UDC 341.123 (045) DOI: 10.17721/2415–881x.2019.83.16-25

Sergiy Zaporozhets

PhD in Political science, Natsionalnyi Universytet Oborony Ukrainy imeni Ivana Chernyakhovskoho (Kiev, Ukraine)
https://orcid.org/0000–0002–5080–4942
e-mail: zaporozhets_serg@ukr. net

THE STATE OF PROVIDING INFORMATION SECURITY OF UKRAINE IN THE MILITARY SPHERE IN A HYBRID WAR

Abstract

The article is devoted to the study of the state of information security of Ukraine in the military sphere in the context of hybrid warfare, analysis of the role and place of information security of the state and the military sphere in conditions of hybrid warfare. The list of the main threats to the information security of the state in the military sphere is established. The recommendations for neutralization of hybrid threats and the organization of counteraction in solving the hybrid war against Ukraine are given: conducting a systematic analysis of the use of the means, forms and methods of information fighting in the military sphere, determining the directions of ensuring information security of the state in this sphere; improvement of legislation on coordination of activities of public authorities and bodies of military administration in solving problems of providing information security; improving the types and means of protection of information in the information and telecommunication networks involved in the management of troops and weapons from unauthorized access; improving the forms and methods of counteracting information and psychological operations aimed at weakening the state's defense capability; training of specialists in the field of information security in the military sphere.

Establishment of the system of providing information security of the state in the military sphere in the conditions of hybrid war should be carried out in accordance with the following basic principles: high degree of integration of the information system of the Armed Forces of Ukraine into the information security system of the state; the preventive-defensive nature of the activities of information-fighting structures aimed at counteracting the challenges, dangers and threats to the national security of the state in the military sphere in any form of their manifestation; a clear division of information security responsibilities between the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukrain.

It is revealed that one of the main tendencies in the development of the military-political situation in the world is the acceleration of the development of information technologies, increasing the capabilities of states to conduct information-psychological operations and operations in cyberspace, increasing the sensitivity of society to the death of civilians and the loss of military personnel in military configurations.

Key words: information security; hybrid war; military sphere; national security of the state; information threats

УДК 341.123 (045) DOI: 10.17721/2415–881x.2019.83.16-25

Запорожець Сергій Анатолійович

Кандидат політичних наук, Національний університет оборони України імені Івана Черняховського (м. Київ, Україна)
https://orcid.org/0000–0002–5080–4942
e-mail: zaporozhets_serg@ukr.net

СТАН ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ У ВОЄННІЙ СФЕРІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Резюме

Стаття присвячена дослідженню стану забезпеченню інформаційної безпеки України у воєнній сфері в умовах гібридної війни, аналізу ролі та місця інформаційної безпеки держави та воєнної сфери в умовах гібридної війни. Актуальність теми даної наукової роботи полягає в тому, що наразі Україна перебуває у воєнному конфлікті з Росією, і виходячи з сучасних реалій активізується в цьому міждержавному протиборстві і невійськові заходи, зокрема політичні, економічні, інформаційні. В таких умовах стрімко зростає рівень та значно розширюється спектр інформаційних загроз в національній, міжнародній та воєнній безпеці. Методологічну основу представленої статті складають перш за все такі загальнонаукові принципи як об'єктивність, системність та міждисциплінарність. Реалізація дослідницької мети, яка була зазначена вище у цьому дослідженні, передбачала також застосування комплексу таких методів як порівняння, узагальнення, а також проблемного підходу. Як результат, було встановлено перелік основних загроз інформаційній безпеці держави у воєнній сфері і надано рекомендації щодо нейтралізації гібридних загроз і організації протидії при розв'язанні гібридної війни проти України.

Ключові слова: інформаційна безпека; гібридна війна; воєнна сфера; національна безпека держави; інформаційні загрози

Вступ

На даний час визначальним впливом на розвиток військово-політичної обстановки в світі є прагнення Російської Федерації не допустити втрати глобального лідерства, зберегти однополярний світ будь-якими засобами, включаючи військовим. Далеко не всі цивілізовані держави беззастережно сприймають спроби нав'язати всьому світу диктат окремої агресивної держави, що призводить до різкої активізації міждержавного протиборства, основу якого складають невійськові заходи: політичні, економічні, інформаційні. В таких умовах стрімко зростає рівень та значно розширюється спектр інформаційних загроз в національній, міжнародній та воєнній безпеці. Особлива небезпека цих загроз полягає в можливості призвести до катастрофічних наслідків у плані воєнної та національної безпеки держави, що може спричинити втрату суверенності країни.

