УДК 316.485.26:316.776 DOI: 10.30748/nitps.2019.37.02

В.Ю. Богданович[1], О.В. Дублян[1], О.В. Передрій[1], П. Пацек[2]
[1] *Центральний науково-дослідний інститут Збройних Сил України, Київ, Україна*
[2] *Академія військового мистецтва, Варшава, Польща*

СТРУКТУРНО-ЛОГІЧНА ПОСЛІДОВНІСТЬ ТА ПРИНЦИПИ ОРГАНІЗАЦІЇ ПРОТИДІЇ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ З БОКУ НЕДРУЖНЬОЇ ДЕРЖАВИ

Розглядається системно-логічна послідовність організації асиметричної протидії інформаційно-психологічним впливам з боку недружніх держав, яка посилює можливості політичного керівництва держави щодо функціонування в умовах гібридних загроз, зокрема при здійсненні проти нього інформаційно-психологічних впливів в зовнішньополітичній та внутрішньополітичній сферах. Основними засобами ведення інформаційного протиборства є національні й транснаціональні засоби масової інформації, а також будь-які інші інформаційні мережі, здатні впливати як на світогляд, політичні погляди, правосвідомість, менталітет, духовні ідеали й ціннісні установки окремої людини, так і на суспільство і його політичну еліту в цілому. Зазначені обставини на перший план висувають проблему нарощування можливостей держави щодо реалізації національних інтересів в умовах сучасного інформаційного протиборства. Показано, що найбільш вразливою формою інформаційного протиборства для держави-мішені виступають спеціальні інформаційні операції (СІО), що проводяться проти суб'єктів, які приймають стратегічні рішення. Ефективне функціонування держави-мішені в умовах нав'язуваного інформаційного протиборства можливе на основі побудови структурно-логічної послідовності організації асиметричної протидії інформаційно-психологічним впливам з боку недружніх держав на основі запропонованих принципів.

Ключові слова: *інформаційне протиборство, інформаційно-психологічний вплив, спеціальна інформаційна операція, асиметрична протидія, держава-мішень, послідовність організації протидії.*

Вступ

Постановка проблеми у загальному вигляді. На початку XXI-го століття різко посилилася залежність політичного керівництва держав від можливостей протистояти інформаційно-психологічним впливам в зовнішньополітичній та внутрішньополітичній сферах. Трансформація світового порядку, геополітична конкуренція провідних держав в боротьбі за контроль над енергоресурсами та шляхами їх транспортування, розвиток процесу глобалізації свідчать про те, що поряд із традиційними силовими методами й засобами рішення завдань у цих сферах усе більше використовуються інформаційні.

Основними засобами ведення інформаційного протиборства є національні й транснаціональні засоби масової інформації, а також будь-які інші інформаційні мережі, здатні впливати як на світогляд, політичні погляди, правосвідомість, менталітет, духовні ідеали й ціннісні установки окремої людини, так і на суспільство в цілому. Зазначені обставини на перший план висувають проблему нарощування можливостей держави і її політичного керівництва здійснювати інформаційне протиборство при реалізації національних інтересів в таких умовах. Однією із дієвих форм сучасного інформаційного протиборства виступають спеціальні інформаційні операції (СІО), що проводяться проти суб'єктів, що приймають стратегічні рішення. Ефективна протидія СІО в процесі нав'язуваного інформаційного протиборства можлива на основі побудови структурно-логічної послідовності організації протидії інформаційно-психологічним впливам з боку недружніх держав на основі нових принципів, що і визначає **мету** даної публікації.

Аналіз останніх досліджень, публікацій. Спеціальні інформаційні операції, які проводяться проти суб'єктів, що приймають стратегічні рішення, та іміджу держави, частково описані в [1–2; 7–8], але представлений опис має лише вербальний характер і не дозволяє дослідити ці операції з використанням сучасного методичного апарату та моделювання.

У монографії [3] представлена методологія комплексного використання військових і невійськових сил і засобів сектора безпеки і оборони для протидії сучасним загрозам воєнного та гібридного характеру для забезпечення воєнної безпеки України. Але протидія інформаційно-психологічним впливам (загрозам) розглянута лише у загальному вигляді.

З огляду на це, м**етою статті є** формування структурно-логічної послідовності та розробка нових принципів організації протидії інформаційно-психологічним впливам з боку недружніх держав.

