процесів, як забезпечення здійснення правосуддя відповідно до встановлених демократичних стандартів. В Європейському Союзі діє спеціальна програма сприяння для підвищення адміністративної спроможності та розвитку судової гілки влади («Action Plan for strengthening administrative and judicial capacity»). Метою реалізації програми є оцінка ефективності діяльності суб'єктів публічного управління, в тому числі судових органів, аналіз узагальненої звітності щодо результатів відбувалися обмін найкращим досвідом, узагальнення та вироблення рекомендацій [14].

Отже, впровадження Європейського адміністративного простору в Україні передбачає застосування європейських принципах публічного управління (адміністрування), забезпечення високоефективної системи публічної служби, реалізації міжнародних договорів та програм сприяння; контролю стандартів якості громадських послуг, дотримання обов'язкових процедурах консультування із громадськістю, урахування прецедентного практики Європейського Суду з прав людини як джерела національного законодавства тощо.

ЛІТЕРАТУРА

1. Preparing Public Administration for the European Administrative Space. SIGMA Papers № 23. URL: www.sigmaweb.org/pdf/SIGMA_SP23_98E/pdf
2. Панейко Ю.Л. Наука адміністрації і адміністративного права: у 2 т. Загальна частина. Авґсбурґ, 1949. 118 с.
3. Публічна служба. Зарубіжний досвід та пропозиції для України / за заг. ред. В.П. Тимощука, А.М. Школика. Київ : Конус Ю, 2007. 735 с.
4. Авер'янов В., Андрійко О. Актуальні завдання створення нового законодавства про державну службу в Україні. *Юридичний журнал.* 2005. № 8(38). С. 53–55.
5. Цуркан М.І. Правове регулювання публічної служби в Україні. Особливості судового розгляду спорів : монографія. Харків : Право, 2010. 216 с.
6. Старилов Ю.Н. Курс общего административного права: в 3 т. Москва : НОРМА, 2002. Т. I: История. Наука. Предмет. Нормы. Субъекты. 728 с.
7. Про запобігання корупції : Закон України від 14.10.2014 р. № 1700-VII. *Відомості Верховної Ради України* (ВРР). 2014. № 49. Ст. 2056.
8. Рунова Н. Публічна служба в Україні: проблеми дефініції. *Публічне право*. 2012. № 3(7). С. 269–274.
9. Линник Т.В. Теоретико-правова проблематика реформування публічної служби в Україні. *Форум права*. 2012. № 3. С. 553–558.
10. Кодекс адміністративного судочинства України від 06.07.2005 р. *Відомості Верховної Ради України*. 2005. № 35–37. Ст. 446.
11. Механізми координації європейської політики: практика країн-членів та країн-кандидатів / Н. Гнидюк (ред.), А. Новак-Фар, Я. Гонцяж, І. Родюк. Київ : Міленіум, 2003.
12. Перелік програм та фінансових інструментів ЄС, відкритих для України. URL: http://www.mk.gov.ua/store/files/announce_1499425690.pdf
13. About ISA². URL: https://ec.europa.eu/isa2/isa2_en
14. Horizon 2020. URL: http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016-2017/annexes/h2020-wp1617-annex-ga_en.pdf

УДК 342.9
DOI https://doi.org/10.32782/2524-0374/2019-4/26

ПРОБЛЕМНІ ПИТАННЯ ПРОВЕДЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ СЕКТОРОМ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

PROBLEMATIC ISSUES OF SPECIAL INFORMATION OPERATIONS PERFORMED BY THE SECURITY AND DEFENSE SECTOR OF UKRAINE

Верголяс О.О., аспірант Науково-дослідного інституту інформатики і права
Національна академія правових наук України
виконавчий директор
Інформаційне агентство «Петро і Мазепа медіа»