У цих умовах увагу сучасних дослідників все частіше привертає феномен гібридної війни як прихованого конфлікту, що володіє складною внутрішньою структурою і протікає у вигляді інтегрованого військово-політичного, фінансово-економічного, інформаційного і соціально-культурного протистояння, що не має певного статусу. Сутність гібридної війни, як і будь-якої

іншої війни, полягає в перерозподілі ролей суб'єктів політичного процесу на глобальному або регіональному рівні. Однак здійснюється воно переважно невійськовими засобами, без окупації поваленої країни, руйнування її інфраструктури та масової загибелі населення. Інформаційно-комунікаційні технології дозволяють домогтися переведення країни під зовнішнє управління при мінімальному рівні військового насильства, за рахунок концентрованого тиску в фінансово-економічних, інформаційно-психологічних сферах з використанням кіберзброї.

Розгляду питань забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни присвячені роботи вітчизняних вчених: М. Биченка, В. Горбуліна, Д. Дубова, Я. Жаркова, О. Литвененка, О. Левченка, Ю. Міхєєва, М. Ожевана, А. Рось, В. Шамаєва та інших. Проте зазначені дослідження та наукові праці містять лише фрагментарні наукові розробки у забезпеченні інформаційної безпеки України у воєнній сфері в умовах гібридної війни. Проблема обґрунтування стану забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни залишається мало дослідженою.

Мета статті — визначення необхідних інформаційних загроз та врахування їх під час забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни.

Методи дослідження

Методологічну основу представленої статті складають перш за все такі загальнонаукові принципи як об'єктивність, системність та міждисциплінарність. Реалізація дослідницької мети, яка була зазначена вище у цьому дослідженні, передбачала також застосування комплексу таких методів як порівняння, узагальнення, а також проблемного підходу.

Результати

Розвиток української держави в останні п'ять років пов'язаний з переосмисленням ролі інформаційної безпеки держави, пошуком і визначенням напрямків та механізмів захисту інформаційного простору. Захист інформаційного простору повинний стати одним із значущих завдань модернізації української державності, який зумовлює багато в чому зміст і динаміку внутрішньополітичних процесів в українському суспільстві, специфіку самоідентифікації України, що трансформується в світовому співтоваристві.

У загальному вигляді під загрозами інформаційній безпеці України у воєнній сфері мається на увазі сукупність дій іноземних держав (їх спілок), міжнародних терористичних організацій і кримінальних структур (угруповань), що створюють небезпеку порушень суверенітету, територіальної цілісності, зміни конституційного ладу, перешкоджають реалізації національних інтересів, сприяють розмиванню національних цінностей і руйнуванню основних підвалин способу життя, здійснюють негативний інформаційний та інформаційно-психологічний вплив та підривають рівень обороноздатності країни.

На даний час проблема забезпечення інформаційної безпеки України у воєнній сфері стоїть ще гостріше, оскільки значно зросла роль накопичення, обробки і поширення інформації, зокрема, у прийнятті стратегічних рішень, збільшилася кількість суб'єктів інформаційних відносин і споживачів інформації. Інформація грає все більшу роль в процесі життєдіяльності людини.

Формально інформаційна безпека — це стан захищеності основних сфер життєдіяльності по відношенню до небезпечних інформаційних впливів. Часто найнебезпечніші інформаційні впливи називають інформаційною зброєю. Інформаційна зброя — засоби знищення або розкрадання інформаційних масивів, добування з них необхідної інформації після подолання системи захисту, обмеження або заборони доступу до них законних користувачів; дезорганізація роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем, всіх засобів високотехнологічного забезпечення життя суспільства і функціонування держави.

