

УДК 355/359].07(477)

**Сальнікова О. Ф., д-р наук з держ. упр., ст. наук. співроб.<sup>1</sup>** (0000-0002-7190-6091);

**Іващенко А. М. канд. техн. наук, доцент<sup>2</sup>** (0000-0002-8131-5463);

**Сівоха І. М.<sup>1</sup>** (0000-0001-5377-2520)

<sup>1</sup> – Навчально-науковий центр стратегічних комунікацій у сфері забезпечення національної безпеки та оборони Національного університету оборони України імені Івана Черняхівського, Київ;

<sup>2</sup> – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## **Застосування рефлексивного управління в стратегічних комунікаціях для протидії загрозам гібридного характеру**

**Резюме.** У сучасному світі поєднання пропаганди, дезінформації, психологічного тиску, атак на інформаційні та комунікаційні системи являють собою небезпеку, яка не менше за традиційні системи озброєнь. Результативні сценарії протидії гібридним загрозам базуються на використанні сучасних технологій стратегічних комунікацій, управління суб'єктами воєнних конфліктів, обробки інформації. У статті проводиться аналіз основних концепцій сучасних війн гібридного типу, визначається місце, мета, завдання і особливості стратегічних комунікацій. Для розроблення сценаріїв протидії загрозам гібридного характеру пропонується інтегроване використання технологій стратегічних комунікацій і рефлексивного управління.

**Ключові слова:** сучасні війни гібридного типу; стратегічні комунікації; інформаційні технології; рефлексивне управління.

**Постановка проблеми.** Війна гібридного типу з використанням широкого набору воєнних і невоєнних інструментів для здійснення тиску на Україну, зміни її стратегічного вибору та існуючого устрою, створюють серйозні виклики для національної безпеки. Складнішою є протидія загрозам гібридного характеру та виявлення гібридних атак, особливо на ранніх стадіях. Удосконалення методів протидії, зокрема інформаційних і комунікаційних, використання для цього сучасних наукових методів, є актуальною проблемою. З врахуванням суперечливих позицій науковців і практиків щодо застосування стратегічних комунікацій в протидії гібридній війні, зазначене обумовлює необхідність дослідження основних концепцій сучасних війн гібридного типу, визначення місця, мети, завдань і особливостей стратегічних комунікацій, розроблення рекомендацій щодо інтегрованого використання технологій стратегічних комунікацій і сучасної теорії і методів управління в протидії гібридній війні.

**Аналіз основних досліджень і публікацій.** Сучасні стратегії протидії на основі широкого застосування інформаційної зброї, як одного з ключових факторів стримування, розглядаються в роботах воєнного теоретика Ф. Хоффмана [1], колишнього міністра оборони США Дж. Мэттиса [2], професора Лондонської

школи економіки М. Калдор [3], розробках корпорації RAND.

Питання стратегічних комунікацій, як скоординованого і належного використання комунікативних можливостей держави: публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних і психологічних операцій, заходів, спрямованих на просування цілей держави [4], розглядаються як у національних документах оборонного планування, так і широким колом вітчизняних науковців [5-8]. Так, Стратегія національної безпеки України визначає загрози в інформаційній сфері та напрями протидії їм. У Воєнній доктрині України одним з основних інструментів реалізації державної політики в інформаційній сфері визначено стратегічні комунікації. Стратегічним оборонним бюлетенем України визначено розвиток стратегічних комунікацій одним з основних напрямів удосконалення системи управління силами оборони. Автори [6] обґрунтували структуру системи стратегічних комунікацій Міністерства оборони та Збройних Сил України і показали схожість процесів, що відбуваються під час комунікацій, із управлінськими процесами. У [7] надаються рекомендації із застосування стратегічних комунікацій в системі управління Збройними Силами України.