У статті доводиться, що найнебезпечнішою загрозою інформаційній безпеці, як на міжнародному, так і на національному рівні, в сучасних умовах виступає інформаційна війна, причому спеціальні інформаційні операції (СІО) одночасно можуть використовуватись і як інструмент ведення інформаційної війни, і як інструмент забезпечення інформаційної й національної безпеки. Також аналізуються актуальні проблеми проведення СІО складовими елементами сектора безпеки і оборони України. Основна проблема проведення СІО сектором безпеки і оборони України полягає, передусім, у слабкій нормативній урегульованості, а точніше – у відсутності належних правових засад для проведення СІО. Воєнна доктрина України і Доктрина інформаційної безпеки України опосередковано визначають СІО як елемент стратегічних комунікацій, що загалом відповідає загальносвітовому тренду. При цьому правові межі для проведення стратегічних комунікацій визначені п. 2.7 Концепції стратегічних комунікацій Міністерства оборони України та Збройних сил України, де, зокрема, визначено, що СІО не проводяться стосовно 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, поза межами району проведення антитерористичної операції або інших місць (районів) підготовки та застосування Збройних сил. У статті обґрунтовується, що відсутність правової регламентації проведення СІО в мирний час ускладнює можливість їх проведення не лише Збройними силами України та іншими військовими формуваннями, але й іншими складовими елементами сектора безпеки і оборони відповідно до їх компетенції. Крім того, залишається фактично позбавленим належного правового підґрунтя проведення СІО структурами силам безпеки з метою протидії деструктивним СІО, спрямованим проти України. Таким чином, констатується необхідність подальшого розвитку правової основи проведення СІО сектором безпеки і оборони України, а також потреба впровадження в практику регламентації, планування і проведення СІО в Україні стандартів НАТО.

Ключові слова: інформаційне протиборство, спеціальні інформаційні операції, правове регулювання, стандарти НАТО.

The article states that information warfare is the most dangerous threat to information security, both at the international and national levels, and that special information operations (SIO) can be used both as a tool for information warfare and as an instrument for providing information and national security. The actual problems of conducting SIO in the components of the security and defense sector of Ukraine are also analyzed. The main problem of the SIO in the security and defense sector of Ukraine is, first of all, in the weak normative settlement, or rather, in the absence of the proper legal framework for the SIO. The Military Doctrine of Ukraine and the Doctrine of Ukraine's Information Security indirectly define the SIO as an element of strategic communications, which in general corresponds to the global trend. At the same time, legal limits for strategic communications are defined in art. 2.7 of the Strategic Communications Concepts of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, where, inter alia, it is determined that the current legislation does not stipulate conducting of the SIO against Ukrainian citizens (except the members of terrorist groups and illegal armed formations), as well as conducting the SIO in the territory of Ukraine outside the area of the anti-terrorist operations or other places (areas) of the preparation and use of the Armed Forces. The article substantiates that the lack of legal regulation of conducting SIO in peacetime complicates the possibility of their carrying out not only by the Armed Forces of Ukraine and other military formations, but also other components of the security and defense sector in accordance with their competence. In addition, it remains virtually devoid of proper legal basis for conducting SIO by security forces structures in order to counter the destructive SIO directed against Ukraine. It is thus stated that further development of the legal basis for the performing SIO by the Security and Defense Sector of Ukraine is necessary, as well as the introduction of the NATO standards in the regulation, planning and implementation of SIO in Ukraine.

Key words: information confrontation, special information operations, legal regulation, NATO standards.

Найнебезпечнішою загрозою інформаційній безпеці, як на міжнародному, так і на національному рівні, в сучасних умовах виступає інформаційна війна, причому спеціальні інформаційні операції (далі – СІО) одночасно можуть використовуватись як інструмент ведення інформаційної війни, так і як інструмент забезпечення інформаційної безпеки. Нині інформаційні відносини не просто достатньо розвинені – вони набувають характеру визначальних, суттєво опосередковуючи інші суспільні відносини, отже, загрози інформаційній безпеці, особливо коли йдеться про індустріально-розвинені країни, нині досить реальні. Відсутність належного правового регулювання в питаннях інформаційної безпеки та інформаційного протиборства може дати змогу деяким державам та угрупованням здійснювати напади в рамках інформаційної війни, уникаючи відповідальності за зазначені дії [1]. Тож нині забезпечення інформаційної безпеки, межі ведення інформаційних війн та, зокрема, проведення СІО − це та сфера, де ефективне правове регулювання та належна регламентація необхідні вже нині.