Аналіз накопиченого досвіду, а також досвіду роботи над Доктриною інформаційної безпеки України дозволяє запропонувати наступні визначення інформаційної безпеки: — такий стан озброєності знаннями особистості, суспільства і держави, при якому досягається захи-

щеність і реалізація їх життєво важливих інтересів і гармонійний розвиток незалежно від наявності внутрішніх і зовнішніх загроз; — такий стан інформаційного забезпечення завдань національної безпеки, при якому досягається, гармонійний розвиток потреб і використання інформації особистістю, суспільством і державою незалежно від наявності внутрішніх і зовнішніх загроз; — такий стан інформаційного середовища, при якому гарантується його розвиток і використання в інтересах особистості, суспільства і держави; — захищеність від різного роду зовнішніх і внутрішніх загроз систем формування і поширення інформаційних ресурсів, що забезпечує їхнє ефективне використання в інтересах особистості, суспільства і держави [6].

Значущість інформаційної безпеки як складової воєнної безпеки України пояснюється залежністю реалізації національних інтересів України у військовій сфері від інформаційних загроз. З аналізу основних загроз національним інтересам України у воєнній сфері випливає, що реалізаційною основою більшості цих загроз є інформаційні впливи. Наведемо показові приклади.

З-поміж різних загроз стабілізації воєнно-політичної обстановки та недопущенню збройних конфліктів в Україні розрізняються такі: висунення територіальних претензій до України; втручання у внутрішні справи України; нестабільність воєнно-політичної обстановки навколо України; активізація сепаратистських сил і підтримання їх ззовні; заяви та акції, що дискредитують внутрішню і зовнішню політику України; войовничість політичного керівництва сусідніх країн; загострення міжетнічних і міжконфесійних суперечностей; нестабільність соціально-політичної обстановки в деяких країнах Центральної Європи [4, с. 53].

Всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні, причому їх інформаційна складова досить вагома.

Основним знаряддям ведення війни є армія або іррегулярні збройні, воєнізовані формування, здатні вести безперервні і систематичні військові дії. Поряд зі збройною боротьбою, що становить специфічний зміст війни, в ній застосовуються також економічні, дипломатичні, науково-технічні, інформаційні, ідеологічні, психологічні засоби і методи нав'язування противнику своєї волі, ослаблення його військових можливостей і зміцнення власних позицій. Застосування технічних засобів (зброї) для фізичного придушення противника, підпорядкування його своїй волі — є визначальною ознакою сутності інформаційної війни. Цим інформаційна війна відрізняється від інших видів політичної боротьби та інших форм застосування зброї, а саме вторгнення, військового інциденту, військової блокади, загрози силою, спеціальної операції, в тому числі АТО.

Разом з тим в сучасних умовах війна не обов'язково повинна асоціюватися з початком військових дій — продовження політики може здійснюватися насильницьким шляхом не тільки військовими, а й невійськовими засобами.

Таким чином, центральною віссю війни є збройна боротьба, а все інше групується навколо неї і утворює складну гібридну систему, в рамках якої розвивається протистояння в різних сферах людської діяльності: соціально-економічної, адміністративно-політичної та соціально-культурної. Невизначеність процесів розвитку протистояння обумовлює хиткість контурів конфліктів сучасності, вимагає нових підходів до розробки і реалізації забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни та протидії і нейтралізації задумів противника.

Спроба об'єднати різнорідні визначення в одне привела до появи поняття «гібридна війна», яке в даний час досить часто використовується різними авторами, нерідко вкладають в нього різні смисли. Така строкатість визначень, з одного боку, надає терміну «гібридна війна» високу ступінь нестійкості і не дозволяє включити його в існуючу класифікацію воєн і конфліктів, а з іншого — робить його теоретично привабливим, тому що він може вмістити в себе велику кількість смислів. При цьому нічого принципово нового в понятті «гібридна війна» немає [1, с. 14].

Отже, гібридність — це властивість будь-якої війни, оскільки протиборчі сторони обов'язково прагнуть застосовувати всі наявні в їхньому розпорядженні сили, засоби та способи ведення бойових дій. Сьогодні поняття «гібридність» відображає суттєві зміни характеру сучасних воєн, які відрізняються різноплановістю, а військові дії в разі конфлікту з високотехнологічним супротивником будуть вестися як уже в звичних середовищах — на суші, в морі та повітрі, так і в нових сферах — космічній та кібернетичній. Також важлива характеристика сучасних війн — багатовимірність, яка передбачає поєднання інформаційного, військового, фінансового, економічного і дипломатичного впливу на супротивника в реальному часі [2, с. 157]. У гібридної війні по-іншому проявляють себе фактори тертя і зносу війни, що вимагає їх врахування під час забезпечення інформаційної безпеки України у воєнній сфері.