Виклад основного матеріалу

Технічний прогрес призвів до удосконалення засобів комунікації, завдяки чому сучасний світ став більш взаємозв'язаним. Процеси глобалізації активно впливають на формування моделі світоустрою, яку психіка і свідомість людини повинні усвідомити сьогодні. Багатогранність інформаційної сфери робить інформаційно-психологічні засоби дії не лише малопомітними, гуманними, але у ряді випадків і надзвичайно небезпечними.

Інформаційно-психологічні впливи, незважаючи на уявну невинність і безпечність, довели свою високу результативність в досягненні перемоги однієї протиборчої сторони над іншою. Тому духовний, інтелектуальний і інформаційний потенціали перетворилися на фундаментальні чинники національної безпеки [2–3].

Увесь хід розвитку світової історії підтверджує, що країни, які мають високий рівень розвитку інформаційних технологій, мають значну перевагу над іншими країнами. Мета будь-якої війни і політики уряду будь-якої країни – змусити супротивника, конкурента, партнера прийняти вигідне для своєї країни рішення. Суспільна думка сама по собі перетворилася на щонайпотужніший інструмент досягнення цієї мети. Здійснюючи вплив за допомогою тієї або іншої інформації, що доводиться по засобах комунікації, на світогляд, свідомість, психіку людей, вдається досягати того, що уряди країн, які піддалися інформаційній дії, приймають “нав'язані”, невигідні для свого народу і своєї країни рішення [3].

Завдяки насиченості світу новітніми засобами відтворення, передачі і отримання інформації, значно спростилися процеси інформаційно-психологічної дії на людей. Мозок людини, її психіка, свідомість піддаються змінам, і самі, у свою чергу, здатні змінювати існуючу об'єктивну реальність за допомогою діяльності людей [2]. У цьому і велике благо для людини і велика небезпека стати жертвою чиєїсь маніпуляції. Сучасні технології інформаційної дії дозволяють дезорієнтувати людину в подіях, що відбуваються, управляти її поведінкою і вчинками непомітно для неї самої. Причому сьогодні така дія можлива не лише на рівні свідомості, але і на підсвідомому рівні. Інформаційно-психологічна дія дозволяє управляти не лише окремими особами, але і великими соціальними групами, державними інститутами і цілими державами. Управління великими групами людей за допомогою формування необхідного маніпулятора громадської думки через формування того або іншого відношення до події (коментар) через засоби масової інформації (ЗМІ) та соціальні мережі виявилося досить ефективним [9].

Рішення, що приймаються по отриманій не вчасно, неповній або спотвореній інформації, завжди супроводжуються втратами економічного, політичного, військового і іншого характеру. З прадавніх часів існування і виживання людини залежали від того, наскільки повно і своєчасно вона отримувала інформацію про загрози і небезпеки і того, наскільки вчасно і адекватно реагувала на них [2; 4].

Аналіз сучасного інформаційно-психологічного протиборства [2–3, 10] свідчить, що найбільш вразливими його формами для держави-мішені є: інформаційна атака; інформаційна агресія; інформаційна операція; спеціальна інформаційна операція.

Протидія інформаційно-психологічним впливам з боку недружніх держав представляє собою комплекс заходів суб’єктів сектору безпеки і оборони України, що опікуються забезпеченням інформаційно-психологічної безпеки, щодо нейтралізації виявленого деструктивного впливу або його деескалації до допустимого рівня.

Найбільший ефект організованої протидії досягається у разі створення окремої системи протидії під єдиним керівництвом.

Основними завданнями системи протидії доцільно визначити:

максимально знизити очікувані деструктивні рівні реалізації інформаційно-психологічних впливів (ІПСВ) у визначальних сферах національної безпеки (нейтралізувати ІПСВ з найменшими втратами для держави);

максимально зберегти імідж держави на міжнародній арені;

максимально зберегти імідж воєнно-політичного керівництва держави (всередині держави і за рубежем) в умовах здійснення цілеспрямованих ІПСВ;

не допустити порушення соціально-політичної стабільності всередині держави;

зберегти стратегічних партнерів та союзників, не допустити нанесення шкоди їхньому іміджу;

мінімізувати ресурси, що залучаються для нейтралізації деструктивних ІПСВ;

дискредитувати державу-джерело (агресора) деструктивного ІПСВ в очах міжнародної спільноти;

не допустити повторення аналогічного сценарію здійснення деструктивного ІПСВ на державу.

