Розвиток та застосування Повітряних Сил, інших видів Збройних Сил України, удосконалення їх системи управління

УДК 327.5

DOI: 10.30748/nitps.2020.41.01

В.Ю. Богданович¹, А.М.Сиротенко², О.В. Дублян¹

¹ *Центральний науково-дослідний інститут Збройних Сил України, Київ*

² *Національний університет оборони України ім. І. Черняхівського, Київ*

КОНЦЕПЦІЯ АСИМЕТРИЧНОЇ ПРОТИДІЇ ВОРОЖІЙ ДЕРЖАВІ ДЛЯ НЕЙТРАЛІЗАЦІЇ ЇЇ ВПЛИВУ НА ВИЗНАЧАЛЬНІ СФЕРИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ (закінчення)

початок у № 3(40), 2020 С. 13-24

5. Структурно-логічна послідовність та принципи організації протидії інформаційно-психологічним впливам з боку недружньої держави

На початку XXI-го століття різко посилилася залежність політичного керівництва держав від можливостей протистояти інформаційно-психологічним впливам (ІПВ) 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 все більше використовуються інформаційні [1].

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 (CIO), що проводяться проти суб'єктів, що приймають стратегічні рішення. Ефективна протидія CIO в процесі нав'язуваного інформаційного протиборства можлива на основі побудови структурно-логічної послідовності та розробки нових принципів організації протидії інформаційно-психологічним впливам з боку недружніх держав.

Спеціальні інформаційні операції, які проводяться проти суб'єктів, що приймають стратегічні рішення, та іміджу держави частково описані в [2–3], але представлений опис має лише вербальний харак-

тер і не дозволяє дослідити ці операції з використанням сучасного методичного апарату та моделювання.

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 [3–4].

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 [4].

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 діяль-

ності людей [3]. 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 виявилось досить ефективним.

Рішення, що приймаються по отриманій не вчасно, неповній або спотвореній інформації, завжди супроводжуються втратами економічного, політичного, військового і іншого характеру [3; 5].

Аналіз сучасного інформаційно-психологічного протиборства [3–4] свідчить, що найбільш вразливими його формами для держави-мішені є: інформаційна атака; інформаційна агресія; інформаційна операція; спеціальна інформаційна операція.

Протидія ІПВ з боку недружніх держав представляє собою комплекс заходів суб'єктів СБОУ, 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 ІПВ у визначальних сферах національної безпеки;

- максимально зберегти імідж держави на міжнародній арені;

- максимально зберегти імідж військово-політичного керівництва держави (всередині держави і за рубежом) в умовах здійснення цілеспрямованих ІПВ;

- 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 ІПВ;

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

- не допустити повторення аналогічного сценарію здійснення деструктивного ІПВ на державу.

Логічна послідовність організації протидії інформаційно-психологічним впливам з боку інших держав може бути представлена у вигляді послідов-

но виконуваних обчислювальних, логічних, порівняльних та інших процедур (рис. 1):

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

2. Виявлення, реєстрація і рейтингування каналів впливу. Практика свідчить, що для здійснення ІПВ можуть бути задіяні до декількох сотень інформаційних каналів. Виявлення ІПВ здійснюється, як правило, в автоматичному або в ручному режимах. Рішення про факт ІПВ 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. Виявленням каналів, по яким був здійснений ІПВ, експертами визначаються пріоритети для подальшого розгляду.

3. Аналіз контенту ІПВ, ознак акції, атаки, операції або агресії. Експертами-фахівцями у сфері інформаційного протиборства аналізується контент зафіксованих ІПВ, встановлюється, на кого спрямовується цей вплив. По контенту впливу та його ознакам експерти з використанням методу Ісікави [6] 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 [7], 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 військово-політичного керівництва держави всередині країни і за рубежом. За окремою методикою [8] 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.

Рис. 1. Структурно-логічна послідовність організації протидії інформаційно-психологічним впливам з боку недружніх держав
Джерело: розроблено авторами.

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 [9], 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 [8, С. 113].

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 рубежом. По кожному із цих об'єктів оцінюється потрібний рівень деескалації ППВ:

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

7. Прийняття рішення на протидію. Особа, що приймає рішення (ОПР), оцінює потрібні ресурси R_{potrj} для деескалації ППВ на ту групу об'єктів, очікуваний (прогнозний) вплив на які перевищив їх порогого 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 ППВ 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 протидію. 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 ППВ.

Перший принцип обґрунтування рекомендацій – це достатність сформованого потенціалу асиметричної протидії, під яким розуміється інтегрована сукупність різномірних (військових і невійськових)

сил та засобів, що залучаються під єдиним управлінням для деескалації ППВ на об'єкт, що вибраний для захисту.