Властивістю багатовимірності в повній мірі володіють гібридні військові конфлікти некласичного характеру за участю в бойових діях збройних формувань недержавних суб'єктів, в числі яких міжнародний тероризм, приватні військові компанії, для яких характерна розмита національна і ідеологічна приналежність. Змінюється співвідношення військових і невійськових засобів дій, до яких вдаються сторони конфліктів. До невійськових засобів насильства в гібридної війні відносяться традиційна і публічна дипломатія, правові економічні, ідеологопсихологічні, інформаційні, гуманітарні, розвідувальні, технологічні та деякі інші інструменти впливу. Правильно обрана стратегія дозволяє досягти кумулятивного, системного ефекту від застосування сукупності всіх цих засобів. Важливу роль набувають психологічні заходи, спрямовані на забезпечення підтримки і співпраці з дружніми і нейтральними країнами.

Забезпечуючи інформаційну безпеку у воєнній сфері слід знати, що у гібридної війні до відкритого застосування сили нерідко переходять лише на етапі завершення конфлікту, використовуючи з цією метою існуючу нормативно-правову базу миротворчої діяльності та операцій з кризового урегулювання. Це важливий фактор, що вимагає якісних видозмінених показників, що визначають військові конфлікти нового покоління і їх стратегії.

По-перше, реалізується тенденція переходу від лінійної до нелінійної моделі війни, заснованої на застосуванні непрямих асиметричних дій, що дозволяє за рахунок досить обмеженого впливу домогтися істотних, нерідко стратегічних результатів.

По-друге, змінюються системоутворюючі елементи, що визначають зміст самої філософії війни як гуманітарної складової вчення про війну. В умовах, коли гібридна війна проти України перетворилася в повсякденний фактор існування нашої країни, успішне протистояння загрозам нового виду в вирішальною мірою залежатиме від здатності своєчасно сформувати нове знання про війну і на цій основі визначити завдання забезпечення інформаційної безпеки держави у воєнній сфері в цілому та стратегію будівництва Збройних Сил зокрема.

Стратегія гібридної війни Росії проти України націлена на виснаження нашої країни і передбачає широкий спектр дій, що включають використання військових і іррегулярних формувань одночасно з проведенням в рамках єдиного задуму і плану операцій по хаотизації економіки, сфери військової безпеки, соціально-культурної сфери, а також застосування кібератак. Держава-агресор таємно, без формального оголошення війни атакує структури державного управління, економіку, інформаційну та соціально-культурну сферу, сили правопорядку і ЗС України. Потім, на певному етапі розгортаються військові дії за участю місцевих бунтівників, найманців, приватних військових компаній, підтримуваних кадрами, зброєю і фінансами з-за кордону і деякими внутрішніми структурами: олігархами, злочинними, сепаратистськими і псевдорелігійними організаціями (за прикладом ОРДЛО).

Важлива складова цієї стратегії — цілеспрямована на воєнну сферу та безпеку нашої держави, щоб втягнути її в непомірні виснажливі військові витрати шляхом провокування локальних конфліктів в прикордонних районах і стратегічно важливих регіонах, проведення у кордонів масштабних військових навчань за провокаційним сценаріями, розгортання дестабілізуючих

систем зброї, використання можливостей «п'ятої колони» і агентурних мереж. Час дії стратегії змору — багато років.

Руйнівний імпульс операціям гібридної війни надає поєднання стратегій розтрощення і змору, що дозволяє формувати своєрідний руйнівний тандем для цілеспрямованого використання властивостей глобальної критичності сучасного світу з метою підриву фундаментальних основ існуючого світопорядку, дестабілізації окремих країн, примушування їх до капітуляції і підпорядкування країні-агресору. В основі поєднання стратегій розтрощення і змору лежать механізми поетапного посилення і експлуатації критичності в цілях хаотизації обстановки в країні на яку агресор намагається вплинути [7, с. 76].

Операції гібридної війни розглядаються в найширшому контексті, що охоплює внутрішню і зовнішню політику, фінанси та економіку країни, інформаційно-комунікаційну сферу, моральний дух армії і населення та інші фактори, що впливають на здатність нації до спротиву. Крім того, на кожному етапі гібридного військового конфлікту успішна стратегія призводить лише до попереднього результату, який може бути зведений до нуля через дипломатичні втручання більших держав.