Логічна послідовність організації протидії інформаційно-психологічним впливам з боку інших держав може бути представлена у вигляді послідовно виконуваних обчислювальних, логічних, порівняльних та інших процедур (рис. 1):

1. *Моніторинг каналів, по яким здійснюються ІПСВ*. До програми моніторингу вносяться ознаки інформаційних і психологічних впливів, відомі на сьогодні.

2. *Виявлення, реєстрація і рейтингування каналів впливу*. Практика свідчить, що для здійснення ІПСВ можуть бути задіяні до декількох сотень інформаційних каналів. Виявлення ІПСВ здійснюється,

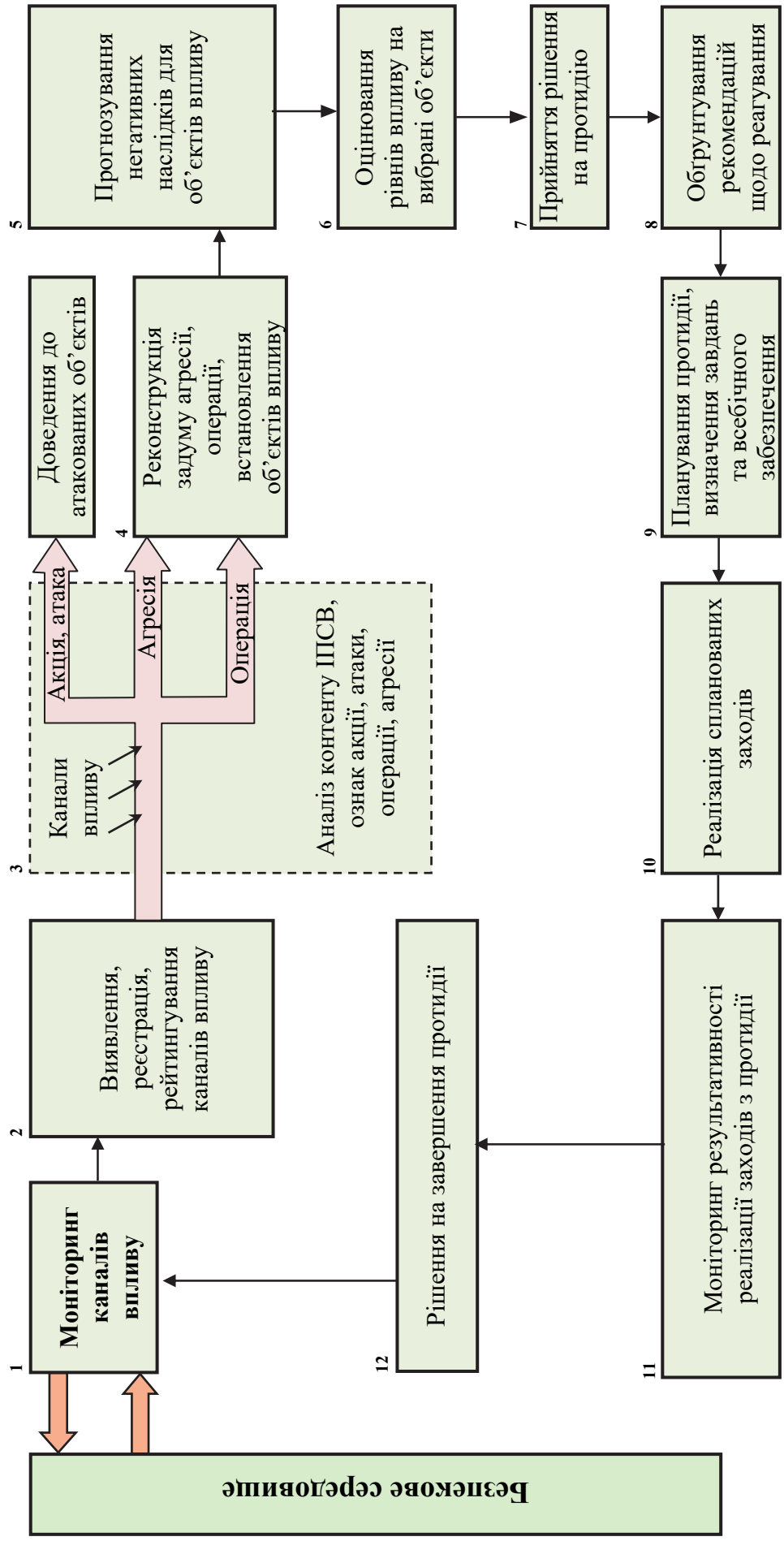

Рис. 1. Системно-логічна послідовність організації протидії інформаційно-психологічним впливам з боку недружніх держав

як правило, в автоматичному або в ручному режимах. Рішення про факт ІПСВ приймається підготовленими експертами з інформаційно-психологічної сфери. Далі цей факт реєструється встановленим порядком (наприклад, записується у спеціальний журнал або в паспорт), при можливості, встановлюється приналежність відправлення та місцезнаходження джерела. Виявленим каналам, по яким був здійснений ІПСВ, експертами визначаються пріоритети для подальшого розгляду.

3. *Аналіз контенту ІПСВ, ознак акції, атаки, операції або агресії.*

Експертами – фахівцями у сфері інформаційного протиборства аналізується контент зафіксованих ІПСВ, встановлюється, на кого спрямовується цей вплив. По контенту впливу та його ознакам експерти з використанням методу Ісікави [3] попередньо визначають "потужність" впливу, чи це акція, атака, чи може бути складовою операції або агресії, у тому числі гібридної. У разі, якщо вставлено факт інформаційно-психологічної акції або атаки проти конкретного об'єкта, то про це повідомляється об'єкт для організації самооборони (протидії). Якщо експерти встановили можливість інформаційної агресії або ознаки операції, то переходять до наступного етапу.

4. *Реконструкція задуму операції, агресії та встановлення об'єктів впливу.* По результатам вивчення контенту, встановлених об'єктів впливу та ознак "потужності" впливу експерти методом генерації ідей або методом мозкового штурму визначають задум гібридної агресії (операції), її ймовірну мету та об'єкти впливу, прогнозують головний напрям (основний об'єкт) агресії (операції).