Другий принцип – комплексна вразливість держави – ініціатора ППВ, що означає розробку таких заходів з протидії, які б одночасно деструктивно впливали на політичну сферу та політичне керівництво недружньої держави, її економіку, формували у міжнародній спільноті 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 ППВ 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 ППВ.

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 витокати інформації про проведення спеціальної операції називати “фейками” або провокаціями держави, що здійснює ППВ, або її партнерів.

Критеріями прийняття рішення на асиметричне реагування доцільно вибрати:

критерій досягнення потрібного рівня деескалації ППВ на j -й об'єкт;

критерій достатності виділених ресурсів;

критерій потрібного часу для деескалації ППВ.

Якщо умова досягнення визначених критеріїв виконується, то приймається рішення щодо нейтралізації ІПВ 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 ІПВ на об'єкт, що вибраний для захисту. Системне визначення завдань означає, що завдання визначається на основі наведених принципів та з врахуванням досягнення очікуваного системного ефекту.

10. Реалізація спланованих заходів проводиться у формі спеціальної операції, організація та проведення якої здійснюється за окремими настановами з обмеженим доступом.

11. 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 ІПВ тощо. По даним моніторингу приймається рішення на завершення протидії.

12. Прийняття рішення на завершення протидії. Умовами прийняття рішення на завершення протидії можуть бути:

нейтралізація ІПВ до прийнятного рівня;

недружня країна відмовилася від подальшого здійснення ІПВ на державу-мішень.

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

6. Концептуальний підхід до формування змісту локальної спеціальної операції асиметричної протидії та визначення часткових завдань суб'єктам, що залучаються до неї

В умовах, коли однією із конфліктуючих сторін виступає значно сильніша у воєнному відношенні держава, друга сторона, щоб відстояти свою незалежність та зберегти територіальну цілісність, вимушена вдаватися до асиметричних дій. На превеликий жаль, на даний час теоретичні основи ведення асиметричних війн не розроблені, а досвід ведення таких війн у світі узагальнено досить поверхнево.

Тому існує нагальна потреба у розробці теоретичних основ і практичних рекомендації щодо впровадження у практику забезпечення воєнної безпеки технологій підготовки та ведення асиметричної війни. Вирішення цього завдання доцільно розпочати з розробки концептуального підходу до формування замислу локальної спеціальної операції асиметричної протидії (ЛСОАП).

Основою підготовки та проведення ЛСОАП має бути розроблений та затверджений відповідною посадовою особою замисел та план-графік спеціальної операції. У замислі повинні бути відображені такі основні положення:

1. Мета локальної спеціальної операції.

2. Висновки із оцінки обстановки (противник та його основні параметри, зокрема чисельність особового складу, що залучений до агресії, чисельність резерву, співвідношення воєнних потенціалів, допустимі втрати особового складу супротивника, за яких він відмовляється від подальших бойових дій $M_{одон}$, допустимі втрати озброєння і військової техніки супротивника, за яких він відмовляється від агресії $M_{овтдон}$, оцінений інтегральний рівень воєнної загрози, прогностні ризики деструктивного впливу на визначальні сфери національної безпеки, найбільш вразливі місця (точки) нанесення збитку противнику асиметричними діями).

3. Бойові завдання суб'єктам, що залучаються до ЛСО. Особливістю даного пункту замислу є не тільки зміст бойового завдання, але і визначений ступінь його впливу на досягнення мети ЛСО, який оцінюється за 8-бальною шкалою експертним шляхом з використанням моделі M7 [2]. Крім того, для кожного суб'єкта формується мережева граф-модель проведення асиметричних заходів, у якій вершини представляють собою завдання або їх етапи, а дуги визначають часові нормативи їх виконання. Бойові завдання повинні відповідати можливостям залучених до операції суб'єктів, рівню їх підготовки, часу на підготовку до проведення ЛСО, обстановці, що склалася. Повинні також враховуватися цінність та обмеженість ресурсів, можливі втрати особового складу та озброєння і військової техніки, ризики та можливі негативні наслідки у разі недосягнення мети ЛСО тощо.

4. Завдання щодо підготовки району проведення ЛСО.

5. Порядок та способи виведення суб'єктів, із яких сформовано потенціал асиметричної протидії, в район проведення ЛСО.

6. Управління в ході проведення ЛСО. Основна та резервна системи зв'язку та порядок взаємодії з іншими складовими сил оборони.

7. Легендування ЛСО.

8. Спеціальне інформаційне, психологічне та іміджове забезпечення проведення ЛСО.

9. Порядок виходу із ЛСО.

