ISSN 3041-1238 № 1 (2) 2024

DOI: https://doi.org/10.26642/sas-2024-1(2)-119-123
УДК 253:351.86:323

Вітер Д.В.
д.філос.н., с.н.с., головний науковий співробітник Центру воєнно-наукових досліджень Національного університету оборони України

Руденко О.М.
д.держ.упр., проф. Національного університету «Чернігівська політехніка»

Руденко О.О.
аспірант Державний університет «Житомирська політехніка»

Інформаційно-комунікативна складова мережевої протидії загрозам національній безпеці у воєнній сфері

Анотація. У статті концептуалізовано шляхи формування стратегічних орієнтирів забезпечення національної безпеки у сфері протидії інформаційно-психологічним загрозам. Розглянуто елементи стратегії національної безпеки, які є потенційно визначними з огляду на розвиток активних форм інформаційних операцій з боку противника у сучасному конфлікті, у тому числі воєнному. Зроблено акцент на застосування підрозділів сил спеціальних операцій у сфері мережевої протидії загрозам національної безпеки у воєнній сфері. Урахування цього потребує вироблення та впровадження конкретних механізмів державного управління у сфері забезпечення національної безпеки, які спрямовані на протидію інформаційно-психологічних загрозам. Зокрема, йдеться про необхідність адекватного представлення цього питання у стратегії національної безпеки шляхом визначення особливості мережевої протидії загрозам національної безпеки у воєнній сфері. Зокрема, йдеться про розвиток застосування нових способів дистанційного впливу на противника, тобто, розширення простору ведення бойових дій та середовищ війни, розвиток нових форм оборони та оборонних заходів, зростання значення розвідувально-диверсійних дій в тилу противника, інтелектуалізація війн, зорієнтованих на переважне використання високоточної та роботизованої зброї. Підкреслено необхідність удосконалення механізмів державного управління стратегічно важливими сферами інформаційного середовища на основі інформаційно-комунікативних компонентів мережевої протидії загрозам національної безпеки у воєнній сфері. Підкреслюється, що інформаційні заходи є невід'ємною частиною державного реагування на загрози національній безпеці та однією з основних складових інформаційної війни, спрямованої на досягнення перемоги в інформаційному просторі.

Ключові слова: воєнна безпека; інтернет; інформаційно-психологічна операція; інформаційно-комунікативна політика; національна безпека.

Вступ. Інформаційно-комунікативні заходи стали невід'ємною частиною політики держави у сфері забезпечення національної та воєнної безпеки, одною з основних складових інформаційної війни, спрямованої на досягнення перемоги не лише на полі бою, але й в інформаційному просторі. У цьому сенсі на передній план війні вийшли інформаційні операції з метою завоювання інформаційної переваги в районі ведення бойових дій та на ТВД.

Повномасштабна агресія рф проти України не обходиться без інформаційно-психологічних атак з боку російських збройних сил та спеціальних служб, які їх підтримують, а центри інформаційно-психологічних операцій (ІПСО) – це саме той військовий елемент, який може забезпечувати ефективне протистояння противнику не лише в інформаційній боротьбі. Сьогоднішня дійсність України наочно підтвердила, що майже всі дипломатичні, економічні, військові, політичні та інші кроки держави здійснюються у тісному інформаційному супроводі. Сила сучасної держави залежить не лише від її економічного та політичного потенціалу, але й від власної системи інформаційної безпеки [3], яка набуває особливого значення у сфері забезпечення національної безпеки та протидії загрозам національній безпеці у воєнній сфері.