5. *Прогнозування негативних наслідків для об'єктів впливу.* По отриманим відомостям про розпочату агресію чи операцію методом експертного опитування проводиться прогнозування можливих деструктивних наслідків для кожного із визначених об'єктів та національної безпеки у цілому. Зокрема, прогнозується можливе зниження іміджу держави на міжнародній арені та іміджу воєнно-політичного керівництва держави всередині країни і за рубежем. За окремою методикою [5] прогнозується зниження рівня соціально-політичної стабільності всередині держави. Окремим пунктом експерти прогнозують масштаб нанесення шкоди іміджу стратегічних партнерів та союзників, прогнозують можливий рівень допомоги з їх боку.

6. *Прогнозування рівнів впливу на вибрані об'єкти.* Експерти прогнозують очікувані рівні впливу K_{ipvj} на кожен *j*-й (j=1,J, де J – кількість об'єктів впливу) вибраний об'єкт за шкалою Сааті [6] (табл. 1).

Таблиця 1

Рівні градації шкали Сааті

Рівень впливу	Дуже низький	Низький	Середній	Високий	Дуже високий
Відлік за шкалою	1	3	5	7	9

Джерело: [6, стор. 37].

Для кожного j-го об'єкта попередньо методом експертного опитування визначається поріг забезпечення інформаційно-психологічної безпеки k_{porj}. Ті об'єкти, для яких прогнозний очікуваний рівень впливу перевищує поріг забезпечення інформаційно-психологічної безпеки, виділяються в окремий перелік. Методом експертного опитування оцінюються їх пріоритети у залежності від їх впливу на зниження іміджу держави на міжнародній арені та іміджу воєнно-політичного керівництва держави всередині країни і за рубежем. По кожному із цих об'єктів оцінюється потрібний рівень деескалації ІПСВ:

$$\Delta_{dj} = K_{ipvj} - k_{porj} .$$

7. *Прийняття рішення на протидію*. Особа, що приймає рішення (ОПР), оцінює потрібні ресурси R_{potrj} для деескалації ІПСВ на ту групу об'єктів, очікуваний (прогнозний) вплив на які перевищив їх пороги забезпечення інформаційно-психологічної безпеки. Якщо ресурсів достатньо, то ОПР приймає рішення на протидію, яка може бути або симетричною, або асиметричною. Якщо ресурсів недостатньо, то ОПР приймає рішення на деескалацію ІПСВ на один або декілька об'єктів, які мають найбільший рейтинг. У такому випадку протидія, як правило, організується як асиметрична.