Впливаючи на інформаційну безпеку держави у гібридного військового конфлікту є три різних виміру, обумовлені фактором його багатовимірності, а також тимчасовим і просторовим факторами. Багатовимірність передбачає поєднання інформаційного, військового, фінансового, економічного і дипломатичного впливу на супротивника в реальному масштабі часу. Часовий фактор пов'язаний з тривалістю впливу на противника при реалізації стратегії виснаження, а просторовий — з одночасним охопленням стратегією всій території держави. Дані вимірювання, в свою чергу, визначають розмах і зміст заходів щодо протистояння гібридної війні.

Відповідно до даної особливісті провідна роль в гібридної війні відводиться інформаційно-психологічному та економічному впливу на противника. Застосування непрямих асиметричних дій і способів ведення війни дозволяє позбавити протиборчу сторону фактичного суверенітету без захоплення території держави військовою силою. На відміну від війни класичного типу в гібридної війні немає лінії фронту. Звідси випливає, що необхідно, зокрема, передбачити в оборонній стратегії перехід від форми прикриття простору воєнної, військово-політичної, економічної сфери держави до функціонального контролю над найважливішими стратегічно елементами кожної сфери.

Відсутні в гібридної війні і сторони конфлікту, які в традиційній війні є його носіями. Військові дії не оголошуються, сторони конфлікту не визначені, в той час як в міжнародно-правових документах вважається, що конфлікт як фаза протиріччя можливий лише тоді, коли його сторони представлені суб'єктами. Де їх немає — не може бути й конфлікту.

Поєднання глобалізаційних змін і інформаційно-комунікаційної революції уможливило помітний якісний перехід в гібридній війн на етапі визначення мети, коли держава-агресор утримується від масованого військово-силового впливу на противника і вдається до гнучкого поєднання економічних, інформаційно-психологічних, дипломатичних, кібернетичних і інших заходів. Ставка робиться на оволодіння стратегічною ініціативою в ході проведення комплексних операцій з економічного та інформаційно-психологічному знищення противника, спрямованих на придушення його волі і підпорядкування зовнішнім керуючим імпульсам за рахунок хаотизації обстановки і дезорганізації системи державного і військового управління [8, с. 102].

Вищі інтереси, пов'язані з війною, зберігаються і припускають наявність рішучої мети — розгром противника шляхом нанесення йому поразки на всіх фронтах: ідеологічному, економічному, військовому, дипломатичному. Боротьба на кожному з фронтів — це організоване насильство для примусу до відповідних політичних, військових, економічних, ідеологічних та інших поступок. Наявність декількох фронтів гібридної війни вимагає забезпечення можливості оперативного зосередження критично важливих зусиль і ресурсів на найбільш загрозли-

вому напрямку. Сьогодні найбільш активні фронти гібридної війни проти України — інформаційний, економічний та військовий тиск.

Розвиток сучасного військового тренда призводить до розширення локальних і регіональних конфліктів, для яких характерна зміна форм вирішення міждержавних протиріч. Війна між державами з масштабним застосуванням насильства стає хаосом, на зміну їй йдуть «нові війни», в основу яких покладено принципово інший тип організованого насильства, що представляє собою поєднання військових (бойових) дій, організованої злочинності, терористичних атак і масованого впливу в сфері інформаційно-комунікаційних технологій. Поряд з традиційними середовищами протистояння формуються нові: кіберпростір, космос і все більш витончена боротьба в воєнній сфері.

Кіберпростір — дуже специфічна сфера діяльності і середовище, яке має відносно автономний характер, має великий вплив на розвиток економіки, політичного життя, культури, техносфери, військової справи. Завдання підвищеної складності в даній сфері — виявлення джерела загрози і кібератак, усунення ефекту анонімності. Кіберпростір перетворюється на каталізатор нового спектру загроз і підвищеного ступеня стратегічної невизначеності. У кіберсередовищі найбільш рельєфно проявляється дія закону переходу кількісних змін у якісні. Саме тут спостерігаються практично революційні темпи розвитку боротьби, зумовлені запровадженням передових інформаційно-комунікаційних технологій і загальносвітовими тенденціями використання можливостей, що відкриваються для атак проти кібервразливих критично важливих об'єктів інфраструктури. Це пов'язано, зокрема, з масштабним переходом на цифрові системи управління виробничими і технологічними процесами на атомних електростанціях і деяких інших високотехнологічних підприємствах, а також з розширенням підключення офісних і промислових корпоративних комп'ютерних мереж до інтернету.

