© Brailovskyi M., Ivanchenko I., Opirskyi I., Khoroshko V. Information and psychological confrontation in Ukraine // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 3, pp. 144-149.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.25.14459

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНЕ ПРОТИБОРСТВО В УКРАЇНІ

Микола Браіловський[1], Ігор Іванченко[2], Іван Опірський[3], Володимир Хорошко[2]

[1] Київський національний університету імені Тараса Шевченка
[2]Національний авіаційний університет
[3] Національний університет «Львівська Політехніка»

БРАІЛОВСЬКИЙ Микола Миколайович, к.т.н., доцент

Рік народження: 1972, м. Київ, Україна.
Освіта: Українська державна академія зв'язку ім. О.С. Попова, 1994 рік.
Посада: доцент кафедри кібербезпеки та захисту інформації.
Наукові інтереси: національна безпека, методи та засоби технічного захисту інформації, захист кіберпростору, соціальна інженерія.
Публікації: понад 130 наукових публікацій, серед яких наукові статті, колективні монографії, тези та матеріали доповідей на конференціях, підручники та науково-методичні посібники.
E-mail: bk1972@ukr.net.
Orcid ID: 0000-0002-3148-1148.

ІВАНЧЕНКО Ігор Сергійович, к.т.н.

Рік та місце народження: 1987 рік, м. Бердянськ, Запорізька обл., Україна.
Освіта: Національний авіаційний університет, 2009 р.
Посада: доцент.
Наукові інтереси: моделі та системи кібербезпеки, програмні методи захисту інформації, методи і моделі розмежування доступу та підтримки цілісності інформаційних ресурсів.
Публікації: понад 40 публікацій, серед яких наукові стаття, колективні монографії, навчальні посібники, тези та матеріали доповідей на конференції, навчально-методичні праці.
E-mail: igor-p-l@ukr.net.
Orcid ID: 0000-0003-3415-9039.

ОПІРСЬКИЙ Іван Романович, д.т.н., доц.

Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: доцент кафедри захисту інформації з 2016 року.
Наукові інтереси: методи і засоби технічного захисту інформації, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки,прогнозування несанкціонованого доступу, математичні методи та моделі захисту інформації, спецвимірювання.
Публікації: понад 100 наукових публікацій, серед яких наукові статті, колективні монографія, навчальні посібники, тези та матеріали доповідей на конференціях, навчально-методичні праці.
E-mail: iopirsky@gmail.com.
Orcid ID: 0000-0002-8461-8996.

ХОРОШКО Володимир Олексійович, д.т.н., професор

Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: кібербезпека, інформаційне протиборство.
Публикации: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Анотація. *На сьогодні інформаційна війна є тотальним явищем, де неможливим є визначення її початку та кінця. Це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті та приховані цілеспрямовані інформаційні впливи держав одна на одну, з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи з допомогою таких засобів, використання яких дозволяє досягти задуманих цілей. Описано 4 підходи до визначення інформаційної війни, які вміщують політико-правові, соціально-економічні, психологічні дії, що передбачають захоплення інформаційного простору ворога, знищення його комунікацій, позбавлення засобів передачі повідомлень тощо, а також концептуальні питання та основи теорії мережево-центричної системи управління й організації бойових дій та кібердій або кібернетичної війни. Досліджено впровадження стратегії кібернетичного підходу до організації дій під час проведення військових операцій для отримання максимального ефекту від впливу на три сфери - моральну, ментальну, фізичну і визначено достатність такого підходу до збільшення мобільності, точності та вогневої мощі озброєння. Також було досліджено вплив на найбільш уразливі об'єкти із використанням системного кібернетичного підходу, що дало змогу оцінити застосування його у сучасних умовах щодо вироблення стратегії та тактики ведення боротьби в інформаційному полі.*

Ключові слова: *інформаційно-психологічні впливи, інформаційна війна, інформаційна зброя, інформаційне поле, стратегія, кібернетична війна, кібердії.*