Найбільш складними положеннями замислу є вибір найвразливіших місць (“больових” точок) противника та обґрунтування часткових завдань суб’єктам інтегрованого потенціалу асиметричної протидії.

Основними найбільш вразливими місцями (“больовими” точками) противника є:

воєнний, економічний та морально-психологічний потенціали держави та збройних сил;

безпека об’єктів критичної інфраструктури;

живучість систем розвідки, управління, вогневого ураження;

безпека систем життєзабезпечення військових формувань;

міжнародний імідж держави, збройних сил, правоохоронних органів спеціального призначення тощо.

Обґрунтування часткових завдань суб’єктам сформованого інтегрованого потенціалу асиметричної протидії може здійснюватися за процедурою, наведеною у [2].

Під формуванням інтегрованого потенціалу асиметричної протидії загрозам воєнного характеру будемо розуміти ітераційний процес вибору раціонального складу сил і засобів СБОУ та визначення їх необхідних спроможностей щодо створення необхідного рівня деескалації загрози $\Delta K_{нзн}$ на вибраний момент прогнозування T_{np} . Процес формування гіпотетичного потрібного рівня деескалації загрози суб’єктами, що належать до політичної, економічної, інформаційної та воєнної сфер, з використанням методу Ісікави [6] наведено на рис. 2.

Рис. 2. Приклад формування гіпотетичного потрібного рівня деескалації загрози з використанням методу Ісікави

Джерело: розроблено авторами.

Для скорочення викладки позначення на рис. 2 розглянуті на прикладі інформаційної сфери. Для інших сфер викладки аналогічні, змінюються лише індекси назв сфер.

Для інформаційної сфери:

– $P_{I1} \dots P_{In}$ – показники загрози та їх “вага” в

інформаційній сфері;

– $P_{I1}^* \dots P_{In}^*$ – показники загрози та їх допустима залишкова “вага” після реалізації потрібного рівня деескалації загрози;

– $\Delta I_1 \dots \Delta I_n$ – мінімально допустиме зменшення

“ваги” (пріоритетів) показників загроз за шкалою Сааті [9] після реалізації потрібного рівня деескалації загрози;

– $\{P_{In}\}$ – множина завдань суб’єкта інформаційної сфери щодо деескалації загрози.

Визначені множини завдань суб’єктам, що утворили інтегрований потенціал протидії, є необхідними мінімально допустимими спроможностями цих суб’єктів і розглядаються як їх часткові операційні завдання.

Традиційно завдання вважається виконаним, якщо визначено достатню кількість виконавців із спроможностями, що забезпечили його виконання, задіяні ресурси не перевищили виділених, а втрати не перевищили допустимих.

Оскільки запропонований метод формування інтегрованого потенціалу асиметричної протидії являє собою найвищий рівень системного використання суб’єктів СБОУ для нейтралізації загрози в системі забезпечення воєнної безпеки, то цільова функція деескалації загрози має бути орієнтованою на досягнення синергетичного ефекту як результату використання складної системи [8; 10].

Синергетичний ефект від асиметричних заходів протидії у вибраних вразливих (“больових”) точках противника може бути отриманий завдяки чітко спланованому їх впровадженню в політичній, економічній, інформаційно-комунікаційній, кібернетичній і власне воєнній сферах.

Для практичної реалізації зазначеної вимоги пропонується відмінний від традиційного когнітивний підхід до процесу підготовки та виконання часткових операційних завдань суб’єктами, який базується на теорії та методах експертних систем [11], експертно-значущих проміжних сценаріїв (ЕЗПС) [8; 12], аналізу ієрархій [9] та ін.

Когнітивний підхід передбачає формування воєнними ЕЗПС (рис. 3), під якими розуміють вибрані експертами відносно самостійні етапи визначення завдань, без яких розробити операційне завдання неможливо. Стисло опишемо часткові завдання, які вирішують на кожному із зазначених ЕЗПС.

Сценарій № 1 – виявлення в ході моніторингу загрози z , оцінювання її рівня, порівняння з пороговим рівнем та прийняття рішення на її асиметричну деескалацію.

Сценарій № 2 – вибір суб’єктів для формування інтегрованого потенціалу асиметричної протидії. Здійснюється методом мозкового штурму експертами-фахівцями у сфері національної та воєнної безпеки з використанням баз даних відповідної експертної системи (ЕС).

Рекомендується вибирати ті суб’єкти, які опікуються сферами, у яких найвагомніше проявляються ознаки виявленої загрози воєнного характеру. При цьому можуть використовуватися паспорти

загроз [10].