Комплексний характер гібридних загроз ускладнює виявлення їх джерела, яке, як правило, є анонімним. Невідомість джерела гібридних загроз і невизначеність часу і місця їх прояву в ході гібридної війни сприяють розбіжностям зусиль розвідки, відволікають сили і засоби на другорядні напрямки, призводять до втрати часу на вироблення заходів протидії і, як наслідок, до зростання збитків.

Таким чином, розробка і реалізація забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни повинна включати наступні етапи:

перший — чітке формулювання сенсу і цілей війни;

другий — виявлення слабких і уразливих сторін у сферах забезпечення внутрішньої і зовнішньої безпеки держави;

третій — формування комплексу гібридних загроз з урахуванням місцевої специфіки для впливу на об'єкт зі сторони агресора;

четвертий — вироблення чіткого планування на основі конкретного врахування національних сил і засобів, призначених для впливу на вузькі і вразливі місця в політико-адміністративній, фінансово-економічній та воєнній сферах;

п'ятий — протистояти послідовному руйнівному впливу на ключові сфери управління державою з зосередженням основних зусиль на найбільш критичних факторах, що забезпечують військову безпеку держави (економіка, фінанси, моральний дух армії і населення);

шостий — запобігати розгортання неоголошених військових дій, в ході яких країна-агресор атакує державні структури і регулярну армію за допомогою місцевих сепаратистів, підтримуваних зброєю і фінансами з-за кордону. Важливе місце відводиться діям «п'ятої колони», яка використовується для дестабілізації обстановки в державі та підриві конституційного ладу.

Щоб не допустити раптовості застосування проти України сучасних підривних технологій, особливу увагу слід приділити розкриттю комплексу заходів, реалізованих агресором при підготовці і веденні гібридної війни. Для цього розвідку необхідно організувати з урахуванням наступних основних особливостей гібридної війни: — гібридна війна не оголошується, військо-

ві дії протягом тривалого часу можуть не проводитися, відсутні фронт і тил, а операції охоплюють всю територію України; — держава-агресор протягом певного часу не розкриває себе, не проводить масштабних мобілізаційних заходів, прагне вести війну чужими руками, використовує найманців, приватні військові компанії, активізує дії внутрішніх іррегулярних формувань, «п'ятої колони» і агентів впливу; — формально відсутній єдиний керівний центр гібридної війни, загальна цільова установка по руйнуванню нашої держави розробляється і узгоджується на рівні урядових органів, керівництва транснаціональних корпорацій, фінансово-банківських структур, окремих впливових осіб; — плани дій по дестабілізації адміністративно-політичної, соціально-економічної і воєнної сфер може передбачати створення на території України розподілених мережевих структур з високим ступенем самостійності і здатністю до самосинхронізації. Заздалегідь відпрацьованими канали їх фінансового, матеріально-технічного, інформаційного, кадрового забезпечення, створеними складами зброї, боєприпасів, засобів зв'язку, місцями для підготовки бойовиків; — використання сил спеціальних операцій проти стратегічно важливих об'єктів, для викрадень і вбивств політичних лідерів та надання підтримки іррегулярним формуванням; — регулярні збройні сили агресора починають діяти на заключних етапах гібридної війни під приводом «гуманітарної інтервенції», проведення операції з примусу до миру. Отримання мандата ООН для цього бажано, але не обов'язково.

Підчас гібридної війни за єдиним загальним задумом і планом виконується комплекс операцій, що представляє комбінацію військових і невійськових, таємних і відкритих дій, операції по дезінформації та пропаганди. Здійснюються підготовка і розгортання іррегулярних збройних формувань, сил спеціальних операцій, а іноді і регулярних збройних сил. Задум кожної операції тісно пов'язаний із загальним задумом війни і являє собою рішення, виражене в найбільш загальних рисах і включає мету і шляхи його досягнення.