Вступ

На всіх етапах розвитку людської цивілізації інформація була як найважливішим об'єктом, так і засобом боротьби між людьми, народами, державами. Окремі факти здійснення інформаційного впливу на широку аудиторію можна виявити протягом усієї історії суспільства. Зрозуміло, що в різні періоди інтенсивність застосування тих чи інших способів впливу як і досконалість його організації, дуже різняться. Політика ведення інформаційних війн та застосування інформаційних впливів з'явилися ще у первісні часи, разом з тим маємо зазначити, що системне вивчення цих феноменів почалось лише у XX столітті. Втім перші, поодинокі спроби дослідження цих тем мали місце і в давні часи. Серед дослідників давніх часів маємо відзначити роботи Аристотеля [1], Сунь Цзи [2]. В епоху Відродження над цією проблемою працював Н. Макіавеллі, видавши книгу «Государ» [1]. Так, загальновідомим є факт поїздки княгині Ольги з Києва до Константинополя, проте ні візантійські, ні руські джерела не висвітлюють причину та мету подолання такого довгого шляху. Здійснення інформаційних впливів (приховування інформації; подача її частково, у певному ракурсі та інші) було зафіксовано літописцем на теренах України ще за часів Київської Русі. Войовничий князь Святополк заздалегідь повідомляв про свій похід, проте залишав у таємниці напрям та сили, котрі планував задіяти. Це давало можливість навести паніку у стані військ противника та швидко розгромити його [3]. В той XIX ст. питання інформаційного протиборства розглядав К. фон Клаузевіц в книзі «Про війну» [4]. Протягом XX-XXI ст. цими питаннями дуже плідно займалися та досягли значних успіхів багато вчених з різних країн світу. Першим документально засвідченим дослідженням з теорії інформаційного протиборства є робота Мартіна Лібікі «Що таке інформаційна війна?». Великий внесок у розробці питань інформаційної війни внесли американські вчені: З. Бжезинський, Д. Бойд, Д. Уорден, В. Лінда, А. Себровскі, Д. Гарстка, Дж. Стейн, Г. Маклюєн, а також російські: С. Расторгуєв, С. Кара-Мурза, А. Манойло, І. Панярін, С. Макаренко та інші. Крім того, серед українських дослідників слід відзначити Г. Почепцова, О. Литвиненка, В.В. Остроухова, В. Ліпканя, Л.Ф. Компанцеву, Р. Грищука та інших.

Вперше термін інформаційна війна увів в обіг китайський теоретик Шень Веньгуань [5,6]. А одним із перших у відкритому виданні написав про феномен інформаційних воєн М. Маклюєн у 1960 роках. Вже тоді було відомо, що «холодна війна ведеться» за допомогою інформаційних технологій, так як у всі часи війни велися за допомогою передових технологій. Слід зауважити, що гібридна війна була винаходом Євгена Месснера білогвардійським полковником, який був начальником штабу Корнилівської дивізії. Він розробив теорію мятеж-війни. У 1967 році він видав в Аргентині книгу «Теорія третьої світової». Генеральний Штаб Радянського Союзу почав впроваджувати та розробляти цю концепцію наприкінці 70-х – на початку 80-х років XX століття. Фактично розгляд воєнних дій та їх організації з позицій воєнної кібернетики були сформульовані М. Огарковим у ці роки. Росія цю концепцію взяла на озброєння та зараз її використовує [6]. Інформаційна війна є тотальним явищем, де неможливим є визначення її початку та кінця, тож дослідження та узагальнення застосування тих чи інших способів впливу як їх досконалість є *актуальною науковою задачею*.

Метою роботи є вироблення стратегії та тактики ведення боротьби в інформаційному полі через визначення найбільш уразливих об'єктів із використанням системного кібернетичного підходу, що дасть змогу оцінити застосування його у сучасних умовах.

Основні піходи до визначення інформаційної війни.

Інформаційна війна є тотальним явищем, де неможливим є визначення ii початку та кінця. Це наявність боротьби між державами за допомогою інформаційної зброї, тобто це відкриті то приховані цілеспрямовані інформаційні впливи держав одна на одну, з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи з допомогою таких засобів, використання яких дозволяє досягти задуманих цілей.

В роботі [8] відзначається, що нині є 4 підходи до визначення інформаційної війни:

– перший підхід трактує її як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору ворога, знищення його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі;

– за другим підходом інформаційна війна – це найгостріша форма протистояння в інформаційному просторі, де першочергового значення набувають такі якості взаємодії, як безкомпромісність, висока інтенсивність суперечки та коротко тривалість гострого суперництва;

– за третім підходом інформаційна війна інтерпретується як форма забезпечення та ведення військово-силового дій за допомогою найсучасніших електронних засобів;

– четвертий підхід ототожнює інформаційні війни з кібернетичними війнами.

