо оперативного маскування, радіоелектронної боротьби, програмно-математичного впливу на інформаційно-керовані системи, фізичного знищення (або виведення з ладу) об’єктів інформаційної інфраструктури. У ході таких операцій здійснюються заходи, що передбачають вплив на

свідомість людей і спрямовані на зрив процесу прийняття рішень, а також дії з метою порушення роботи або знищення елементів інформаційної інфраструктури [2; 6 – 7].

У ході інформаційних операцій використовуються різні прийоми протиборства: одержання інформації про супротивника як у результаті аналізу відкритої інформації, що циркулює в ЗМІ, інформаційних системах тощо, так і в результаті її перехоплення, несанкціонованого доступу з наступним викривленням, знищенням, "перекодуванням" з метою формування оцінки, наміру й орієнтацій населення й осіб, що ухвалюють стратегічні рішення; придушення елементів інфраструктури державного й військового управління; радіоелектронна боротьба тощо. Методи інформаційної війни надзвичайно різноманітні: дезінформація, пропаганда, наклеп, неправда, приховування істотної інформації, зсув понять, відволікання уваги, інформаційне табуювання й інші.

Фахівці також визначають інформаційні операції як сукупність заходів гласного та негласного характеру, спрямованих на приховане керування процесами інформаційної сфери. На відміну від пропагандистських заходів, вони мають обмежену у часі тривалість, підпорядковані конкретній меті та координуються єдиним центром – спеціальними службами [4]. Зокрема, як інформаційні операції в ході гібридної війни РФ проти України В. Панченко характеризує події навколо обстрілу блокпоста під Слов'янськом, після якого вщент згоріло все майно, але залишились неспаленими паперові візитівки лідера Правого сектору Д. Яроша, а також фішингову атаку на сайт ЦВК України під час виборів Президента України у травні 2014 року, коли відображені на ньому результати голосування свідчили про перемогу знову ж таки Д. Яроша [8, с. 14-15]. Фактично в даному випадку мова йде про СІО.

Отже, СІО – це інформаційні операції, які проводяться в інтересах забезпечення національної безпеки з використанням сил безпеки і оборони [9] (у даному випадку вважаємо недоцільним запропонований С. Макаренком поділ інформаційних операцій за метою та завданнями на інформаційне забезпечення, СІО та інформаційне протиборство [5], адже в сучасних умовах СІО з високою результативністю застосовуються саме як інструмент інформаційного протиборства).

Наразі 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 [10]. Втім згадана Доктрина жодним чином не регламентує власне проведення СІО та не дає уявлення про їхню сутність. Певною мірою цю прогалину усуває Воєнна доктрина України, яка опосередковано визначає СІО як елемент стратегічних комунікацій.

Зокрема, у ч. 16 ст. 4 розділу 1 Воєнної доктрини України зазначається, що стратегічні комунікації 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 [11]. Втім таке визначення одночасно додає нових питань в частині розуміння СІО як правового феномену, зокрема – у чому полягає різниця між інформаційними і психологічними операціями, і чи не може за допомогою СІО відбуватися просування цілей держави.

Слід зауважити, що спираючись на стандарти НАТО науковці вирізняють серед компонентів системи стратегічних комунікацій безпосередньо інформаційні операції

(Information Operations) та психологічні операції (PSYOPS), однак до проведення СІО можуть мати безпосереднє відношення також інші компоненти цієї системи, зокрема:

- інформаційні заходи міжнародного військового співробітництва (International Military Cooperation);
- дії в кіберпросторі, включаючи соціальні мережі;
- залучення ключових лідерів до проведення інформаційних заходів (Key Leaders Engagement);
- інформування про ситуацію (Visual Info/Situation Awareness);
- документування подій на полі бою (Combat Camera);
- розвідувальне забезпечення проведення інформаційних заходів;
- демонстрація дій військ (Show of Force);
- введення в оману (MILDEC);
- безпека операцій (Operation Security);
- протиборство в електромагнітному просторі (EMW) тощо [12 – 15].

СІО можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки інформаційного протиборства.

При інформаційно-технічній боротьбі головними об'єктами впливу й захисти 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.

Як зазначають В. Фурашев та Д. Ланде, зміст СІО спрямований на реалізацію попередньо спланованих психологічних дій в мирний і воєнний час на ворожу, дружню або нейтральну аудиторію засобами впливу на настанови та поведінку з метою досягнення політичних або воєнних переваг. Ці операції поєднують психологічні дії зі стратегічними цілями, психологічні консолідуючі дії та психологічні дії з безпосередньої підтримки бойових дій.