8. *Обґрунтування рекомендацій щодо реагування*. Симетричне реагування, яке здійснюється за умови достатності ресурсів і високої захищеності об'єктів впливу, описане у літературі по інформаційно-психологічному протиборству. Асиметричне реагування у літературі висвітлено лише у постановочному плані. Тому є потреба у більш детальному його розгляді. Звісно, що конкретні заходи щодо асиметричного реагування, у більшості випадків, носять закритий характер. Ми зупинимось лише на основних принципах та загальних критеріях прийняття рішення на асиметричне реагування на найбільш небезпечні ІПСВ.

Перший принцип обґрунтування рекомендацій – це *достатність сформованого потенціалу асиметричної протидії*, під яким розуміється інтегрована сукупність різнорідних (військових і невійськових) сил та засобів, що залучаються під єдиним

управлінням для деескалації ІПСВ на об'єкт, що вибраний для захисту.

Другий принцип – комплексна вразливість держави – ініціатора ІПСВ, що означає розробку таких заходів з протидії, які б одночасно деструктивно впливали на політичну сферу та політичне керівництво недружньої держави, її економіку, формували у міжнародної спільноти її негативний імідж, агресивність її зовнішньої політики, образ порушника міжнародного права тощо.

Третій принцип – нарощування "потужності" протидії за рахунок використання коаліційної протидії недружній державі. Це означає, що для нарощування "потужності" протидії у найкоротший термін держава-мішень має звернутися до своїх союзників та стратегічних партнерів за їх підтримкою щодо протидії ІПСВ недружньої держави.

Четвертий принцип – швидкоплинність реалізації асиметричних заходів. Асиметричні заходи мають здійснюватися в короткі терміни з тим, щоб супротивна сторона не встигала оговтатися, здійснити передислокацію сил та засобів, адаптуватися до дій держави-мішені.

П'ятий принцип – максимізація шкоди недружній державі у різних сферах життєдіяльності до такого рівня, щоб вона припинила ІПСВ.

Шостий принцип –гіпертрофія завданих збитків недружній державі (тиражування в ЗМІ морального розладу, алкоголізму, наркоманії, безчинств по відношенню до окремих верств свого населення, росту злочинності тощо)

Сьомий принцип – скритність і мінімізація ознак державної приналежності (легендування) з тим, щоб державі-мішені можна було витоки інформації про проведення спеціальної операції називати "фейками" або провокаціями держави, що здійснює ІПСВ або її партнерів.

Критеріями прийняття рішення на асиметричне реагування доцільно вибрати:

1. Критерій досягнення потрібного рівня деескалації ІПСВ на j -й об'єкт

$$\Delta_{dj} = K_{ipvj} - k_{porj}.$$

2. Критерій *достатності виділених* ресурсів $R_{potrj} \leq R_{vydj}$.

3. Критерій потрібного часу $T_{ptdpotrj} \leq T_{ptddopj}$.

Якщо умова досягнення визначених критеріїв виконується, то приймається рішення щодо нейтралізації ІПСВ симетричним методом, якщо хоча б одна із умов не виконується, то приймається рішення на асиметричну протидію.

9. *Планування протидії, визначення завдань та всебічного забезпечення.* Планування протидії передбачає розробку детального плану (сценарію) асиметричної протидії сформованим потенціалом та системне визначення конкретних завдань кожному суб'єкту із інтегрованої сукупності різнорідних (військових і невійськових) сил та засобів, що залучаються для деескалації ІПСВ на об'єкт, що вибраний для захисту. Системне визначення завдань означає, що завдання визначається на основі наведених у п.8 принципів та з врахуванням досягнення очікуваного системного ефекту. Реалізація запланованих завдань проводиться у формі спеціальної операції, організація та проведення якої здійснюється за окремими настановами з обмеженим доступом.