Вперше концептуальні питання та основи теорії мережево-центричної системи управління й організації бойових дій та кібердій або кібернетичної війни (реалізована у воєнних доктринах США «Joint Vision 2010», «Joint Vision 2020»). Основні аспекти взяття держави під зовнішній контроль для реалізації своїх інтересів шляхом придушення волі населення і влади держави-жертви до опору на основі використання широкого набору інноваційних технологій, які комплексно застосовуються, були описані в 1989 році в статті Вільяма Лінда «Обличчя війни, яке змінюється: на шляху до четвертого покоління» [9]. Основним у війнах четвертого покоління, за поглядами В. Лінда, є віна культур, ініціація, підтримка і підживлювання ззовні та організація всередині держави психологічного та інформаційного тиску на її населення та керівництво, взяття їх під зовнішній контроль та управління, створення умов для виникнення та сприяння зростання в країні соціально-економічного хаосу та само виснаження військових, фінансових та інших ресурсів [9].

Цілеспрямовані всеохоплюючі агресивні атаки на традиційні культурно-історичні та інші цінності населення, на репутацію найбільш ефективних керівників сфери державного та державно-воєнного управління. Створення умов для зниження рівня виховання, культури, освіти громадян. Організація на території країни-жертви тактами «конфліктів низької інтенсивності» за участю зовнішніх, внутрішніх та теоретичних сил.

Стратегія та тактика ведення боротьби в інформаційному полі.

Впровадження та стратегію кібернетичного підходу (кібернетичний цикл Бойда) до організації дій під час проведення військових операцій для отримання максимального ефекту від впливу на три сфери (моральну, ментальну, фізичну) здійснив Джон Бойд під час проведення операції «Буря в пустелі» в 1991 році. Він розглянув війну як поєднання цих трьох складових: руйнування волі противника, підриву загальної віри і спільних поглядів; дії, спрямовані на деформацію і створення сприйняття противником реальності на основі дезінформації та створення неправильних уявлень про ситуацію; руйнування фізичних ресурсів противника (озброєння, жива сила, інфраструктура та предмети постачання). При цьому всі дії як своїх сил, так і сил противника він запропонував розглядати в рамках кібернетичного циклу, що має в своїй структурі чотири процеси: спостереження, орієнтація, рішення, дія («петля Бойда»), який, за думкою автора, сам відтворюється і саморегулюється [9].

На основі робіт Бойда та його послідовників виділені наступні постулати теорії OODA (Observe - спостерігай, Orient - орієнтуйся, Decide - вирішуй, Act - дій) [7]:

1. Військова діяльність (бойові дії) протиборчих сторін здійснюється в однакових кібернетичних циклах OODA.

2. Зміст основних елементів циклу OODA такий:

– спостереження – збір інформації від внутрішніх і зовнішніх джерел;

– орієнтація – формування множини можливих планів (варіантів) і оцінка кожного з них за сукупністю критеріїв;

– рішення – вибір найкращого плану дій для практичної реалізації;

– дія – практична реалізація вибраного плану дій.

3. Цикл OODA є моделлю військової діяльності окремих осіб і організації для війни і конфліктів будь-якого рівня (тактичного, оперативного й стратегічного).

4. Напрямки досягнення перемоги (одержання конкурентних переваг):

– скорочення часу виконання циклу OODA;

– поліпшення якості прийнятих у циклі рішень.

5. Збільшення швидкості всіх чотирьох елементів циклу OODA – головний шлях досягнення перемоги.

Із чотирьох етапів OODA-циклу три безпосередньо пов'язані з обробкою інформації та з комп'ютерними технологіями. Четвертий етап (дія) носить у цілому «кінематичний» характер і пов'язаний з переміщенням у просторі, захистом і поразкою противника на основі бойових дій.