Операції гібридної війни можуть містити витончені кібератаки, економічний та політичний тиск і використання вразливих місць противника. Багато з подібних тактик не нові, проте останнім часом вони придбали небачену раніше швидкість, масштаб та інтенсивність впливу на обстановку в цілях її хаотизації. В умовах, що склалися сенс гібридної війни Росії проти України полягає в ліквідації української державності, фрагментації країни та перекладі окремих її частин під зовнішнє управління. Мета гібридної війни полягає у використанні технологій керованого хаосу для руйнування адміністративно-політичної, фінансово-економічної та воєнної сфер управління громадської діяльності людей з подальшим встановленням повного контролю держави-агресора над територією і населенням. Загрозлива реальність гібридної агресії проти нашої країни потребує вжиття невідкладних заходів протидії.

Забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни може бути оборонним або наступальним та служити основою загального плану впровадження заходів протидії противнику або атакуючого впливу на нього з урахуванням мінливих політичних ситуацій і обстановки. Забезпечення повинно базуватися на даних всіх видів розвідки. Поряд з розкриттям загального задуму гібридної війни і її конкретних операцій завдання розвідки полягає в добуванні відомостей про приховані підривні елементи, які діють в мережі, що складається з ізольованих осередків на всій території країни. У цьому контексті в регіонах може бути корисним створення розвідувально-ударних груп з власними каналами оперативного, надійного і прихованого зв'язку.

Головну увагу слід приділяти розкриттю наступних дій противника по: — пошуку джерел сталого фінансування протестного руху, а потім збройних формувань як з боку зовнішніх зацікавлених сил, так і з використанням внутрішніх можливостей; — виявлення екстремістських громадських груп і політичних об'єднань, здатних брати участь в запланованих акціях ненасильницького, а потім і силового характеру, аж до громадянської війни; — визначенню практичних гасел, максимально наближених до реальних вимог екстремістських громадських груп, дії яких в результаті можуть використовуватися для підриву легітимності і зламу існуючої

влади; — підготовці лідерів, здатних очолити політичний протест, який має кінцевою метою державний переворот; — навчання в спеціалізованих таборах польових командирів і бойовиків для силових акцій, організація мобілізаційних пунктів за кордоном і маршрутів перекидань найманців; — підтримки екстремістських елементів в опозиції і здійснення експансії в регіони, перш за все за рахунок координованого використання контрольованих опозицією електронних вітчизняних і зарубіжних ЗМІ; — важливе місце відводиться завоювання підтримки з боку міжнародних організацій та міжнародної громадськості; — організації мережевих структур управління підривними діями, постачання, зв'язку та моніторингу обстановки.

Висновки

Розробка і застосування Росією стратегій гібридної війни, тестування її в ряді пострадянських країн містить пряму загрозу національній безпеці Україні. Більш того, гібридна війна проти України сьогодні набула конкретних рис. Гібридна війна, нав'язана Україні сусідньою державою, фактично перетворилася на засіб міждержавного протистояння, а розмах операцій і руйнівні ефекти впливу на всі життєво важливі сфери держави дозволяють використовувати загрозу нарощування дестабілізуючих операцій як засіб стратегічного стримування, тиску і залякування. Інформаційно-психологічні операції націлені на розвал і фрагментацію країни, підрив здатності до опору, дискредитацію лідерів, внесення розколу в ряди союзників і партнерів.

Отже, держава з метою забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни має вживати таких заходів: проведення систематичного аналізу застосування засобів, форм та способів інформаційної боротьби у воєнній сфері, визначення напрямів забезпечення інформаційної безпеки держави у цій сфері; удосконалення законодавства з питань координації діяльності органів державної влади та органів військового управління під час вирішення завдань забезпечення інформаційної безпеки; удосконалення видів і засобів захисту інформації в інформаційно-телекомунікаційних мережах, що задіяні в управлінні військами і зброєю, від несанкціонованого доступу; удосконалення форм і способів протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності держави; підготовка спеціалістів з питань інформаційної безпеки у воєнній сфері.

Створення системи забезпечення інформаційної безпеки держави у воєнній сфері в умовах гібридної війни має здійснюватися відповідно до наступних основних принципів: високий ступінь інтегрованості системи інформаційної боротьби Збройних Сил України в систему забезпечення інформаційної безпеки держави; превентивно-оборонний характер діяльності структур інформаційної боротьби, спрямованої на протидію викликам, небезпекам та загрозам національній безпеці держави у воєнній сфері у будь-якій формі їх прояву; чіткий розподіл повноважень з питань інформаційної безпеки між Міністерством оборони України і Генеральним штабом Збройних Сил України; чітке розмежування завдань і функцій органів військового управління (структурних підрозділів, військових частин), які залучаються до виконання завдань щодо забезпечення інформаційної безпеки національних інтересів у воєнній сфері та органів військового управління (структурних підрозділів, військових частин), які залучаються до забезпечення інформаційної безпеки підготовки та застосування Збройних Сил [5, с. 54–55].