Словосполучення “стратегічні комунікації” має глибокий сенс. “Стратегічні” свідчить про те, що мету комунікацій визначають на найвищому політичному рівні, охоплюють все суспільство і поширюють на

міжнародну аудиторію. Завдання комунікацій відповідають національним цінностям і спроможностям та направлені на поліпшення національної стратегічної позиції порівняно з позицією противника. “Комунікації” означають не лише діалог, а й спрямовану “згори донизу” інформаційну діяльність. Поняття “стратегічних комунікацій” на сучасному етапі розвитку суспільства підкреслює актуальність інтеграції всіх інструментів впливу на окремих людей, цільові групи, країни та на їх поведінку в єдиний комплекс [8].

Водночас, питання впливу стратегічних комунікацій на процеси прийняття рішень та управління в умовах гібридної війни залишаються відкритими.

**Метою статті** є аналіз основних концепцій сучасних війн гібридного типу і визначення особливостей інтегрованого використання технологій стратегічних комунікацій і рефлексивного управління в умовах загроз гібридного типу.

**Виклад основного матеріалу.** Гібридні війни (ГВ) плануються і проводяться державними і недержавними суб'єктами з урахуванням, що їх дії залишаються нижче звичайного рівня виявлення та реагування, чому сприяють високі швидкості, обсяг і доступність інформаційних обмінів. Окремо такі дії здаються незначними, однак у сукупності мають на меті занурення країни-мішені в хаос. На сьогодні не існує погодженого визначення терміна ГВ, що суттєво ускладнює розроблення відповідної нормативно-правової бази.

Так, *Ф.Хоффман* визначає ГВ як “фатальний міждержавний конфлікт з тривалим періодом ведення війни нестандартними засобами” [1].

*Національна воєнна стратегія США* [9] визначає гібридний конфлікт як проміжний стан між внутрішнім і міждержавним конфліктами, якому притаманні бойові дії з такими ознаками: поєднання звичайних збройних сил і нерегулярних сил для створення невизначеності, перехоплення ініціативи і послаблення супротивника; застосування як традиційних воєнних, так і асиметричних форм і способів; участь збройних формувань, які заперечують свою причетність до будь-якої держави.

Як вказується в цьому документі, “Імовірність залучення США до міждержавного конфлікту оцінюється як низька, але зростаюча. Якщо це станеться, то наслідки будуть величезними. Насильницькі екстремістські організації, навпаки, являють собою безпосередню загрозу для транснаціональної безпеки, поєднуючи легкодоступні технології з екстремістською ідеологією. Там, де перетинаються державне і недержавне насильство, існує область конфлікту, у якій суб'єкти з'єднують техніки, можливості та ресурси, для досягнення своїх цілей. У таких гібридних конфліктах можуть брати участь збройні сили, що приховують свою ідентичність, як Росія зробила в Криму, або до них залучаються рудиментарні можливості насильницьких екстремістських організацій з формування регулярних збройних сил, як це продемонструвала терористична організація ІДІЛ в Іраку і Сирії”. Отже, ГВ визначається такою, яка відповідає певному діапазону лінійної залежності імовірності виникнення конфлікту  $P$  та його наслідків  $I$  (рис. 1).