Щоб зберегти часові рамки OODA-циклу дій своїх сил і забезпечити більш високий, ніж у противника, темп бою, необхідно прискорити всі чотири

етапи циклу, які реалізуються. Протягом XX століття всі зусилля учених, інженерів та військових були спрямовані на вдосконалення озброєння і технологій у частині кінематичного частки петлі OODA. Результатом цих зусиль було збільшення мобільності, точності та вогневої мощі озброєння. Однак на сучасному етапі наступила технологічна межа кінематичної частини OODA-циклу – могутніші види зброї наносять на прийнятний супутній збиток, а більш швидкісні та більше захищені платформи озброєння та засоби доставки вражаючого фактора до цілі припускають непомірні на сучасному етапі матеріальні витрати. У зв'язку з цим з'явилася необхідність в удосконаленні інших етапів OODA-циклу.

Оскільки перші три етапи OODA-циклу пов'язані безпосередньо із процесами збору інформації, її розподілу, осмислення, аналізу та прийняття рішень на основі отриманої інформації, то чим швидше здійснюються збір, розподіл, аналіз, сприйняття інформації, тим швидше приймається рішення. Саме швидкість та правильність прийняття рішень – найбільш важливі в сучасних реальних бойових діях. Це послужило поштовхом до розробки концепції мережево-центричної військової діяльності.

Питання систематичного порушення управління та функціонування держави були запропоновані та реалізовані під час підготовки операції «Буря в пустелі» в 1991році полковником ВПС США Уорденом. Він розробив системний, кібернетичний підхід до сучасних бойових дій, назвавши його «операції на основі ефектів», який врахував розробки Дж. Бойда та став подальшим розвитком кібернетичної концепції мережево-центричної організації дій з елементами теорії обмеження систем. Відповідно до цієї концепції є п'ять основних сегментів: збройні сили, населення, інфраструктура, системи життєзабезпечення, воєнно-політичне керівництво – життєво важливих для будь-якої держави. Кожна держава має в них свої унікальні місця - вразливості («центри тяжіння». Їх правильне виявлення та деструктивний вплив на них призводить до ефекту системного «паралічу» держави в тих чи інших сферах або в цілому.

Центральним кільцем такої системи є її найбільш уразливий об'єкт (рис. 1). Менш уразливі об'єкти за ступенем, але не менш важливі за значенням знаходяться ближче до зовнішнього кільця. Справедливо слід відзначити те, що Дж. Уорденом зазначається, що кожне зі складових має свої центри тяжіння [10].

Вплив на такі центри викликає зміни у процесах управління на об'єктах впливу і, як наслідок чинить вплив на усю систему. Характерним за такої теорії є те, що ступінь впливу центру тяжіння на усю систему залежить від ступеню наближеності її до центрального кільця. Як випливає з теорії Дж. Уордена об'єктами впливу виступають зв'язки між кільцями та зв'язки всередині самих кілець. Таким чином, диференціювання суб'єктів або об'єктів впливу на кільця дозволяє виявляти в них ті, які відносяться до критичної кібернетичної інфраструктури. Саме таке диференціювання дозволяє сприйняти їх як єдине взаємопов'язане ціле. Це забезпечує спочатку викриття об'єктів (суб'єктів) з критичною кібернетичною інфраструктурою, а потім до порушення зв'язків між ними. Причому інструментами впливу або засобами є: політичні, інформаційні, економічні та військові, які впливають на об'єкти або центри тяжіння.

У центрі моделі Дж. Уордена є воєнно-політичне керівництво держави, національні лідери, які становлять критично важливу складову в архітектурі системи національної безпеки та оточені й захищені чотирма іншими кільцями. Так, другим кільцем є система життєзабезпечення, виробництва, фабрики,заводи, банки, які під час війни є життєво важливі для забезпечення функціонування військово-промислового комплексу. Державна інфраструктура – автомобільні шляхи, залізниці, лінії електропостачання – створюють третє кільце. Четвертим кільцем є соціум (народонаселення), а останнім, п'ятим, є зовнішнім кільцем є збройні сили [7, 10].

Ця модель реалізується за схемою «війна з середини назовні». Однак американська схема добре спрацьовує в зонах конфлікту, в яких збройні сили розглядаються місцевим населенням як зовнішній агресор.

На відміну від цієї моделі, Росія тривалий час мала на території Криму підтримку з боку місцевого населення та значні військові формування Чорноморського флоту, які ніколи не сприймалися в ролі ворога (Рис. 2).