Виклад основного матеріалу. У 2012 р. у США було введено новий термін – «військові операції інформаційної підтримки» (Military Information Support and/to Operations – MISO), який мав забезпечити перегляд загальної політики державної пропаганди. Очікувалося, що зміни стосуватимуться й військової сфери, проте на сьогодні в армії США тактика дій сил психологічних операцій залишилася майже без змін. Водночас у Китаї класика психологічної війни поступово входить у площину інтернет-війн. Якщо провести порівняльну характеристику частки інтернет-сегменту інформаційно-психологічних операцій, то у рф він наближається до 15 %, тоді як у Китаї можна говорити майже про 50 %. Фактично Китай не збирається залишати традиційні методи психологічної війни – друковану, усну, телевізійну та

радіопропаганду. Очевидним є доволі консервативне ставлення до дотримання головного політичного вектору держави – так званої політики «м'якої сили» щодо інших країн. При цьому інтернет, як основа інформаційних систем командування, контролю, каналів зв'язку, комп'ютерів, спостереження та розвідки (наприклад, американська C4ISR), що забезпечує створення певного єдиного інформаційного простору на полі бою, залишається одним з головних елементів інформаційно-комунікативної системи управління не лише різними засобами ведення війни, але й ведення боротьби нового покоління. Так, обидві сторони спеціальної військової операції в Україні активно використовують Інтернет для управління військами та докладають великих зусиль, щоб зберегти його задля успішного ведення війни в інформаційному просторі. Наприклад, щоб зменшити втрати ЗС та збільшити потік інформації про порушення ворогом умов ведення війни через інформаційно-комунікативну систему проводиться компанія «віктимізації за довіреністю» (формування макровіктимного мислення) шляхом поширенням фейків і посиленою пропагандистською кампанією всередині країн ЄС та США, спрямованою на протидію рф. У даному випадку вибірковість у підборі інформації та атаках на свідомість людей – обов'язковий механізм віктимізації.

Найвідчутніший результат у ході проведення спеціальної військової операції мала зміна інформаційної політики держави у сфері оборони. Якщо в перші дні спостерігався спокійний, більш оборонний підхід Міністерства оборони України, то сьогодні інформаційна війна стала потужнішою ніж самі бойові дії. Потрібно віддати належне українським спецпропагандистам та створеному центру інформаційної спеціальної пропаганди та кіберзахисту при Міністерстві оборони України у взаємодії з спеціальним підрозділом Служби безпеки України. Інформаційне забезпечення дій українських військ здійснюється на дуже високому рівні. Масштабний потік дезінформації, в якому трапляються рідкісні вкраплення правди – обов'язкова умова при таких операціях – створює відчуття, що Україна не лише героїчно стримує натиск російських військ, але й ось-ось розгромить противника. Розрахунок робився на якісну перевагу частин збройних сил рф над їхніми українськими опонентами в мобільності, бойовій підготовці, а також сучасному озброєнні та військовій техніці. Натомість треба розуміти, що російське військово-політичне керівництво позиціонувало операцію проти України як боротьбу з київським режимом, а не з українським народом [2].

В інформаційному просторі з'явилася та поширювалося колосальна кількість спеціально складених або випадково виникаючих фейків, що спотворюють реальну інформацію про події. Українська сторона швидше ніж російська розпочала активну роботу в інформаційному полі, тому за час першого місяця війни, російська федерація визнала поразку в інформаційній війні. Переважну частину контенту про події, що відбуваються в Україні, генерує в потрібному для себе ключі українська сторона, і їй активно допомагають закордонні партнери. Можливо, тому що поточний конфлікт багато в чому виглядає як «братовбивчий конфлікт», російське керівництво намагається мінімізувати дані не лише про втрати російської сторони, а й взагалі про дії угруповання збройних сил рф в Україні. Єдине офіційне зображення, яке бачить населення – це інформація з так званих народних республік Донецької і Луганських областей.

РФ продовжувала підготовку до наступальних дій, довівши на початок лютого 2022 р. угруповання сил і засобів до остаточної стадії готовності під прикриттям проведення широкомасштабних стратегічних російсько-білоруських навчань. У цей же період проводилася програма відволікання опонентів шляхом активного мусування теми гарантій зі стратегічної безпеки в Європі у засобах масової інформації та за дипломатичними каналами, що значною мірою було димовою завісою для завершення підготовки операції проти України, яка виразилася у тривалому запереченні на всіх рівнях факту розгортання угрупування для удару по Україні.