Дослідженню питань здійснення стратегічних комунікацій суб'єктами сектору безпеки і оборони та, зокрема, проведення СІО складовими елементами сектору безпеки і оборони України приділяли увагу у своїх працях такі науковці, як М. Стрельбицький, В. Пилипчук, М. Шилін, А. Марущак, О. Морозов, В. Ліпкан, О. Литвиненко, І. Слюсарчук, М. Чеховська, Ю. Лапутіна, Н. Іванова, В. Панченко та інші. Водночас проблемні питання проведення СІО сектором безпеки і оборони досі лишаються висвітленими недостатньо, що підтверджує актуальність цієї статті.

Мета статті полягає в з'ясуванні проблемних питань проведення СІО сектором безпеки і оборони України, передусім, в аспекті правового регулювання.

Основна проблема проведення СІО сектором безпеки і оборони України полягає, насамперед, у слабкій нормативній урегульованості, а точніше – у відсутності належних правових засад для проведення СІО.

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, супровід 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 [2]. Втім, згадана Доктрина жодним чином не регламентує власне проведення СІО та не дає уявлення про їхню сутність. Як і Воєнна доктрина України [3], Доктрина інформаційної безпеки України опосередковано визначає СІО як елемент стратегічних комунікацій, що загалом відповідає загальносвітовому тренду – такого висновку можемо дійти, спираючись на досвід США [4−5]. 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 становлять Конституція України та закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 р. № 287, Воєнна доктрина України, затверджена Указом Президента України від 24 вересня 2015 р. № 555, Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО, підписана 22 вересня 2015 р., Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14 березня 2016 р. № 92, Стратегічний оборонний бюлетень України, уведений в дію Указом Президента України від 6 червня 2016 р. № 240, Державна програма розвитку Збройних мил України на період до 2020 р., уведена в дію Указом Президента України від 22 березня 2017 р. № 73, Доктрина інформаційної безпеки, затверджена Указом Президента України від 25 лютого 2017 р. № 47, Річна національна програма під егідою Комісії Україна − НАТО на 2017 р., затверджена Указом Президента України від 8 квітня 2017 р. № 103, Концепція стратегічних комунікацій Міністерства оборони України та Збройних сил України, затверджена Наказом Міністерства оборони України від 22 листопада 2017 р. № 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 [6], під інформаційними операціями розуміють узгоджені за метою, завданнями, місцем і часом з іншими діями військ (сил) інтегровані 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 сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом психологічних акцій (дій) та інших дій суб'єктів психологічних операцій, які проводяться за єдиним замислом і планом для здійснення впливу на емоційний стан, мотивацію, раціональне мислення визначених цільових аудиторій та зміни моделей їхньої поведінки у спосіб, що сприятиме досягненню політичних і військових цілей України. 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 складників сил оборони для виконання завдань [7]. Це визначення цілком може застосовуватись щодо СІО.

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

Окреслюючи правові межі для проведення стратегічних комунікацій, п. 2.7 Концепції стратегічних комунікацій Міністерства оборони України та Збройних сил України [6] визначає, що у процесі 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 складники стратегічних комунікацій не проводяться стосовно громадян України (крім тих, які є членами терористичних угруповань та незаконних збройних формувань). Також вони не проводяться на території України поза межами території, на якій введено правовий режим воєнного стану, поза межами району проведення антитерористичної операції або інших місць (районів) підготовки та застосування Збройних сил.

У листопаді 2017 р. до Верховної Ради України було внесено проект Закону України «Про внесення змін до Закону України «Про оборону України» щодо деяких питань підготовки держави до оборони» (реєстр. № 7272). Його головна ідея – розширення правового поля держави щодо застосування Сил спеціальних операцій ЗС України. Передбачається створення правових підстав для ведення спеціальної розвідки та військових інформаційно-психологічних операцій не тільки в умовах дії правового режиму воєнного стану, але і в мирний час в інтересах підготовки держави до оборони, тобто йдеться про проведення СІО «захисного» характеру, метою яких є забезпечення безпеки [8], а відповідно, така законодавча новація є безумовно виправданою в умовах гібридної війни. Варто також зауважити, що відсутність таких змін до чинного законодавства ускладнює можливість проведення СІО не лише Збройними силами України та іншими військовими формуваннями, але й іншими складниками сил оборони для виконання завдань, що на них покладаються. Крім того, залишається фактично позбавленим належного правового підґрунтя проведення СІО силами безпеки відповідно до їх компетенції, в тому числі з метою протидії деструктивним СІО.