Сценарій № 3 – оцінювання потрібного рівня деескалації загрози $\Delta K_{нзп}(T_{np})$. Потрібний рівень деескалації загрози оцінюється з використанням бази знань ЕС про загрози (якщо така створена) [11] та комп’ютерної технології М7 ітераційним способом шляхом зниження показників “ваги” (пріоритетів) загроз за шкалою Сааті доти, поки не буде досягнута умова

$$\Delta K_{нзп}(T_{np}) = K_{\partial} \Delta K(t_1), \quad (1)$$

де K_{∂} – коефіцієнт деескалації (набуває фіксованих значень: у разі використання несилових засобів $K_{\partial} = 1,1$; у разі використання силових засобів $K_{\partial} = 1,2$ [10]);

$\Delta K(t_1)$ – зміна рівня воєнної загрози як різниця між отриманим поточним рівнем воєнної загрози $K(t_1)$ на час t_1 та пороговим K_{np} (визначається у правовому просторі держави).

Сценарій № 4 – визначення нейтралізаційних завдань для кожного s -го суб’єкта, що утворюють інтегрований потенціал асиметричної протидії та їх вагових показників $(P_{s1}^* \dots P_{sn}^*)$. Може бути здійснено з використанням бази знань ЕС про загрози, удосконаленого методу аналізу ієрархій, експертного оцінювання та комп’ютерної технології М7. Практика показує, що досягнення необхідної “ваги” показника P_s^* можна забезпечити певною множиною окремих завдань (заходів), що реалізуються у s -й сфері. Чим більше таких заходів здійснюється, тим швидше досягається потрібний результат, але при цьому зростають (і не завжди пропорційно) ресурси на їх проведення, що може бути заблоковано на сценарії № 8.

Множину таких заходів для кожної s -ї сфери експертам цієї ж сфери доцільно формувати методом мозкового штурму з використанням бази знань ЕС про загрози. До того ж експерти повинні бути готовими оцінювати потреби у ресурсах для реалізації запропонованих варіантів асиметричних заходів.

Сценарій № 5 – оцінювання поточного (прогнозованого) рівня деескалації загрози $\Delta K_{нзп}(T_{np})$ [13].

Визначений сценарієм № 4 варіант множини завдань (заходів) для кожної сфери (третій рівень трирівневої ієрархічної моделі) вводять в комп’ютерну технологію М7 і за її допомогою обчислюють поточний (прогнозований) рівень деескалації загрози $\Delta K_{нзп}(T_{np})$. При цьому може уточнюватися “вага” (пріоритет) кожної сфери, що буде враховуватися під час перерозподілу ресурсів у разі потреби.

Рис. 3. Послідовність визначення завдань складовим інтегрованим потенціалу асиметричної протидії з використанням методу експертно-значущих проміжних сценаріїв
Джерело: розроблено авторами.

Підвищення точності прогнозування може бути досягнуто за рахунок використання ЕС, уточнення за її допомогою факторів та умов, які найбільше впливатимуть на динаміку рівня розглядуваної загрози.

Сценарій № 6 – перевірка на достатність отриманого поточного (прогнозованого) рівня деескалації загрози

$$\Delta K_{нзпр}(T_{пр}) \geq \Delta K_{нзп}(T_{пр}). \quad (2)$$

Якщо умова (2) виконується, то для кожної s -ї сфери в сценарії № 4 фіксуються відповідні множини завдань $\{Z_s\}$ та їх “вага” (пріоритети). Якщо зазначена умова не виконується, то з використанням ЕС здійснюється нова ітерація вибору суб’єктів у сценарії № 2 або вибирається новий варіант зниження показників “ваги” (пріоритетів) загроз за шкалою Сааті у сценарії № 3, або формується новий варіант множини нейтралізаційних завдань у сценарії № 4.

Сценарій № 7 – ураховуючи накопичений досвід та відповідний методичний матеріал, який занесений у відповідну базу знань ЕС, проводять оцінювання потрібних ресурсів $R_{\Sigma z}$ для виконання зафіксованого в сценарії № 4 варіанта множини завдань усіма суб’єктами щодо деескалації виявленої загрози z .

Сценарій № 8 – перевірка оцінених у сценарії № 7 потрібних ресурсів $R_{\Sigma z}$ на відповідність виділеним ресурсам $R^*_{\Sigma z}$.

Якщо умова $R_{\Sigma z} \leq R^*_{\Sigma z}$ не виконується, то здійснюється нова ітерація або у сценарії № 4, або у сценарії № 3, або у сценарії № 2.

Якщо умова $R_{\Sigma z} \leq R^*_{\Sigma z}$ виконується, то особі, яка приймає рішення, надається для затвердження проект управлінського рішення щодо нейтралізації виявленої загрози визначеним складом суб’єктів з обґрунтованими завданнями кожному суб’єкту.