Основне завдання інформаційних операцій полягає у маніпулюванні масами на рівні суспільної та індивідуальної свідомості найчастіше з метою:

- внесення у свідомість ворожих, шкідливих ідей та поглядів;
- дезорієнтації та дезінформації мас;
- послаблення певних переконань, устоїв;
- залякування свого народу образом ворога;
- залякування супротивника своєю могутністю;
- забезпечення ринку збуту для своєї економіки [16, с. 49-50].

Квінтесенцією інформаційного забезпечення СІО інформаційно-психологічного характеру є їх інформаційний етап, тож на його дослідженні зупинимось детальніше.

Інформаційний етап СІО передбачає створення чи/та вибір інформаційного приводу як тригеру (автоматичні поведінкові реакції людини, що виникають у відповідь на яку-небудь подію) [17 – 19] для всієї операції. 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 суб'єктів СІО (особу чи коло осіб) до вчинення певних дій чи до бездіяльності відповідно до намірів, цілей та оперативного задуму організаторів операції.

Загалом, у плануванні ІПВ можна користуватись схемою, 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" [20]. Кожна із зазначених тем викликають окрему, специфічну реакцію в аудиторії, що і є головною метою інформаційного етапу СІО у процесі підбору чи створення інформаційного приводу. Саме запланованe 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.

Інформаційний привід є невід'ємною частиною СІО і повинен бути тісно пов'язаний з третім етапом операції – закріпленням результатів ІПВ, оскільки інформаційний привід є тригером до дії чи бездіяльності цільової аудиторії в рамках СІО, адже саме дія чи бездіяльність і є головною метою ІПВ, результати якого фіксуються у закріплювальному етапі СІО.

У якості прикладу інформаційного приводу в СІО пропонуємо розглянути СІО "Гюльчатай" (далі – операція), яка була проведена міжнародним центром "Миротворець" [21 – 22].

Навесні 2015 року невідомими (на той момент) було вбито проросійського журналіста та публіциста Олеся Бузину (16.04.2015 р.) та колишнього народного депутата від Партії регіонів, Олега Калашнікова (15.04.2015 р.). Адміністраторами однойменного сайту центру "Миротворець" "заднім числом" було розміщено на сайті профілі персональних даних, вбитих з місцями проживання, фотографіями, контактними даними тощо, а опісля – розміщено статтю про нагороду "агента 404" (404 – це код помилки, що міститься у відповіді сервера на запит користувача та свідчить про відсутність запитуваної інформації на сервері – *прим. Авт.*) 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 афілійованих до них бандитських угруповань та злочинців.

Оскільки доступ пересічному користувачу мережі Інтернет до бази даних терористів та осіб, що підозрюються у співпраці з терористичними 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 (А. Медведько та Д. Поліщук, підозрювані у вбивстві О. Бузини, 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. 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 цієї конкретній операції відсутній, оскільки організатори використали наявний інформаційний привід та наявні адміністративні та оперативні ресурси, напрацьовані попередніми операціями.

2. Інформаційний привід. Використано наявну подію, гучне вбивство. Повертаючись до вищенаведеної схеми, 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” відомостями, стосовно наявності профілю персональних даних, зазначених осіб було широко поширено серед проросійської аудиторії, в тому числі такі відомості були поширені 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” 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 персональні дані (прізвище, ім’я, по-батькові, позивний) у цю базу, мимовільно надаючи команді центру “Миротворець” відомості 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 відомості 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.

В цілому формалізація етапів проведення СІО на теоретичному рівні має синхронізуватися із вдосконаленням нормативно-правового підґрунтя їх проведення, котре, як вже зазначалося вище, наразі не може вважатися не лише досконалим, але й елементарно достатнім. Доцільним у подальшому вдосконаленні нормативно-правового регулювання СІО вважаємо орієнтування на стандарти НАТО, перевагою яких є впровадження у практику планування та проведення СІО детального аналізу комплексу факторів обстановки, механізмів координації складових сектору безпеки і оборони та інших державних органів, групових методів роботи, відпрацьованих й перевірених провідними зарубіжними країнами при забезпеченні національної безпеки прийомів й способів інформаційного впливу [9, с. 153-154].

Висновки.