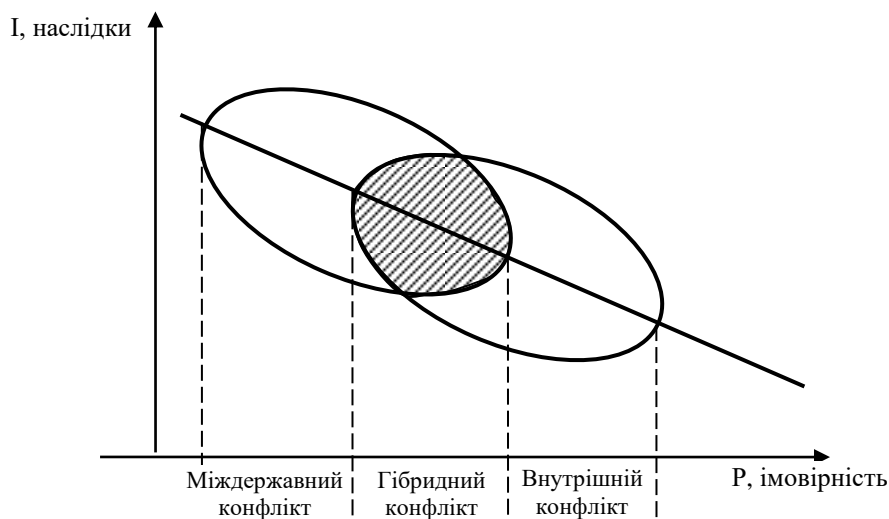


Рис. 1. Спектр сучасних конфліктів за поглядами США [9, р. 8]

*Російський підхід* [10] до сучасних війн базується на теорії управління воєнними конфліктами. Як регульована (вихідна) величина використана руйнівна сила війни (глобальні, воєнно-політичні і воєнні наслідки I), яка має десять базових дискретних рівнів, кожному з яких відповідає певна імовірність P виникнення і відповідний воєнно-політичний сценарій (рис. 2).

На рівні *несилового протистояння* реалізується три сценарії, найбільший з яких за наслідками, отримав назву ГВ. Крім того, на рівні ГВ знаходиться точка біфуркації (неповернення), у якій мішень війни стає нестійкою до зовнішнього впливу, і виникає

невизначеність: або стан хаосу і подальшої руйнації, або перехід на нову, більш диференційовану і результативну систему управління. Із досягненням точки біфуркації сторони конфлікту приймають рішення на мирне врегулювання, або здійснюється перехід до подальшого нарощування інтенсивності бойових дій, включно до глобального конфлікту. Цим визначається загроза ГВ як нового виду міждержавного протистояння. Водночас ГВ розглядається як феномен, який включає різні форми і способи впливу на противника і не може бути локалізованим тільки на одному з рівнів протистояння.