Практична реалізація описаних експертно-значущих сценаріїв потребує специфічного управління у секторі безпеки і оборони, а також відповідного інформаційно-аналітичного та ресурсного забезпечення, що дозволить реалізовувати асиметричні заходи протидії у неочікуваних для держави-агресора місцях (“больових” точках), завдавати йому неприйнятної збитку і тим самим примушувати противника відмовлятися від застосування військової сили проти держави-жертви агресії.

7. Базові засади оцінювання результативності проведення локальної спеціальної операції асиметричної протидії в інтересах забезпечення достатнього рівня воєнної безпеки держави

Україна здійснює стратегічний перегляд концепції оборони з урахуванням досвіду подолання поточної кризи, запровадження нових методів кері-

вництва обороною, які ґрунтуються на євроатлантичному досвіді за критерієм – висока ефективність за прийнятних витрат. Одночасно передбачається створення результативного механізму формування і реалізації державної політики з питань забезпечення воєнної безпеки. Першочерговим завданням визначено створення дієвої системи управління сектором безпеки і оборони держави.

Формування національних оборонних спроможностей передбачає поліпшення взаємодії і координації дій органів державної влади та складових СБОУ з урахуванням особливостей сучасної збройної боротьби, у ході якої широко використовуються не лише традиційні військові сили та засоби, а й різноманітні невійськові. Основним обмеженням при цьому виступають ресурси, які держава виділяє для зниження рівня воєнної небезпеки.

Основними вимогами до системи забезпечення воєнної безпеки є гарантування надійного захисту держави від зовнішніх і внутрішніх загроз, запобігання виникненню збройного конфлікту, а у разі збройного конфлікту – його локалізація і нейтралізація тими ресурсами, які є у розпорядженні держави.

Виходячи із засад внутрішньої і зовнішньої політики, характеру актуальних загроз національній безпеці основними завданнями воєнної політики України у найближчий час і в середньостроковій перспективі визначено створення цілісного СБОУ як головного елемента системи забезпечення воєнної безпеки, інтеграція спроможностей його складових для своєчасного й ефективного реагування на наявні та потенційні загрози, забезпечення підвищення спроможностей сил оборони, необхідних для досягнення цілей воєнної політики з урахуванням наявних у держави можливостей і ресурсів.

Прийнятні витрати розглядаються переважно розвиненими демократичними країнами, у яких громадянське суспільство виступає основною соціально-політичною силою, що визначає внутрішню і зовнішню політику цих країн, у тому числі й у воєнній сфері, та здійснює суспільний контроль за владою. Громадянське суспільство головною цінністю визначає життя людини, її права і безпеку. Для громадянського суспільства неприйнятний військовий шлях вирішення зовнішньополітичних проблем, якщо бойові дії пов’язані із значними втратами своїх громадян. Проте таке положення стосується тільки ситуацій, які не загрожують існуванню цих держав. У разі ж агресії проти них ставлення до втрат своїх військ буде абсолютно іншим, і держави, поза сумнівом, підуть на жертви заради збереження свого суверенітету і незалежності.

Оскільки сучасна геополітична ситуація така, що розвинені країни й їх союзи домінують в економічному, політичному, інформаційному і військово-мудовищенні, тому прямої військової загрози для

них не існує [8], хоча і зберігається реальна загроза тероризму [14], у боротьбі проти якого Захід може піти на певні жертви. Використовувати ж військову силу в ситуаціях, які не загрожують існуванню держави, стає складніше по мірі становлення громадянського суспільства.

Таким чином, для розвинених демократичних країн все більшого значення у воєнній сфері набуває цивілізаційний чинник, що зумовлює рівень допустимих втрат у живій силі під час вирішення зовнішньо-політичних проблем військовим шляхом.

Досвід воєнних конфліктів різного масштабу в останнє десятиліття свідчить про те, що рівень допустимих втрат становить десятки, якщо не одиниці, людських життів і стає одним з найважливіших чинників заборони застосування військової сили [15–16]. Євроатлантичний досвід свідчить, що під час планування використання військової сили очікувані втрати особового складу держави, що проводить наступальні дії, мають статус ресурсного обмеження від 0,5 до 1,0%. Для держави-жертви агресії втрати особового складу, населення, інфраструктури тощо у такому конфлікті значно більші. Світовий досвід показує, що значно слабша у військовому відношенні країна, проводячи асиметричні заходи протидії загрозам військовими і невійськовими суб'єктами сектору безпеки і оборони здатна завдати противнику неприйнятної збитку і тим самим примусити навіть більш сильного у воєнному відношенні противника відмовитися від застосування військової сили проти неї.