Активна інформаційна складова, постійний рух військ з одного краю країни в інший, робота дипломатичних співробітників на всіх майданчиках з питань приховування військової готовності до дій – таки дії росії були виправдані з раціональної військової точки зору. Водночас, з початком повномасштабних військових дій багатьма шарами населення рф було сприйнята як помилкою та небажаними діями керівництва держави. Щоб зменшити соціальну напругу та змінити відношення населення на початок і хід проведення спеціальної операції, керівництвом росії було вжито заходів з активізації публікуванню матеріалів, що дискредитують та дегуманізують «київський режим» (проголошені цілі спеціальної операції – денацифікація, демілітаризація та декомунізація) [2, с. 25].

У цілому в умовах спеціальної військової операції рф на території України до ведення інформаційної війни та проведення інформаційно-психологічних операцій залучено спеціальні підрозділи збройних сил росії, до складу яких входять групи спеціальних журналістів (8–10 окремих груп), які працюють безпосередньо на російські інформаційні канали. До їх складу входять 3–4 особи – журналіст, оператор, водій (може доповнюватися охоронцем); оперативні групи психологічних операцій (4 групи ПсО) – мобільні підрозділи загону ПсО у складі 2–4 осіб. На території окупованих районів вони виконують завдання з:

- усної пропаганди, у тому числі й роботі з місцевим населенням;
- поширення пропагандистської літератури та іншої необхідної інформації;
- створення пропагандистських груп у населених пунктах, що складаються з місцевих активістів, їх організації та координації дій;
- надання сприяння роботі російських журналістів;

– збору інформації та визначення найбільш гострих проблем у населення для використання цього надалі, як інформаційного приводу;

– моніторингу поточного морально-психологічного стану місцевого населення.

Загін психологічних операцій дислокується на російській стороні кордону, неподалік Ростова-на-Дону, разом із пунктом управління розвідцентру Головного розвідувального управління генерального штабу збройних сил рф. Загін ПсО здійснює основну керівну роль в інформаційно-психологічних заходах на території України. Його завданнями є:

– збирання, обробка та аналіз інформації про поточний морально-психологічний стан населення України та підрозділів російських збройних сил (зона інтересів загону ПсО поширюється на всю територію України);

– керівництво підрозділами ПсО, що виконують спеціальні завдання з інформаційного впливу;

– розробка та здійснення інформаційно-психологічних операцій на території України.

Також активно використовуються агенти диверсійної психологічної роботи в інших областях України – фахівці від Головного розвідувального управління генерального штабу збройних сил або Федеральної служби безпеки рф, які виконують завдання з:

– створення диверсійно-пропагандистських груп в інших областях України серед місцевого авторитетного населення;

– навчання місцевих груп проведенню підривних пропагандистських акцій;

– забезпечення окремих груп необхідним матеріально-технічним майном;

– безпосереднього проведення мітингів, акцій протесту та поширення пропагандистських матеріалів.

Для протидії інформаційно-психологічним операціям противника (як реального, так і потенціального) використовуються підрозділи сил спеціальних операцій (ССО) шляхом розроблення спеціальних операцій (СО), які спрямовані на мінімізацію негативного інформаційно-психологічного впливу противника. Це здійснюється в єдиному комплексі сучасних способів інформаційної боротьби, серед яких одне з провідних місць посідає мережева протидія у всіх актуальних і потенційних сферах. Водночас забезпечення комплексного підходу до планування і застосування у багатосферних операціях ССО здійснюється з урахуванням їх ролі та місця у нетрадиційних війнах, які ведуться з метою дестабілізації внутрішньої ситуації в державі шляхом встановлення контролю над урядами, органами державного управління та населенням в окремих регіонах держави, передбачають проведення СО із залученням опозиційних рухів, терористичних і кримінальних організацій. Як правило, йдеться про СО, спрямовані на дестабілізаційну, підривну діяльність, розвідку, інформаційну війну, а також застосування прямих ударів (дій) для забезпечення традиційних військ (сил), зменшення оперативної стійкості противника, здійснення впливу і контролю місцевості та населення держави. В останньому випадку йдеться про досяжність геополітичних цілей держави шляхом використання потенціалу ССО з вирішення завдань щодо деструктивного впливу на суспільні та індивідуальні погляди, ціннісні орієнтації особистості та суспільства, дезорієнтації населення і дезорганізації процесу суспільно-політичного розвитку на території держав-противників.