Для впровадження у практику регламентації, планування та проведення СІО в Україні можуть бути рекомендовані, зокрема, такі стандарти НАТО: AC / 322 CP / 1 Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) [9]; Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability (STANAG 4586) [10]; AJP-3.4.4 Allied Joint Doctrine for Counterinsurgency (COIN) [11]; AJP-3.9 Allied Joint Doctrine for Joint Targeting [12]; AJP-3.10 Allied Joint Doctrine for Information Operations [13]; AJP-5 Allied Joint Doctrine for Operational-Level Planning [14] тощо.

Аналіз зазначених документів дає змогу дійти висновку, що проведення СІО за стандартами НАТО передбачає врахування особливостей інформаційного середовища, в якому «люди і автоматизовані системи спостерігають, орієнтують, вирішують та реагують на інформацію, отже, 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 мати 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 варто 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 такі:

– застосування «ефект-орієнтованого» підходу, який передбачає комбінацію летальних і нелетальних засобів з акцентуванням на причинах та наслідках в інформаційній сфері;

– особиста участь командування СІО в її проведенні з метою забезпечення контролю за усією 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 подальшу 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 у процесі 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.

У процесі формування 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 із проведення психологічних операцій, представник сил спеціальних операцій, офіцер зв'язку, фахівець із радіоелектронної боротьби, фахівець із комп'ютерних мережевих операцій, «фахівець з обману», фахівець із планування, синхронізації дій та оцінювання ефектів, фахівець із безпеки операцій.

У процесі 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 загалом має передбачати деталі стратегічного і політичного наміру, наявні обмеження, очікувані ефекти інформаційних дій тощо. Все це підлягає узагальненню у вигляді інформаційної матриці 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 в сукупності з необхідністю забезпечувати безпеку СІО робить доцільним застосування до планування й проведення СІО методології управління ризиками.

Воєнна доктрина України і Доктрина інформаційної безпеки України опосередковано визначають СІО як елемент стратегічних комунікацій, що загалом відповідає загальносвітовому тренду. При цьому правові межі для проведення стратегічних комунікацій визначені п. 2.7 Концепції стратегічних комунікацій Міністерства оборони України та Збройних сил України, де, зокрема, визначено, що СІО не проводяться стосовно 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, поза межами району проведення антитерористичної операції або інших місць (районів) підготовки та застосування Збройних сил. Варто також зауважити, що відсутність правової регламентації проведення СІО в мирний час ускладнює можливість їх проведення не лише Збройними силами України та іншими військовими формуваннями, але й іншими складовими сектору безпеки і оборони. Отже, необхідним є подальший розвиток правового підґрунтя проведення СІО сектором безпеки і оборони України, а також впровадження у практику регламентації, планування та проведення СІО в Україні стандартів НАТО.

ЛІТЕРАТУРА

1. 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)

2. Доктрина інформаційної безпеки України, затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення 28.11.2018)

3. Указ Президента України № 555/2015 «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 р. «Про нову редакцію Воєнної доктрини України». URL: http://www.president.gov.ua/documents/5552015-19443 (дата звернення 30.11.2018).

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

5. 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).

6. Концепція стратегічних комунікацій Міністерства оборони України та Збройних сил України, затверджена Наказом Міністерства оборони України від 22 листопада 2017 р. № 612. URL: https://zakon.rada.gov.ua/rada/show/v0612322-17 (дата звернення 08.02.2019).

7. Про оборону України : Закон України від 6 грудня 1991 р. URL: https://zakon.rada.gov.ua/laws/ show/ 1932-12 (дата звернення 08.02.2019).

8. Т.Попова. Правове поле для спецназу. URL: https://www.radiosvoboda.org/a/28373318.html (дата звернення 12.02.2019).

9. CONSULTATION, COMMAND AND CONTROL BOARD (C3B), 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 05.03.2019).

10. 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 (дата звернення 03.03.2019).

11. 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 05.03.2019).

12. 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 05.03.2019).

13. 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 04.03.2019).

14. 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 05.03.2019).