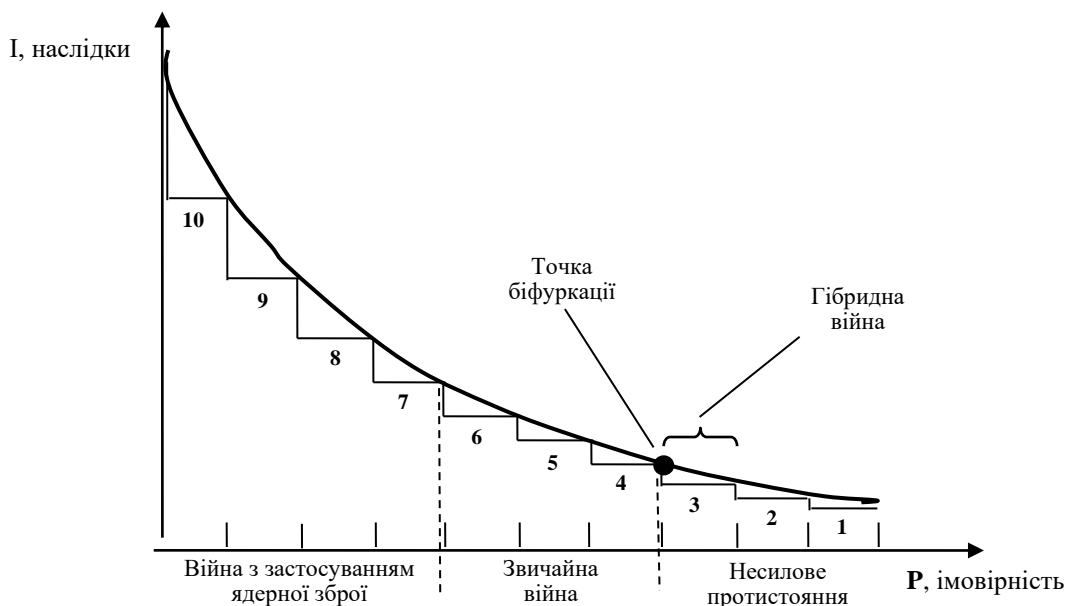


Рис. 2. Спектр сучасних конфліктів за поглядами РФ

Позначення шкали I (воєнно-політичні сценарії): 1 - стабільний стан мирової політичної системи; 2 - політична криза з підвищеною інтенсивністю демонстрації воєнної сили; 3 - гібридна війна; 4 - обмежена (локальна) звичайна війна; 5 - широкомасштабна звичайна війна без ураження великих міських агломерацій, хімічних виробництв, атомних електростанцій; 6 - звичайна війна з ураженням великих міських агломерацій, хімічних виробництв, атомних електростанцій, що можливо прирівняти до застосування зброї масового враження; 7 - ядерний конфлікт (кризова ситуація, до якої залучені одна чи декілька країн, які мають ядерну зброю(ЯЗ) і одна з них починає її використовувати як інструмент воєнно-політичного тиску без прямого застосування; 8 - демонстраційне використання ЯЗ у пустинній місцевості без враження людей, військових і економічних об'єктів; 9 - війна з обмеженим використанням ЯЗ; 10 - масоване застосування ЯЗ.

Російській підхід має такі відмінності від західних оцінок:

початок конфлікту визначається з моменту, коли виявляються відмінності інтересів двох держав, це набагато нижчий рівень інтенсивності, ніж той, що використовується в західних визначеннях;

лінійна концепція нарощування інтенсивності гібридної війни замінюється послідовністю параболічного характеру: воєнні та невоєнні операції досягають критичного переломного моменту, а потім їх

інтенсивність може знижуватися під час досягнення стратегічних цілей.

На думку низки зарубіжних дослідників, в основу нової російської концепції війни XXI століття лягли методи рефлексивного управління [11, 12].

Водночас, наведені концепції гібридної війни мають такі недоліки: відсутність базового елементу; нечіткі концептуальні рамки; нездатність охопити комунікації всередині цілісного явища; невизначеність кінцевого стратегічного місцезнаходження.

Отже, за офіційними поглядами, прийнятими в США і Росії, мета ГВ полягає у встановленні зовнішнього управління і тотального контролю над сферою державного управління, яка досягається через створення домінантним суб'єктом (держава-агресор, група держав, транснаціональна корпорація, синдикат) необхідних і достатніх умов для підкорення об'єкта (держава-мішень агресії, соціальна група, громадянське суспільство) [13]. До того ж не передбачається завдання встановлення повного і тотального контролю над суверенітетом і територією, іншими важливими, але не життєво необхідними атрибутами, за винятком забезпечення капітуляції збройних сил. Визначальну роль у досягненні мети ГВ відіграють стратегічні комунікації, основним засобом яких виступає інформація, а елементом забезпечення – комплекс силових акцій.

Завдання системи управління в умовах ГВ - зберегти або ж змінити стан об'єкта агресії відповідно до визначеної стратегії ГВ. Як правило, це завдання досягається за допомогою зворотного зв'язку, тобто інформації про стан об'єкта агресії, впливу на нього зовнішнього середовища і результатів гібридних дій (керуючих команд) [14]. Звідси, основною умовою функціонування структур управління, задіяних в ГВ, є рух потоків інформації. Якщо потік за повнотою недостатній для прийняття рішення, інформація неякісна і неактуальна, процеси управління стають неефективними. Отже,

ефективність управління в ГВ визначається якістю інформації, а головним елементом - канали зворотного зв'язку між суб'єктом і об'єктом ГВ, на основі яких здійснюється координація діяльності всіх структур, задіяних у ГВ.

Принцип зворотного зв'язку передбачає в якості необхідного елемента обмін інформацією, тому управління в умовах ГВ - це інформаційний процес зі зворотним зв'язком. З іншого боку, зворотний зв'язок можна розглядати як потенційний канал рефлексивного управління об'єкта агресії суб'єктом. Такі канали мають стратегічне значення. В умовах протидії ГВ цей принцип діятиме безперервно, оскільки відповідні дії об'єкта впливають на динаміку управлінських рішень суб'єкта системи, які приймаються на основі нової інформації, що надходить.