Росія здійснювала тривалий попередній та послідовний вплив на населення АРК з метою сприйняття військовослужбовців Російської Федерації як захисників населення та виправлення «історичної помилки» щодо належності Криму Україні. Потім почав здійснюватися вплив на керівництво АРК і міста Севастополь, а після цього – масовий інформаційно-психологічний вплив на особистий склад Збройних Сил України. Були взяті під контроль основні об'єкти транспортної інфраструктури та системи життєзабезпечення. Намагання Російської Федерації провести кампанію з введення збройних сил до Криму супроводжувалося діями, які мали всі ознаки підготовленої та продуманої за цілями, заходами й наслідками інформаційно-психологічної операції, спрямованої передусім на російську аудиторію, а з іншого боку – на українську та західну аудиторії [6, 11, 12].

Тактика «гібридної війни», застосована Росією в Криму, була певними змінами поширена й на південно-східні регіони України (Рис. 3).

Так, основний вплив був зосереджений на населені регіони. Наступними об'єктами впливу були державна інфраструктура та системи життєзабезпечення відповідно. Четвертим та п'ятим колам впливу стали Збройні Сили та воєнно-політичне керівництво України [11, 13].

Особливістю проведення інформаційно-психологічних операцій Росії на південному-сході України є постійний пошук і використання актуальних інформаційних приводів, здатних сформувати необхідну громадянську думку. Останнім часом спостерігається тенденція розширення впливу на сфери раніше непритаманні для інформаційного протиборства, а саме на перегляд історії державності України та Росії та міжконфесійні відносини.

Слід зазначити, що інформаційна війна проти України спрямована не лише на розхитування ситуації всередині держави, а і на створення негативного іміджу України в світі. Стартував цей процес ще 2005 році під час першої газової війни. Тоді Україну успішно представили в якості нечесного, а щонайменше

сумнівного, транспортера газу, незважаючи на те, що протягом десятиліть Україна ніколи не допускала зриву поставок природного газу до Європи. Показово, що одночасно з цими звинуваченнями Росія наголошувала на необхідності будівництва газопроводів, альтернативних українській системі. До того ж звинувачення України у крадіжках газу не підкріплювалися конкретними фактами [14].

Слід відзначити, що в останні роки Україна стала об'єктом потужних інформаційних атак зі сторони Росії. Серед найбільш яскравих прикладів такої війни є нав'язування ідеї федералізації, надання російській мові статусу другої державної. В різні часи змінювався перелік провідних тем, таких як проблеми Чорноморського флоту, проблематика паливно-енергетичного комплексу, проблеми Криму, а також діяльність політичних організацій таких як Правий сектор, УНА-УНСО.

Вперше Україну перемогли в цій війні, коли поширювали та спотворювали інформацію про те, що Україна не здатна утримувати й обслуговувати ядерну зброю, внаслідок чого Україна добровільно позбулася ядерного статусу, втративши свій вплив на міжнародній арені.

А далі були «касетний скандал», газові війни України з Росією, звинувачення у продажу «Кольчуг» Іраку та зброї в російсько-грузинській війні. При цьому слід відмітити особливість у тому, що за роки незалежності Україна ніколи не спрацювала на випередження, не займала активну позицію, а завжди обороняється від інформаційно-психологічних атак.

Слід відзначити, що те, що впродовж останніх років робилося російськими медіа технологами на теренах України, часто не розглядалося, як загроза національній безпеці, а попит частини населення України на російські телепрограми не викликали побоювань української влади у тому, що їх перегляд з часом призведе до деструктивного і дестабілізуючого впливу на свідомість громадян, а через їхню свідомість – до зміни ставлення до самої України.

І дійсно видно, що Росія не шкодує фінанси на інформаційну війну, надає інформацію, що держава розвалюється, що Україною керують радикали, фашисти, бандерівці, нацисти, хунта, які чинять масовий безлад, вандалізм, найстрашніше – вбивають людей на вулицях, спалюють будинки комуністів, «регіоналів» та російськомовних громадян.

Сьогодні російсько-українська інформаційна війна ведеться відкрито. Проте Росія проводить інформаційні атаки та акції і проти інших держав.