Якісні зміни цілей, на досягнення яких орієнтуються ССО, потребує суттєвих трансформацій з традиційних на нетрадиційні форми і способи ведення війн, оскільки виклики та загрози у стратегічному і оперативному середовищі динамічно змінюються, надаючи пріоритетного значення новим методам впливу на противника. Зокрема, більш актуальними виявляються інформаційні та когнітивні методи, які у свою чергу визначають необхідність переорієнтації сил і засобів ССО на досягнення інформаційних і когнітивних цілей, які, на відміну від традиційних підходів, не мають чітких характеристик фізичного середовища. Саме формування системи нетрадиційних цілей здійснює безпосередній вплив на концептуальне обґрунтування застосування ССО у багатосферних операціях.

У цілому можна прослідкувати, що відбуваються й зміни у традиційних підходах до застосування ССО, які спрямовані на виявлення нових характерних особливостей СО та спеціальних заходів. Зокрема, йдеться про розвиток застосування нових способів дистанційного впливу на противника, тобто, розширення простору ведення бойових дій та середовищ війни, розвиток нових форм оборони та оборонних заходів, зростання значення розвідувально-диверсійних дій в тилу противника (особливо з урахуванням зростання глибини ешелонування угруповань військ (сил), інтелектуалізація війн, зорієнтованих на переважне використання високоточної та роботизованої зброї. Проблемним питанням наведеного підходу виявляється реалізація компенсаторної функції, яка покладається на ССО під час проведення загальновійськових та спеціальних операцій міжвидовими угрупованнями військ (сил) у ситуації обмеженого ресурсного забезпечення, що знижує можливості реагування на кризові ситуації. Зазвичай приймається положення про те, що ССО мають компенсувати нестачу ресурсів за рахунок залучення підрозділів союзників, партнерів, іррегулярних військових формувань країни, на території якої проводиться СО, підконтрольних лояльному уряду. Проте, за певних ситуацій, пов'язаних з інтенсивним зростанням ризиків, ефективна реалізація компенсаторної функції унеможливлюється, тому потребує уваги система планування СО і спільного застосування військ (сил) та ССО у визначеній операційній зоні у межах модернізації системи всебічного забезпечення, досягнення високого рівня оперативної сумісності

ССО з іншими підрозділами військ (сил), багатонаціональними формуваннями, державними і недержавними організаціями різного рівня, у тому числі й міжурядовими.

Наведений підхід має забезпечити протидію комплексу загроз інформаційній безпеці України, що передбачає [1]:

1. Державна політика у сфері інформаційної безпеки здійснюється з метою недопущення перешкоджання реалізації життєво-важливих інтересів і потреб громадянина, суспільства і держави зовнішніми і внутрішніми загрозами національній безпеці в інформаційній сфері.

2. Загрозами національній безпеці України в інформаційній сфері є: загрози комунікативного характеру в сфері реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, розповсюдження та розвитку національного стратегічного контенту та інформації; загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору.

3. Загрози комунікативного характеру, що включають:

а) зовнішні негативні інформаційні впливи на свідомість людини та спільноти через засоби масової інформації, а також мережу Інтернет з метою зміни психічного та емоційного стану людини, її психологічних і фізіологічних характеристик; здійснення керованого впливу на свободу вибору; поширення закликів до сепаратизму, повалення конституційного ладу чи порушення територіальної цілісності держави;

б) інформаційний вплив на населення України, у тому числі на особовий склад військових формувань, мобілізаційний резерв, з метою послаблення їх готовності до оборони держави;

в) поширення суб'єктами інформаційної діяльності інформації, яка дискредитує органи державної влади, дестабілізує суспільно-політичну ситуацію тощо.