10. *Моніторинг результативності заходів з протидії.* Для ефективного проведення спеціальної операції дуже важливо відстежувати її хід та проблеми, що виникають з тим, щоб забезпечити оперативність реагування на зміни обстановки. Крім того, моніторинг дозволить завчасно виявити дії супротивника по корегуванню своєї стратегії, залученню резервів та запасних варіантів ІСПВ тощо. По даним моніторингу ОПР приймає рішення на завершення протидії.

11. *Прийняття рішення на завершення протидії.* Умовами прийняття рішення на завершення протидії можуть бути:

1. Нейтралізація ІПСВ до прийнятного рівня.

2. Недружня країна відмовилася від подальшого здійснення ІПСВ на державу-мішень.

Висновки

Таким чином, ефективне функціонування держави-мішені в умовах нав'язуваного інформаційного протиборства, зокрема при проведенні проти неї СІО, можливе на основі побудови структурно-логічної послідовності організації протидії інформаційно-психологічним впливам з боку недружніх держав на основі нових принципів.

У наступних публікаціях більш детально будуть розглянуті принципи організації протидії та критерії прийняття рішення на проведення асиметричних заходів щодо нейтралізації виявлених інформаційно-психологічних впливів.

Список літератури

1. Методологія комплексного використання військових і невійськових сил і засобів сектора безпеки і оборони для протидії сучасним загрозам воєнній безпеці України: монографія / В.Ю. Богданович, І.С. Романченко, І.Ю. Свида, А.М. Сиротенко. – К.: НУОУ ім. І. Черняховського, 2019. – 268 с.

2. Операции информационно-психологической войны [Електронний ресурс] / В. Вепринцев, А. Манойло, А. Петренко, Д. Фролов. – 2005. –Режим доступу: http://psyfactor.org/psyops/psyops4.htm (дата звернення 8.02.2018).

3. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія / О.В.Литвиненко. – К.: НІСД, 2003. – 240 с.

4. Панченко В.М. Методика виявлення ознак інформаційного впливу в засобах масової інформації / В.М. Панченко, В.І. Полевий // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3(7). – С. 79-83.

5. Богданович В.Ю. Теоретико-методологічні основи забезпечення національної безпеки України: моногр.: у 7 т., Т. 1: Теоретичні основи, методи й технології забезпечення національної безпеки України / В.Ю. Богданович, І.Ю. Свида, Є.Д. Скулиш; за заг. ред. Є.Д. Скулиша. – К.: Наук.-вид.відділ НА СБ України, 2012. – 548 с.

6. Саати Томас Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. / Науч. ред. А.В. Андрейчиков, О.Н. Андрейчикова. – М.: Издательство ЛКИ, 2008. – 360 с.

7. Методичний підхід до вибору оптимального сценарію проведення інформаційно-психологічної операції / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, К.І. Хударковський // Системи обробки інформації. – 2016. – № 9(146). – С. 149-152.

8. Методичний підхід до формування сценарію проведення інформаційно-психологічного впливу на осіб, що приймають рішення / Г.В. Пєвцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський // Системи обробки інформації. – 2019. – № 1(156). – С. 74-81. https://doi.org/10.30748/soi.2019.156.10.

9. Дубницкий В.Ю. Интервальное оценивание количества участников массовых протестных акций / В.Ю. Дубницкий, Г.Г. Зубрицкая, А.М. Кобылин // Сучасні інформаційні системи. – 2018. – Т. 2, № 4. – С. 11-20. https://doi.org/10.20998/2522-9052.2018.4.02.

10. Алімпієв А.М. Особливості гібридної війни РФ проти України. Досвід, що отриманий Повітряними Силами Збройних Сил України / А.М. Алімпієв, Г.В. Пєвцов // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. – № 2(27). – С. 19-25. https://doi.org/10.30748/nitps.2017.27.03.

References

1. Bogdanovich, V.Yu., Romanchenko, I.S., Svyda, I.Yu. and Syrotenko, A.M. (2019), "*Metodolohiya kompleksnoho vykorystannya viys'kovykh i neviys'kovykh syl i zasobiv sektora bezpeky i oborony dlya protydiyi suchasnym zahrozam voyenniy bezpetsi Ukrayiny*" [*Methodology of integrated use of military and non-military forces and means of the security and defense sector for counteracting modern threats to Ukraine's military security*], NUOU after Ivan Chernyakhovsky, Kyiv, 268 p.