Рефлексивне управління, засноване на теоретичних розробках В. Лефевра [15, 16], обґрунтовує результативне використання комплексних інструментів, що дають змогу впливати на прийняття противником вигідних іншій стороні рішень внаслідок створення певних ситуацій або демонстрації потенційних загроз. За визначенням В. Лефевра, рефлексивне управління - це "процес, у якому один зі супротивників передає іншому підстави для прийняття рішень". Іншими словами, через комунікації зворотного зв'язку відбувається підміна факторів мотивації противника для спонукання його на прийняття не вигідних для себе рішень (рис. 3).

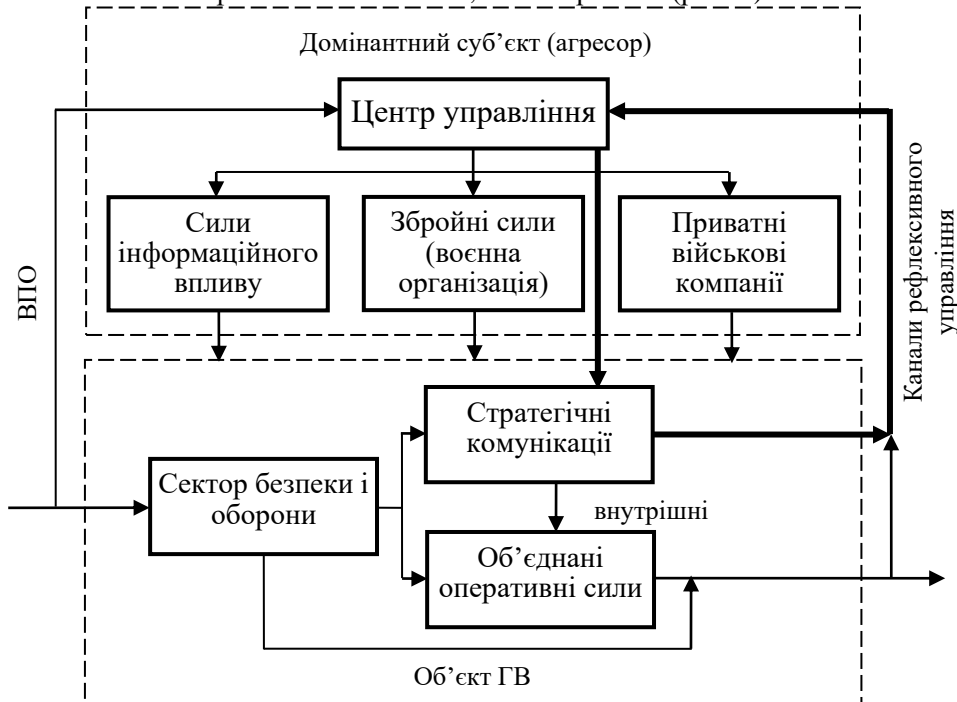


Рис. 3. Застосування рефлексивного управління в стратегічних комунікаціях для протидії загрозам гібридного характеру

Отже, прикладні аспекти рефлексивного управління мають стратегічне значення, є ефективним інструментом ведення ГВ і стратегічних комунікацій, можуть мати істотні переваги над традиційними методами використання воєнних засобів. Застосовуючи стереотипи поведінки, психологічні чинники, персональні відомості про командні кадри (біографічні дані, звички тощо), рефлексивне управління надає можливість збільшити шанси на досягнення перемоги, проте така тактика потребує інформації про супротивника з високим ступенем деталізації і якості, включаючи значні обчислювальні потужності та відповідне програмне забезпечення.