Виходячи із зазначеного, найбільш пріоритетним завданням асиметричної протидії загрозам воєнній безпеці держави-жертви агресії доцільно визначити: *раціонально використовуючи ресурси нанести противнику у найбільш вразливих і неочікуваних для нього місцях (“точках”) таких збитків, за яких він вимушений відмовитися від подальших агресивних дій.*

Асиметричні заходи здійснюються спеціально підготовленими суб'єктами або виділеними ними силами, як правило, у формі локальної спеціальної операції (ЛСО). Кількість ЛСО залежить від противника, ресурсів та можливостей держави-жертви агресії.

Ураховуючи зазначене, очікувана ефективність протидії ($E_{ea}(t)$) агресії держави, що значно перевищує державу-мішень у військовій “потужності”, може бути оцінена сумарним рівнем деескалації загрози на момент часу t за рахунок симетричної (прямой військової) та асиметричної (комплексної) протидії агресії.

$$E_{ea}(t) = K_a(t_{an}) - \sum_{i=1}^I \Delta K_{AC_i}(t_{ik}, R_{res_i}, M_{oc_i}, M_{ovm_i}) - \sum_{i=1}^I \Delta K_{kv}(t_{in}, R_{res}, M_{oc}, M_{ovm}) - \Delta K_{kv}(t_a > t_{JK}, R_{res}, M_{oc}, M_{ovm}),$$

$$\text{при } R_{res_i} \leq R_{res_{ei}}; \quad M_{oc_i} \leq M_{ocdon_i}; \\ M_{ovm_i} \leq M_{ovmdon_i},$$

де $K_a(t_{an})$ – рівень загрози, що несе державі-жертві розв'язувана агресія;

ΔK_{AC_i} – зниження рівня загрози за рахунок проведення i -ї ЛСО;

$\Delta K_{kv}(t_{in})$ – зниження рівня загрози на початок проведення i -ї ЛСО за рахунок комплексного використання військових і невійськових сил та засобів держави-жертви агресії (симетричної протидії);

t – поточний час протидії (відбиття) агресії;

$t_{an}(t_{ak})$ – час початку (закінчення) агресії;

$t_{in}(t_{ik})$ – час початку (закінчення) i -ї, ($i=1, I$), ЛСО;

I – кількість проведених ЛСО;

R_{res} – ресурси, що використовуються при відбитті агресії симетричними методами або комплексним використанням військових і невійськових інструментів [7];

$R_{res_i}(R_{res_{ei}})$ – ресурси (максимально можливі ресурси), що використовуються при проведенні i -ї ЛСО;

M_{oc} – втрати особового складу, у тому числі невійськових суб'єктів сил оборони, що залучаються до відбиття агресії;

M_{ovm} – втрати озброєння і військової техніки в ході відбиття агресії;

$M_{oc_i}(M_{ocdon_i})$ – втрати (допустимі втрати) особового складу при проведенні i -ї ЛСО;

$M_{ovm_i}(M_{ovmdon_i})$ – втрати (допустимі втрати) ОВТ в i -й ЛСО.

Гіпотетичний приклад оцінювання ефективності відбиття агресії держави, що значно перевищує державу-мішень у військовій “потужності” з використанням симетричної і асиметричної протидії у двох ЛСО ($I=2$) показаний на рис. 4.

Звідси ефективність асиметричної протидії агресії ($E_{AC}(t_a)$) у загальному вигляді може бути оцінена, як результат сумарного зниження рівня загрози в проведених ЛСО:

$$E_{AC}(t_a) = \sum_{i=1}^J \Delta K_{AC_i}(t_{ik}, R_{res_i}, M_{oc_i}, M_{ovm_i}).$$

Критерієм прийняття рішення державою-агресором на відмову від подальших агресивних дій є виконання хоча б однієї з умов:

$$E_{ea}(t_{ak}) \leq K_{an}(t_{ak}); \\ M_{oca}(t_{ak}) \geq M_{ocad},$$

де $K_{an}(t_{ak})$ – пороговий рівень загрози, яку спричинила державі-жертві агресії розпочата проти неї агресія;

$M_{oca}(t_{ak})$ – втрати особового складу держави-

агресора, що був задіяний для здійснення агресії, у тому числі залучені бойовики, найманці тощо;

M_{ocad} – допустимі для держави-агресора втрати особового складу.

Рис. 4. Гіпотетичний приклад оцінювання ефективності відбиття агресії держави, що значно перевищує державу-мішень у військовій “потужності” з використанням симетричної і асиметричної протидії у двох ЛСО ($I=2$)

Джерело: розроблено авторами за даними [9].