2. Veprintsev, V., Manoilo, A., Petrenko, A. and Frolov, D. (2005), "*Operacyy ynformacyonno-psykhologhycheskoj vojny*" [*Operations of information and psychological war*], available at: www.psyfactor.org/psyops/psyops4.htm (accessed 8 February 2018).

3. Lytvynenko, O.V. (2003), "*Informacijni vplyvy ta operaciji. Teoretyko-analitychni narysy: monoghrafija*" [*Information influences and operations. Theoretical and analytical essays: a monograph*], NUSR, Kyiv, 240 p.

4. Panchenko, V.M. and Polevyi, V.I. (2011), "Metodyka vyjavlennja oznak informacijnogho vplyvu v zasobakh masovoji informaciji" [Methods of detecting signs of information influence on the mass media], *Information security of man, society, state*, No. 3(7), pp. 79-83.

5. Bohdanovych, V.Yu., Svyda, I.Y. and Skulysh, Y.D. (2012), "*Teoretyko-metodolohichni osnovy zabezpechennyanatsional'noyi bezpeky Ukrayiny: monographiia T. 1. Teoretychni osnovy, metody y tekhnolohiyi zabezpechennya natsional'noyi bezpeky Ukrayiny*" [*Theoretical and methodological bases for ensuring national security of Ukraine in 7 vol. Vol. 1. Theoretical Foundations, Methods and Technologies for the National Security of Ukraine*], Naukovo vydavhichiy viddil NA SB Ukrayiny, Kyiv, 548 p.

6. Saati, Thomas L. (2008), "*Prynjatye reshenyj pry zavysymostjakh y obratnykh svjazjakh: Analytycheskye sety*" [*Decision making in dependencies and feedbacks: Analytical networks*], Publishing house LKI, Moscow, 360 p.

7. Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O. and Khudarkovskyi, K.I. (2016), "Metodychnyi pidkhid do vyboru optymalnoho stsenariiu provedennia informatsiino-psykholohichnoi operatsii" [Methodical approach to the choice of optimum scenario of information and psychological operation], *Information Processing Systems*, No. 9(146), pp. 149-152.

8. Pievtsov, H.V., Zalkin, S.V., Sidchenko, S.O. and Khudarkovskyi, K.I. (2019), "Metodychnyi pidkhid do formuvannia stsenariiu provedennia informatsiino-psykholohichnoho vplyvu na osib, shcho pryimaiut rishennia" [Methodological approach to formation of the scenario realization information and psychological influence on the person who make a decision], *Information Processing Systems*, No. 1(156), pp. 74-81. https://doi.org/10.30748/soi.2019.156.10.

9. Dubnitskiy, V., Zubrytska, H. and Kobylin, A. (2018), "Yntervaljnoe ocenyvanye kolychestva uchastnykov massovykh protestnykh akcyj" [Interval estimation of the number of participants of mass protest actions], *Advanced Information Systems*, No. 2(4), pp. 11-20. https://doi.org/10.20998/2522-9052.2018.4.02.

10. Alimpiiev, A.M. and Pievtsov, H.V. (2017), "Osoblyvosti hibrydnoi viiny RF proty Ukrainy. Dosvid, shcho otrymanyi Povitrianymy Sylamy Zbroinykh Syl Ukrainy" [The features of the hybrid war of the Russian Federation against Ukraine. Experience received by the Armed Forces of the Armed Forces of Ukraine], *Science and Technology of the Air Force of Ukraine*, No. 2(27), pp. 19-25. https://doi.org/10.30748/nitps.2017.27.03.