До інструментів рефлексивного управління відносяться дії, спрямовані на точкові інтелектуальні форми і способи збройної боротьби, ніж на традиційні поняття. До них відносяться: камуфляж (на всіх рівнях); дезінформація, провокації, шантаж, компрометації; відволікання уваги; формування щільного інформаційного потоку, обробка якого потребує значних ресурсів; введення в стан когнітивного дисонансу з блокуванням функції прийняття рішень; виснаження ресурсів противника на рішення малозначущих завдань або фейкових загроз; стимулювання протиріч у середовищі союзників; приспання пильності (зниження напруги або перенесення процесів у прихований формат); спонукання до необачних рішень і дій; психологічний тиск і залякування.

Отже, в умовах протидії ГВ стратегічні комунікації необхідно розглядати як діяльність, яка скоординована на стратегічному (воєнно-політичному) рівні управління, і спрямована на управління процесами прийняття рішень як всередині країни (групи країн), так і за її межами, для досягнення перемоги над противником.

Для досягнення цього СК виконують дві основних функції: внутрішню – забезпечують комунікацію із суб'єктами конфлікту; зовнішню – забезпечують комунікацію з навколишнім середовищем.

Зовнішня комунікація забезпечує стійкість системи протидії. Внутрішня комунікація пов'язана з управлінням воєнним конфліктом, забезпечує постійний зв'язок між суб'єктами і об'єктами управління, що і зумовлює значення інформації. Відсутність достовірної інформації призводить до стагнації структури управління. Вона починає працювати інертно, безрезультатно, що призводить до повного розвалу цієї системи.

Отже, найважливішим елементом протидії ГВ є процес комунікації, прямий і зворотний зв'язок всіх об'єктів.

Необхідне рішення противника формується через зміни його сприйняття. *Сприйняття* - це активний процес, який створює, а не фіксує реальність. Приймаючи рішення, противник використовує інформацію про район конфлікту, свої війська і війська противника, про їх бойові можливості. На основі технологій стратегічних комунікацій забезпечується такий вплив на канали отримання інформації, зміст повідомлень, які переведуть рішення, що приймаються, у потрібне русло. Противник використовує найсучасніші методи оптимізації та проводить пошук оптимального рішення. Однак, це буде не дійсно оптимальне рішення, це буде рішення, яке було заздалегідь визначено нами. Для того, щоб прийняти власне ефективне рішення, необхідно знати, як формується рішення противника, яке ґрунтується на інформації, яку він вважає правдивою. СК у цьому процесі забезпечують функціонування національної системи стратегічного, оборонного і оперативного планування та зниження результативності системи оперативного планування противника.

Коли процес прийняття рішень стає мішенню, необхідно забезпечити безпеку власної стратегічної і оперативної функції. Інформаційні, культурні, структурні та нормативні недоліки в процесі прийняття рішень з питань національної безпеки можуть бути найсерйознішою загрозою безпеці країни проти гібридних нападів.

Зважаючи на це, основними завданнями СК в умовах протидії ГВ можливо визначити такі: деморалізація противника, легітимізація своїх дій в очах населення, мобілізація цільових груп населення, підтримування власних політичних еліт. Для вирішення цих завдань, додатково СК здійснюють: моделювання поведінки противника, імітацію його рішень залежно від умов, вибір найефективнішого інформаційного впливу, вибір каналів впливу.

Для результативного використання технологій стратегічних комунікацій і рефлексивного управління в протидії ГВ пропонується проведення комплексу таких заходів:

зосередження зусиль СК на управлінні конфліктом;

визначення відповідального органу з планування і застосування СК;

розроблення плану застосування СК, до якого включити: мету, оцінку спроможностей, часові рамки, цільову аудиторію, канали передачі інформації, методи доведення інформації, структуру і спрямованість повідомлень, порядок організації взаємозв'язку із ЗМІ, асиметричні комунікації, очікувані результати;

забезпечити використання всього спектра електронних комунікацій: електронні ЗМІ (журнали, газети, інформаційні агентства), соціальні мережі (Facebook, Instagram, Twitter та інші), месенджери (Telegram, Viber) блоги, мобільний зв'язок;