Наразі важливо передусім визначити сутність та місце СІО в системі засобів забезпечення інформаційної та національної безпеки України в цілому, а також окреслити основні вимоги до їх проведення (з урахуванням специфіки всіх основних етапів СІО) з метою забезпечення балансу інтересів національної безпеки та дотримання прав і свобод людини й громадянина, унеможливлення використання інформаційних потужностей для провокації злочинів тощо.

Необхідно враховувати, що у розробці та проведенні СІО інформаційний привід посідає одне з найважливіших місць у операції, оскільки він є точкою входу в процес мотивації чи демотивації цільової аудиторії відповідно до оперативного задуму, цілей та завдань організаторів СІО, які відображаються у наступному етапі операції – фіксувальному, який є віддзеркаленням всієї операції у якому цільова аудиторія здійснює чи відмовляється від здійснення своїх дій, відповідно до оперативного задуму, цілей та завдань організаторів СІО.

Відповідно, правильний та коректний підбір наявного інформаційного приводу чи створення нового інформаційного приводу є одним із найважливіших етапів у проведенні СІО. При цьому впровадження сектором безпеки і оборони України методології проведення СІО, яка використовується у країнах НАТО, та нормативно-правове закріплення відповідних стандартів значно посилить спроможності нашої держави у веденні інформаційного протиборства в умовах гібридної війни.

Використана література

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

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

3. Черных С.Н., Зуева Н.А. Информационная война: традиционные методы, новые тенденции. *Контекст и рефлексия: философия о мире и человеке*. 2017. Т. 6. № 6А. С. 191-199.

4. Литвиненко О.В. Інформаційні впливи та операції. Київ: ВКФ. Сатсанга, 2003. 240 с.

5. 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).

6. Козирацкий Ю.Л., Прохоров Д.В., Козирацкий А.Ю., Голубев С.В. Основы информационной и радиоэлектронной борьбы: учебное пособие. Воронеж: ВАИУ, 2009. 192 с.

7. Иванов И., Чадов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века. *Зарубежное военное обозрение*. 2011. № 1. С. 14-20. URL: http://militaryarticleru/zarubezhnoe-voennoe-obozrenie/2011-zvo/8094-soderzhanie-i-rol-radiojelektronnoj-borby-v (дата звернення 02.12.2018).

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

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

10. Доктрина інформаційної безпеки України: затверджена Указом Президента України "Про рішення Ради національної безпеки і оборони України від 29.12.16 р. "Про Доктрину інформаційної безпеки України". URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення 28.11.2018).

11. Про рішення Ради національної безпеки і оборони України "Про нову редакцію Воєнної доктрини України": Указ Президента України від 2.09.15 р. № 555/2015: http://www.president.gov.ua/documents/5552015-19443 (дата звернення: 30.11.2018).

12. 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).

13. Ліпкан В.А. Сутність гібридної війни проти України. *Імперативи розвитку цивілізації*. 2015. № 2. С. 13-16.

14. 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).

15. Daniel Gage. The continuing evolution of Strategic Communication within NATO. *The Three Swords Magazine*. 27/ 2014. P. 53-55.

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

17. Богданова Ю.О. Психология маркетинга. URL: http://www.aup.ru/books/m500; http://www.gumer.info/bibliotek_buks/psihol/olshansk/15.php (дата звернення: 30.11.2018).

18. Резепов И. Психология рекламы и PR. URL: http://www.e-reading.club/book.php?book=89173 (дата звернення: 29.11.2018).

19. Лизанчук В. Психологія мас-медіа. URL: http://journ.lnu.edu.ua/books/ps-mas-media.pdf (дата звернення: 05.12.2018).

20. Сім орієнтирів "ТСН": Скандали, Сенсації, Страх, Смерть, Секс, Сміх і Гроші. URL: http://ru.telekritika.ua/redpolitics/2008-06-04/38798 (дата звернення: 03.12.2018).

21. Спецоперация "Гюльчатай, открой личку!" или сказ о том, как мы "разводили" вату, пользуясь методами российских пропагандистских СМИ. Ч. 1. URL: https://psb4ukr.org/189342-specoperaciya-gyulchataj-ili-skaz-o-tom-kak-my-razvodili-vatu (дата звернення: 04.12.2018).

22. Спецоперация "Гюльчатай, открой личку!" или сказ о том, как мы "разводили" вату, пользуясь методами российских пропагандистских СМИ. Ч. 2. URL: https://psb4ukr.org/190529-specoperaciya-gyulchataj2 (дата звернення: 04.12.2018).

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