Надійшла до редколегії 16.10.2019
Схвалена до друку 19.11.2019

Відомості про авторів:

Богданович Володимир Юрійович
доктор технічних наук професор
головний науковий співробітник Центрального науково-дослідного інституту Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-0481-9454

Information about the authors:

Volodymyr Bohdanovych
Doctor of Technical Sciences Professor
Chief Research of Central Research Institute of the Armed Forces of Ukraine,
Kyiv, Ukraine
https://orcid.org/0000-0003-0481-9454

Дублян Олександр Володимирович
кандидат військових наук
провідний науковий співробітник
Центрального науково-дослідного інституту
Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0001-5129-3913

Передрій Олександр Вікторович
кандидат військових наук
Начальник управління Центрального
науково-дослідного інституту Збройних Сил України,
Київ, Україна
https://orcid.org/0000-0003-2877-4959

Пацек Петро
доктор філософії викладач
Академії військового мистецтва,
Варшава, Польща
https://orcid.org/0000-0002-2182-2316

Oleksandr Dublayn
Candidate of Military Sciences
Lead Research
of Central Research Institute
of the Armed Forces of Ukraine,
Kyiv, Ukraine
https://orcid.org/0000-0001-5129-3913

Oleksandr Peredrii
Candidate of Military Sciences
Head of Research Department of Central
Research Institute of the Armed Forces of Ukraine,
Kyiv, Ukraine
https://orcid.org/0000-0003-2877-4959

Piotr Pacek
Doctor of Philosophy
Lecturer of the War Studies University,
Warsaw, Poland
https://orcid.org/0000-0002-2182-2316

СТРУКТУРНО-ЛОГИЧЕСКАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ И ПРИНЦИПЫ ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИМ ВОЗДЕЙСТВИЯМ СО СТОРОНЫ НЕДРУЖЕСТВЕННОГО ГОСУДАРСТВА

В.Ю. Богданович, А.В. Дублян, А.В. Передерий, П. Пацек

Рассматривается системно-логическая последовательность организации асимметричного противодействия информационно-психологическим воздействиям со стороны недружественных государств, усиливающая возможности политического руководства государства относительно функционирования в условиях гибридных угроз, в том числе при осуществлении против него информационно-психологических воздействий во внешнеполитической и внутриполитической сферах. Основными средствами ведения информационного противоборства являются национальные и транснациональные средства массовой информации, а также любые другие информационные сети, способные влиять как на мировоззрение, политические взгляды, правосознание, менталитет, духовные идеалы и ценностные установки отдельного человека, так и на общество и его политическую элиту в целом. Указанные обстоятельства на первый план выдвигают проблему наращивания возможностей государства по реализации национальных интересов в условиях современного информационного противоборства. Показано, что наиболее уязвимой формой информационного противоборства для государства-мишени выступают специальные информационные операции (СИО), проводимые против субъектов, принимающих стратегические решения. Эффективное функционирование государства-мишени в условиях навязываемого информационного противоборства возможно на основе построения структурно-логической последовательности организации асимметричного противодействия информационно-психологическим воздействиям со стороны недружественных государств на основе предложенных принципов.

Ключевые слова: *информационное противоборство, информационно-психологическое воздействие, специальная информационная операция, асимметричная противодействие, государство-мишень, последовательность организации противодействия.*

STRUCTURAL-LOGICAL SEQUENCE AND PRINCIPLES OF ORGANIZATION OF COUNTERACTION TO INFORMATION-PSYCHOLOGICAL INFLUENCES BY UNFRIENDLY STATE

V. Bogdanovych, O. Dublian, O. Peredrii, P. Pacek

Currently, there is a rapid formation of a new information space based on modern technologies and communications. This information space already has a significant impact on many aspects of the functioning of any state and ensures the achievement of goals in short periods of time in a significant space.

It is considered the systemic and logical sequence of organization of asymmetric counteraction to information and psychological influences by unfriendly states, which enhances the possibilities of political leadership of the state to function in the conditions of hybrid threats, in particular, when it exerts informational and psychological influences in foreign policy and internal politics. The main means of information confrontation are national and transnational media, as well as any other information networks that can influence on both the worldview, political views, justice, mentality, spiritual ideals and values of the individual, as well as society and its political elite as at whole. These circumstances bring to the fore the problem of increasing the capacity of the state to realize national interests in today's information confrontation. It is shown that the most vulnerable form of information warfare for the target state is the Special Information Operations (SIOs) conducted against strategic decision makers. The effective functioning of the target state in the conditions of imposed information confrontation is possible on the basis of constructing of a structural and logical sequence of organization of asymmetric counteraction to information and psychological influences by unfriendly states on the basis of the proposed principles.

Keywords: *information counteraction, information and psychological influences, special information operation, asymmetric counteraction, target state, sequence of counteraction organization.*