Так, пропагандистські компанії раніше розглядалися як ідеологічний інструмент для просунення концепцій. В перший час так розглядали й пропагандистську кампанію Росії – як просунення ідеї «російського миру». Нова якість являє собою те, що це вже не тільки просунення ідеології, але й інструмент ведення війни. Крім того, що до останнього часу не було ясно, що таке російська пропаганда. Зараз картина прояснилась, це багатофункціональний інструмент з височайшим рівнем експертизи, де задіяні не тільки тролі, які працюють у Європі, США та більшість в Росії, але й велика група експертів, які обслуговують глибоким аналізом актуальні ситуації й дуже швидко реагують на них. Причому це аналіз і психологічний, і політичний та воєнний.

Тільки зараз країни європейської співдружності почали просинатись. Вони почали розуміти, що в 1981 році практично завершили діяльність щодо протидії Радянському Союзу на інформаційному фронті.

У Палаті лордів парламенту Великої Британії відзначили, що розвідка та зовнішньополітична аналітика Заходу програла війну Росії, недооцінивши напрямки її розвитку, і тільки події в Криму та на Донбасі дали можливість зрозуміти, що нічого не змінилося. Росія успадкувала усю систему Радянського Союзу і дуже гарно використовує інформацію як елемент державної сили, в той час як Захід фактично роззброївся.

Крім того, виявляється, що вплив на західні ЗМІ та інституції фактично здійснюється Росією. Також здійснюється підкуп журналістів і європейських політиків, який вимірюється десятками мільйонів доларів. І це без урахування проектів, конвертованих в пропагандистські інструменти – телебачення, радіо, газети, Інтернет-видання, а також у велику кількість інститутів, які працюють в США, Європі та інших місцях. Крім того ще індивідуальні домовленості та угоди з лобістами.

Тому у Європейському Союзі було утворено проект СЕРА задля виявлення інформаційно-психологічних атак та впливів, контролю, збору, аналізу та даванню відсічі або виведення на чисту воду російських пропагандистів у країнах Європи. Програма об'єднує провідних журналістів, активістів і аналітиків ЗМІ із держав Європи, які використовують свій досвід щодо розробки аналітичного інструменту для ефективного вирішення проблем із російською дезінформацією на стратегічному, концептуальному та інституціальному рівнях [15].

Висновки.

Таким чином, щодо України здійснюється неймовірно потужна інформаційна війна. Тому, необхідним є вироблення стратегії та тактики ведення боротьби в інформаційному полі.

Крім того, слід враховувати, що у сучасних умовах суттєво змінився характер збройної боротьби – вона набула ознак «гібридної війни».

Акценти збройної боротьби зміщуються в бік практичної реалізації інформаційних технологій. При цьому дедалі більше значення в досягненні політичних і військових цілей набувають інформаційно-психологічні операції, атаки, акції та дії.

Недооцінка можливостей інформаційно-психологічної зброї, заходів протидії впливам та особливостей конкретної території може стати фатальною під час подальшого загострення воєнно-політичної обстановки навколо України.

Література

[1]. В. Королько, *Основи паблик рилейшнз* / М. К.: «Рефсл-бук» - «Ваклер», 2000, 528 с.

[2]. С. Цзы, *Трактаты о военном искусстве*, М: ООО «Издательство АТС», СПб: Tezza fantastica, 2002, 260 с.

[3]. А. Гуз, *Історія захисту інформації в Україні та провідних країнах світу*, К: КНТ, 2007, 864 с.

[4]. К. Фон Клаузевиц, *О войне*, М: Эксмо, 2007, 260 с.

[5]. Т. Бєльська, "Інформаційно-психологічна війна як спосіб впливу на громадянське суспільство та державну політику", *Технології та механізми державного управління*, №3, С. 49-56, 2014.

[6]. С. Зелинский, *Информационно-психологическое воздействие на массовое сознание*, СПб: Скифия, 2008, 403 с.

[7]. Л. Пирцхалава, В. Хорошко, Ю. Хохлачева, М. Шелест, *Информационное противоборство в современних условиях: монографія*, 2019, 226 с.

[8]. П. Шпига, Р. Рудник, "Основи, технології та закономірність інформаційної війни", *Проблеми міжнародних відносин*, вип. 8, С. 326-339, 2014.