Припинення агресії проти держави-жертви може бути здійснено і за інших умов, наприклад, за рішенням Ради Безпеки ООН, у відповідь на ультиматум створеної коаліції держав тощо.

Отже, розроблені базові засади оцінювання результативності проведення ЛСО асиметричної протидії дали змогу синтезувати модель оцінювання ефективності асиметричної протидії загрозам воєнній безпеці держави за показником сумарного зниження рівня загрози в проведених ЛСО, а також сформулювати систему обмежень та обґрунтувати критерій прийняття рішення державою-агресором на відмову від подальших агресивних дій.

Висновки

Запропонована концепція асиметричної протидії ворожій державі спрямована на нейтралізацію її деструктивного впливу на забезпечення національної безпеки слабшої у воєнному відношенні країни шляхом впровадження технологій підготовки та ведення асиметричної протидії.

На основі розробленої та описаної у попередній публікації узагальненої моделі гібридної агресії

(війни) побудовано концептуальну модель ітераційного формування потенціалу асиметричної протидії загрозам воєнній безпеці держави та запропоновано концептуальний підхід до формування замислу локальної спеціальної операції асиметричної протидії, визначення часткових завдань суб'єктам, що залучаються до неї, визначені базові засади оцінювання результативності проведення локальної спеціальної операції асиметричної протидії в інтересах забезпечення достатнього рівня воєнної безпеки держави.

Практична реалізація концепції в практику забезпечення воєнної безпеки держави, що значно слабша у військовому та економічному відношенні, здатна завдати противнику неприйнятної збитку і тим самим примусити його відмовитися від застосування військової сили проти неї, здійснюючи асиметричні заходи протидії військовими і невійськовими суб'єктами сил оборони.

У наступних публікаціях запропоновані концептуальні підходи будуть деталізовані та представлені у вигляді конкретних методик і практичних рекомендацій воєнно-політичному керівництву та окремим суб'єктам сил оборони держави.

Список літератури

1. Богданович В.Ю. Концепція асиметричної протидії ворожій державі для нейтралізації її впливу на визначальні сфери національної безпеки України (початок) / В.Ю. Богданович, А.М.Сиротенко, О.В. Дублян // Наука і техніка Повітряних Сил Збройних Сил України. – 2020. – № 3(40). – С. 13-24. <https://doi.org/10.30748/ntps.2020.40.02>.

2. 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. Черняхівського, 2019. – 268 с.
3. Операции информационно-психологической войны [Електронний ресурс] / В. Вепринцев, А. Манойло, А. Петренко, Д. Фролов. – Режим доступу: <http://psyfactor.org/psyops/psyops4.htm>.
4. Литвиненко О.В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія / О.В. Литвиненко. – К.: НІСД, 2003. – 240 с.
5. 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.
6. Метод “Діаграма Ісікави” [Електронний ресурс]. – Режим доступу: <http://www.inventech.ru/pub/methods/metod-0019/>.
7. Дубницький В.Ю. Інтервальне оцінювання кількості учасників масових протестних акцій / В.Ю. Дубницький, Г.Г. Зубрицька, А.М. Кобылин // Сучасні інформаційні системи. – 2018. – Т. 2. – № 4. – С. 11-20. <https://doi.org/10.20998/2522-9052.2018.4.02>.
8. Богданович В.Ю. Теоретико-методологічні основи забезпечення національної безпеки України: монографія / В.Ю. Богданович, І.Ю. Свида, Є.Д. Скулиш; у 7 т. Т. 1: Теоретичні основи, методи й технології забезпечення національної безпеки України. – К.: Наук.-вид. відділ НА СБ України, 2012. – 548 с.
9. Саати Томас Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. Пер. с англ. / Томас Л. Саати – М.: Издательство ЛКИ, 2008. – 360 с.
10. Богданович В.Ю. Теоретико-методологічні основи забезпечення національної безпеки України: монографія / В.Ю. Богданович, І.Ю. Свида, Є.Д. Скулиш; у 7 т. Т. 4: Воєнна безпека України та шляхи її забезпечення. – К.: Наук.-вид. відділ НА СБ України, 2012. – 464 с.
11. Экспертные системы: Структура и классификация [Електронний ресурс]. – Режим доступу: <http://www.prorobot.ru/nauka/expert-systems-structure-and-classification.php>.
12. Богданович В.Ю. Методика автоматизованого моделювання експертно-аналітичних сценаріїв виявлення та усунення загроз реалізації національних інтересів / В.Ю. Богданович, А.Л. Висідалко // Наука і техніка Повітряних сил Збройних Сил України. – 2015. – № 3(20). – С. 21-29.
13. Богданович В.Ю. Методичний підхід до визначення необхідних спроможностей складових інтегрованого потенціалу протидії загрозам на виконавчому рівні / В.Ю. Богданович, А.М. Прима // Наука і техніка Повітряних сил Збройних Сил України. – 2017. – № 2(27). – С. 162-166.
14. Власюк О.С. Національна безпека України: еволюція проблем внутрішньої політики: вибр. наук. праці / О.С. Власюк. – К.: НІСД, 2016. – 528 с.
15. Цыгичко В.Н. О категории “соотношение сил” в потенциальных военных конфликтах / В.Н. Цыгичко // Военная мысль. – М., 2002. – № 3. – С. 5-6.
16. Чекинов С.Г. Асимметричные действия по обеспечению военной безопасности / С.Г. Чекинов, С.А. Богданов // Военная мысль. – 2010. – № 3. – С. 13-22.