розширити діалог між сторонами конфлікту, забезпечивши рівнозначне виробництво і споживання інформації сторонами конфлікту, що дасть змогу краще і швидше вибудовувати і коригувати повідомлення залежно від ситуації, що склалася і настроїв обраної аудиторії, перейти до керування перебігом конфлікту;

врахувати обмеженість традиційних ЗМІ, які засновані на монологічній базі та навіть в електронній формі значно поступаються міжнародним мережевим майданчикам, унаслідок чого цільова аудиторія стає пасивним споживачем інформації, що знижує ступінь довіри до СК;

вжити заходи протидії перехопленню і обробки інформації противником для її подальшої негативної зміни та поширення в соціальних мережах і на традиційних ЗМІ;

як частину СК запровадити постійний моніторинг нових засобів масової інформації;

розробити і впровадити автоматизовану систему моніторингу нових засобів масової інформації, соціальних мереж, інших повідомлень та оперативного збору потрібної інформації;

врахувати неможливість забезпечення повного контролю над доведенням інформації до цільової аудиторії при застосуванні нових засобів масової інформації;

вплив на прийняття рішення і процес управління противником розпочати з інформаційно-маніпулятивних підмін наративів: спочатку приховано, непомітно для свідомості цільової аудиторії, коли підміна розкриється, нові наративи вже будуть міцно закріплені, а повернення до старих вже практично неможливо;

забезпечити синхронізацію і структурування всіх вихідних інформаційних процесів СК, виключити відмінності в критеріях оцінки фактів;

поширити вплив технологій СК не тільки на суто військовослужбовців і інших комбатантів, а й цивільне населення району конфлікту, цивільно-військові відносини;

зайняти відповідне місце у процесі розроблення стратегії національної безпеки, як механізм забезпечення взаємозв'язку між метою та діями під час її реалізації;

сформувати національну концепцію протидії гібридній війні, розуміння і сприйняття її цільовими аудиторіями;

розробити єдиний універсальний підхід до роботи СК в умовах гібридної війни, для чого можливо застосування правил бізнес-індустрії, маркетингу.

**Висновки.** Масштабність загроз в інформаційній сфері дає змогу доповнити існуючі види стратегічного стримування (ядерного, сил загального призначення, кібернетичного) ще і стратегічним стримуванням за допомогою використання технологій СК – великомасштабного спеціального впливу на об'єкти інформаційного ресурсу і управління ймовірного противника.

Використання технологій СК на театрі інформаційного протиборства є важливим ресурсом гібридної війни. Результативність стратегічних комунікацій визначить можливість досягнення перемоги в ГВ.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Hoffman F.G. Hybrid Warfare and Challenges. Joint Force Quarterly, 2009. 1<sup>st</sup> Quarter-No52. p. 34–39.
2. Mattis J. Call Sign Chaos: Learning to Lead. Washington, RHP Group, 2019. 320 p.
3. Калдор М. Новые и старые войны: организованное насилие в глобальную эпоху / пер. с англ. А. Апполонова, М. Дондуковского ; ред. перевода А. Смирнов, В. Софронов. М. Институт Гайдара, 2015. 416 с.
4. Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України : наказ МОУ № 612 від 22.11.2017.
5. Почепцов Г. (Дез)інформація / под общ. ред. Н. Лигачевой. К. : Паливода А.В., 2019. 248 с.
6. Вербицька А. М., Савченко В. А., Дзюба Т. М., Кацалап В. О. Система стратегічних комунікацій Міністерства оборони України та Збройних Сил України. *Наука і оборона*. 2017. № 1. С. 34–39.
7. Сальнікова О. Ф., Міщенко В. Б., Шидлюх В. В., Антоненко С. І. Використання технологій стратегічних комунікацій в системі управління Збройними Силами України. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2017. № 3 (30). с. 61–66.
8. Гребенюк М. В. Основи стратегічних комунікацій за стандартами НАТО : навч. посіб. К. : НУОУ ім. Івана Черняхівського, 2017. 180 с.