4. Загрози технологічного характеру в сфері функціонування та захищеності кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору включають:

а) використання іноземними державами кібервійськ, кіберпідрозділів, нових видів інформаційної зброї та зброї кібернетичного характеру на шкоду Україні;

б) прояви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем, шляхом втручання, несанкціонованого доступу або порушення функціонування телекомунікаційних, кібернетичних, автоматизованих комп'ютерних систем, незалежно від форми власності, з метою: вчинення диверсій чи терористичних актів; здійснення підтримки, супроводження чи активізації злочинної, екстремістської чи терористичної діяльності; здійснення з їх допомогою деструктивного інформаційного впливу; перехоплення інформації в телекомунікаційних мережах; створення радіоелектронних перешкод чи блокування інформаційних систем, засобів зв'язку та управління, реалізація програмно-математичних засобів, що порушують функціонування інформаційних систем; включення у програмно-технічні засоби прихованих шкідливих функцій тощо.

Урахування цього потребує вироблення та впровадження конкретних механізмів державного управління у сфері забезпечення національної безпеки, які спрямовані на протидію інформаційно-психологічних загроз. Зокрема, йдеться про необхідність адекватного представлення цього питання у стратегії національної безпеки шляхом визначення особливості мережевої протидії загрозам національної безпеки у воєнній сфері. До таких особливостей належить важливість розроблення моделі оперативної діяльності ССО як в зонах конфліктів, так і за їх межами, з пріоритетною орієнтацією на протидію мережевим загрозам, інформаційна складова яких використовується терористичними, повстанськими та ворожими державними інформаційними мережами, що являють собою загрозу національним інтересам держави [5, с. 129–130]. У цьому аспекті контрольовані державою інформаційні потоки, перш за все, мережеві, здатні перетворюватися на механізми протидії загрозам національній безпеці шляхом формування єдиної системи соціальних рухів та об'єднання нових інформаційних мереж з метою формування у населення країни стійкої мережевої орієнтації з урахуванням конкретних ментальних програм.

Досвід свідчить, що основними тенденціями розвитку форм і способів застосування підрозділів ССО під час планування та проведення сучасних спеціальних операцій (зокрема, небойові операції), є [4]:

– інформаційно-психологічний вплив на населення та збройні сили країни-агресора та регіону, де будуть проводитися заходи;

– охоплення в межах проведення інформаційно-психологічної підготовки району виконання завдань спеціальної операції всіх верств населення за етнічним, національним, мовним, культурним, релігійним складом із залучення інформаційно-пропагандистських матеріалів, орієнтованих на конкретну групу населення поряд із використання в інформаційно-пропагандистських цілях релігійних діячів, а також створення умов для доступу населення та особового складу Збройних Сил до інформаційних джерел (у тому числі, забезпечення технічними засобами отримання інформації, вільного доступу до мережі Інтернет тощо) тощо. З огляду на вказане вище, актуальними виявляються інформаційні та когнітивні

методи, які у свою чергу визначають необхідність переорієнтації сил і засобів ССО на досягнення інформаційних і когнітивних цілей, які, на відміну від традиційних підходів, не мають чітких характеристик фізичного середовища.

У цьому аспекті Сили спеціальних операцій виявляють потужний потенціал стримування та відтягування значних сил противника від виконання основних завдань. Стратегія стримування здебільшого інтегрована в Воєнну стратегію України, яка містить у собі всі елементи національної влади: дипломатичну, інформаційну, військову та економічну, спрямована на організацію всебічного національного опору агресору. І якщо військовий компонент цієї стратегії передбачає операції стримування на окупованих територіях, які мають працювати разом з веденням основних бойових дій щодо звільнення окупованої території, то інформаційний компонент поки ще потребує активного розвитку та урахування в якості одного з визначальних факторів у сучасних конфліктах.

Висновки та перспективи подальших досліджень. Інформаційні заходи є невід'ємною частиною державного реагування на загрози національній безпеці та однією з основних складових інформаційної війни, спрямованої на досягнення перемоги в інформаційному просторі. На передній план у цій війні вийшли російські інформаційні операції з метою завоювання інформаційної переваги в Україні, що актуалізує завдання вироблення та імплементації конкретних механізмів державного управління у сфері забезпечення національної безпеки. Роль інтернету в підтримці та забезпеченні цієї боротьби на сьогодні виявилася дуже великою, і, ймовірно, цей факт вплине на розвиток інформаційних мереж.