Однією з основних тенденцій розвитку воєнно-політичної ситуації у світі є прискорення розвитку інформаційних технологій, збільшення спроможностей держав щодо проведення інформаційно-психологічних операцій та операцій в кіберпросторі, посилення чутливості суспільства до загибелі мирного населення та втрат особового складу військових формувань у воєнних конфліктах.

Україна не зможе змагатися з Росією військовою силою. Саме тому сучасна ситуація настійно вимагає від України та її союзників спільних зусиль щодо прогнозування можливого використання нових підривних технологій і планування відповідних заходів в рамках єдиної протидії гібридної війні зі сторони агресора. В умовах, що склалися успішне вирішення комплексу задач по забезпеченню національної безпеки української держави і її союзників має бути

досягнуто за рахунок консолідації суспільства, зміцнення національної оборони, вибудовування всебічних зв'язків з союзниками і партнерами, підтримки конструктивних організацій забезпечення міжнародної безпеки та рішучої протидії спробам деструктивного впливу в сфері міжнародних відносин.

СПИСОК ЛІТЕРАТУРИ:

1. Бартош А. А. «Трение» и «износ» гибридной войны. Военная Мысль. 2018. № 1. С. 5–13

2. Быченок Н. Н. Основы информационной борьбы: учебник / Н. Н. Быченок, Т. М. Дзюба, А. А. Рось, В. В. Витковский. К.: НУОУ, 2014. 265 с.

3. Быченок Н. Н. Дзюба Т. М., Рось А. А., Витковский В. В., Вищун В. В. Информационная безопасность государства в военной сфере. К.: НУОУ, 2012. 264 с.

4. Быченок Н. Н., Савченко В. А., Дзюба Т. М. Основы обеспечения информационной безопасности государства в военной сфере. К.:НУОУ, 2017. 244 с.

5. Горбулін В. П., Литвиненко О. В. Національна безпека: український вимір. К.: Інтертехнологія. 2008. 104 с.

6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Электронный ресурс. Режим доступу: https://zakon. rada. gov. ua/laws/show/47/2017

7. Панарин И. Н., Панарина П. Г. Информационная война и мир. М.: ОЛМА-ПРЕСС, 2003. 204 с.

8. Новиков В. К. «Дранг нах Остен» — сценарии информационных войн в действии. М.: Горячая линия — Телеком, 2016.180 с.

9. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: «Горячая линия» — Телеком, 2004. 280 с.

REFERENCES:

1. Bartosh A. (2018). «Trenie» i «iznos» gibridnoy voynyi, Voennaya Myisl, №1. pp. 5–13.

2. Byichenok N. (2014). Osnovyi informatsionnoy borbyi: uchebnik, Kyiv, NUOU, 265 p.

3. Byichenok N. (2012). Informatsionnaya bezopasnost gosudarstva v voennoy sfere, Kyiv, NUOU, 264 p.

4. Byichenok N.N., Savchenko V.A. & Dzyuba T.M. (2017). Osnovyi obespecheniya informatsionnoy bezopasnosti gosudarstva v voennoy sfere, Kyiv, NUOU, 244 p.

5. Horbulin V.P. (2008). Natsionalna bezpeka: ukrainskyi vymir, Kyiv, Intertekhnolohiia, 104 p.

6. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpekyUkrainy», available at:https://zakon.rada.gov.ua/laws/show/47/2017

7. Panarin I. N., Panarina P. G. Informatsionnaya voyna i mir. M.: OLMA-PRESS, 2003. 204 s.

8. Novikov V. K. «Drang nah Osten» — stsenarii informatsionnyih voyn v deystvii. M.: Goryachaya liniya — Telekom, 2016.180 s.

9. Malyuk A. A. Informatsionnaya bezopasnost: kontseptualnyie i metodologicheskie osnovyi zaschityi informatsii. M.: «Goryachaya liniya» — Telekom, 2004. 280 s.

Стаття надійшла до редакції 20.09.19