Надійшла до редколегії 10.08.2020

Схвалена до друку 15.09.2020

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>

Сиротенко Анатолій Миколайович

доктор військових наук
Начальник Національного університету оборони України
ім. І. Черняхівського,
Київ, Україна
<https://orcid.org/0000-0002-0266-5706>

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>

Information about the authors:

Vladimir Bohdanovych

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

Anatoliy Sirotenko

Doctor of Military Sciences
Chief of Ivan Chernyakhovsky National Defense
University of Ukraine,
Kyiv, Ukraine
<https://orcid.org/0000-0002-0266-5706>

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>

**КОНЦЕПЦИЯ АСИММЕТРИЧНОГО ПРОТИВОДЕЙСТВИЯ ВРАЖДЕБНОМУ ГОСУДАРСТВУ
ДЛЯ НЕЙТРАЛИЗАЦИИ ЕГО ВЛИЯНИЯ НА ОПРЕДЕЛЯЮЩИЕ СФЕРЫ
НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ
(окончание)**

В.Ю. Богданович, А.М. Сиротенко, О.В. Дублян

В статье обоснованы концептуальные положения организации асимметричного противодействия агрессии более мощного в военном отношении государства со стороны государства-жертвы агрессии в интересах защиты своих фундаментальных жизненно важных национальных интересов. Приведены структурно-логическая последовательность и принципы противодействия информационно-психологическому влиянию со стороны враждебного государства. Предложен концептуальный подход к формированию замысла локальной специальной операции асимметричного противодействия и определения частных задач субъектов, которые к ней привлекаются. Определены базовые основы оценивания результативности проведения локальной специальной операции в интересах обеспечения достаточного уровня военной безопасности государства.

Ключевые слова: асимметричное противодействие, военная сила, военная безопасность, эффективность противодействия, вооруженный конфликт, силовое давление, угроза.

**THE CONCEPT OF ASYMMETRIC COUNTERACTION TO THE HOSTILE STATE FOR NEUTRALIZATION
OF ITS INFLUENCE ON THE DEFINITIVE SPHERES OF NATIONAL SECURITY OF UKRAINE
(end)**

V. Bogdanovich, A. Syrotenko, O. Dublyan

The article substantiates the conceptual theses of the organization of asymmetric counteraction to the aggression of a “powerful” state in militarily sense on the part of the state-victim of aggression in the interests of protection of its fundamental vital national interests. The structural-logical sequence and principles of organization of counteraction to information-psychological influences on the part of the unfriendly state are resulted. Given that asymmetric measures are carried out by specially trained entities or their assigned forces, usually in the form of a local special operation, a conceptual approach to the design of such an operation and the definition of partial tasks for entities involved in it. The use of security and defense actors in the operation should be aimed at achieving a synergistic effect from asymmetric countermeasures. The synergetic effect is expected to be achieved through the clearly planned implementation of asymmetric countermeasures in the political, economic, information and communication, cyber and military spheres. For the practical implementation of this requirement, a different from the traditional cognitive approach to the process of preparation and execution of partial operational tasks by entities, based on the theory and methods of expert systems, expert-significant intermediate scenarios, hierarchy analysis, etc. The approach involves the formation of eight scenarios, which are understood by the experts selected relatively independent stages of task definition, without which it is impossible to develop an operational task. It is proposed to assess the effectiveness of countering state aggression, which significantly outweighs the target state in terms of military power, by the total level of de-escalation of the threat at a certain point in time due to symmetric (direct military) and asymmetric (complex) countering aggression in the form of local special operations.

Keywords: asymmetric counteraction, military power, military security, threat, armed conflict, force pressure, counteraction efficiency.