Список використаної літератури:

1. Концепція інформаційної безпеки України (проект) [Електронний ресурс]. – Режим доступу : https://www.osce.org/files/f/documents/0/2/175056.pdf.
2. Стратегічне управління та державне реагування на загрози національній безпеці у сфері безпеки державного кордону : монографія / *Д.Вітер та ін.* ; Нац. ун-т оборони України ім. Івана Черняховського, Центр воєнно-стратег. дослідж. – Київ : Видання Університету, 2021. – 232 с
3. *Цевельов О.* Російсько-Українська війна: холодна весна 2022 : монографія / *О.Цевельов, Д.Вітер.* – К. : НУОУ, 2022. – 104 с.
4. Psychological Operations and Political Warfare in Long-Term Strategic Planning / *J.Radvani* (ed.). – New York : Praeger, 1990.
5. The Network Illusion: How a Network-Centric Special Operations Culture Impedes Strategic Effect / Ed. by *P.McCabe* ; Foreword by *M.Nagata*. – JSOU Press MacDill Air Force Base, Florida, 2022. – 164 p.

References:

1. «Kontseptsiia informatsiinoi bezpeky Ukrainy (proekt)», [Online], available at: https://www.osce.org/files/f/documents/0/2/175056.pdf
2. Viter, D. et al. (2021), *Stratehichne upravlinnia ta derzhavne reahuvannia na zahrozy natsionalnii bezpetsi u sferi bezpeky derzhavnoho kordonu*, Nats. un-t oborony Ukrainy im. Ivana Cherniakhovskoho, Tsentr voienno-strateh. Doslidzh, Vydannia Universytetu, Kyiv, 232 p.
3. Tsevelov, O. and Viter, D. (2022), *Rosiisko-Ukrainska viina: kholodna vesna 2022*, monohrafiia, NUOU, K., 104 p.
4. Radvani, J. (ed.) (1990), *Psychological Operations and Political Warfare in Long-Term Strategic Planning*, Praeger, New York.
5. McCabe, P. (ed.) (2022), *The Network Illusion: How a Network-Centric Special Operations Culture Impedes Strategic Effect*, Foreword by Nagata, M., JSOU Press MacDill Air Force Base, Florida, 164 p.

Viter D.V., Rudenko O.M., Rudenko O.O.

Information and communication component of the network countermeasure to national security in the military sphere

Abstract. The article conceptualizes ways of forming strategic guidelines for ensuring national security in the field of countering informational and psychological threats. The elements of the national security strategy, which are potentially significant in view of the development of active forms of information operations on the part of the enemy in the modern conflict, including military ones, are considered. Emphasis is placed on the use of special operations forces units in the field of network countermeasures against threats to national security in the military sphere. Taking this into account requires the development and implementation of the public administration specific mechanisms in the field of the national security ensuring, which are aimed at countering informational and psychological threats. In particular, it is about the need to adequately represent this issue in the national security strategy by defining the specifics of network countermeasures against threats to national security in the military sphere. In particular, it is about the development of the use of new methods of remote influence on the enemy, i.e., the expansion of the space for conducting combat operations and the environments of war, the development of new forms of defense and defensive measures, the growing importance of reconnaissance and sabotage actions in the rear of the enemy, the intellectualization of wars focused on the predominant use of high-precision and robotic weapons. This causes additional tasks to creative use of open source information as well as document analysis from documents like the National Security Strategy, National Military Strategy, taking into account that the main task in the field of military security is the development of deterrence potential, combat-ready armed forces and other components of the defense forces, capable of performing complex tasks in a multidimensional space, development of the components of the defense forces and solving the problems of ensuring the defense of the state. Information measures are an integral part of the state response to threats to national security and one of the main components of the information war aimed at achieving victory in the information space.

Keywords: military security; Internet; information and psychological operation; information and communication policy; national security.

Стаття надійшла до редакції 05.02.2024.