9. 2015 National Military Strategy of The United States of America. URL: <https://dod.defense.gov/Portals/1/Documents/pubs/2015-National-Military-Strategy-Summary.pdf>.
10. Кокошин А. А. Вопросы прикладной теории войны. М.: Изд. дом Высшей школы экономики, 2018. 227 с.
11. Sinclair N. Old Generation Warfare: The Evolution – Not Revolution – of the Russian Way of Warfare. *Military Review*—2016, May-June, p. 8–15.
12. Gorka S. How America Will be Attacked. Irregular Warfare, the Islamic State, Russia, and China. *Military Review*. 2016, September-October. p. 30.
13. Сальнікова О. Ф., Сивоха І. М., Іващенко А. М. Стратегічні комунікації в сучасних війнах гібридного типу. *Social Development & Security*, 2019. Vol. 9. No.5. С. 133–142.
14. Іващенко А. М. Еволюція поглядів на стратегію сучасного гібридного конфлікту та сценарії протидії гібридним загрозам. *Зб. наукових праць ЦВСД НУОУ*. 2015. № 1(53). с. 18-23.
15. Lefebvre V. Algebra of Conscience: A Comparative Analysis of Western and Soviet Ethical Systems. Dordrecht, Holland, D. Reidel Publishing, 1982. 220 p.
16. Lefebvre V. Lectures on the Reflexive Games Theory Paperback. September 2, 2010.

Стаття надійшла до редакційної колегії 05.11.2019

**Сальнікова О. Ф., д-р наук по госуд. упр., ст. научн. сотрудник<sup>1</sup>;**  
**Іващенко А. М. канд. техн. наук, доцент<sup>2</sup>;**  
**Сивоха І. М.<sup>1</sup>**

<sup>1</sup> – Учебно-научный центр стратегических коммуникаций в сфере обеспечения национальной безопасности и обороны Национального университета обороны Украины имени Ивана Черняховського, Киев;

<sup>2</sup> – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Киев

### **Использование рефлексивного управления в стратегических коммуникациях для противодействия угрозам гибридного характера**

**Резюме:** В современном мире сочетание пропаганды, дезинформации, психологического давления, атак на информационные и коммуникационные системы представляют опасность не меньшую, чем традиционные системы вооружений. Результативные сценарии противодействия гибридным угрозам основываются на использовании современных технологий стратегических коммуникаций, управлении субъектами военных конфликтов, обработке информации.

Целью данной статьи является анализ основных концепций современных войн гибридного типа и определения, цели, задач и особенностей стратегических коммуникаций.

Для разработки сценариев противодействия гибридной войне предлагается интегрированное использование технологий стратегических коммуникаций и рефлексивного управления.

**Ключевые слова:** современные войны гибридного типа; стратегические коммуникации; информационные технологии; рефлексивное управление.

**O. Salnikova, Doctor of public administration, senior researcher<sup>1</sup>;**  
**A. Ivashchenko, PhD (Technica), associate professor<sup>2</sup>;**  
**I. Sivokha<sup>1</sup>**

<sup>1</sup> – Education and Research Centre for Strategic Communications in sphere of the National Security and Defense of the National Defence University of Ukraine named after Ivan Cherniakhovskiyi, Kyiv;

<sup>2</sup> – Center for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskiyi, Kyiv

### **The use of reflexive control in the strategic communications as a way to counter hybrid threats**

**Resume.** In today's world, the combination of propaganda, disinformation, psychological pressure, and attacks on information and communication systems pose a danger no less than conventional armament. Productive scenarios for counteracting hybrid threats are based on the use of modern technologies of strategic communications, management of subjects of military conflicts, and information processing.

This article is aimed at analyzing the basic concepts of modern hybrid warfare and finding place, purpose, objectives, and features of strategic communications.

An integrated use of strategic communications and reflexive control technologies is proposed to develop hybrid warfare scenarios.

**Keywords:** modern hybrid warfare; strategic communications; information technologies; reflexive management.