[9]. Ю. Даник, "Високотехнологічні аспекти забезпечення національної безпеки й оборони", *Комуникации и сети. Телеком, октябрь*, С. 58-69, 2018.

[10]. Р. Грищук, Ю. Даник, *Основи кібернетичної безпеки*, Житомир: ЖНАЕУ, 2010, 636 с.

[11]. Г. Певцов, С. Залкін, С. Сідченко, К. Хударковський, "Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрямки протидії", *Наука і оборона*, №2, С. 28-32, 2015.

[12]. *Інформаційна безпека держави у контексті протидії інформаційним війнам*. За ред. В.Б. Толубко. К: НАОУ, 2004, 176 с.

[13]. *Світова гібридна війна: український фронт*. За заг. ред. В.П. Горбулін. К: НІСД, 2017, 496 с.

[14]. Е. Магда, "Виклики гібридної війни: інформаційний вплив", *Наукові записки Інституту законодавства Верховної Ради України*, №5, С. 138-142, 2014.

[15]. CEPA [Електронний ресурс]. Online: http://infowaz.cepa.org/ (дата звернення 21.01.2019).

УДК 004.946.5.056

Браиловский М.М., Иванченко И.С., Опирский И.Р., Хорошко В.А. Информационно-психологическое противоборство в Украине

Аннотация. *На сегодня информационная война является тотальным явлением, где невозможно определить ее начало и конец. Это наличие борьбы между государствами с помощью информационного оружия, то есть это открытые и скрытые целенаправленные информационные воздействия государств друг на друга с целью получения преимущества в материальной сфере, где информационные воздействия - это воздействия с помощью таких средств, использование которых позволяет достичь задуманных целей. Описаны 4 подхода к определению информационной войны, содержащие политико-правовые, социально-экономические, психологические действия, предусматривающие захват информационного пространства врага, уничтожение его коммуникаций, лишение средств передачи сообщений и т.д., а также концептуальные вопросы и основы теории сетевой-центрической системы управления и организации боевых действий и кибердействий или кибернетической войны. Исследовано внедрение стратегии кибернетического подхода к организации действий при проведении военных операций для получения максимального эффекта от воздействия на три сферы - моральную, ментальную, физическую и определена достаточность такого подхода к увеличению мобильности, точности и огневой мощи вооружения. Также было исследовано влияние на наиболее уязвимые объекты с использованием системного кибернетического подхода, что позволило оценить применение его в современных условиях по выработке стратегии и тактики ведения борьбы в информационном поле.*

Ключевые слова: *информационно-психологические воздействия, информационная война, информационное оружия, информационное поле, стратегия, кибернетическая война, кибердействия.*

Brailovskyi M., Ivanchenko I., Opirskyi I., Khoroshko V. Information and psychological confrontation in Ukraine

Absract. *Today, the information war is a total phenomenon where it is impossible to determine its beginning and end. This is the existence of a struggle between states with the help of information weapons, that is, it is open and hidden targeted informational influences of states on each other in order to gain an advantage in the material sphere, where informational influences are influences by means of such means, the use of which allows you to achieve your goals. Four approaches to the definition of information war are described, containing political, legal, socio-economic, and psychological actions, involving the capture of the enemy's information space, the destruction of his communications, deprivation of means of transmitting messages, etc., as well as conceptual issues and the basics of network-centric theory control systems and the organization of military operations and cyber actions or cyber war. The implementation of the cybernetic approach strategy for organizing actions during military operations was studied to obtain the maximum effect from the impact on three areas - moral, mental, physical, and the sufficiency of such an approach to increase the mobility, accuracy and firepower of weapons was determined. Impact on such centers causes changes in the management processes of the objects of influence and consequently affects the whole system. It is characteristic of such a theory that the degree of influence of the center of gravity on the whole system depends on the degree of its closeness to the central ring. According to J. Warden's theory, the objects of influence are the connections between the rings and the connections within the rings themselves. Thus, differentiation of subjects or objects of influence on the rings allows to identify in them those that are related to the cyber infrastructure. And the tools or means of influence are political, informational, economic and military, which affect objects or centers of gravity. Also investigated the effect on the most vulnerable objects using the system of the cybernetic approach, which allowed to assess its application in modern conditions of development of strategy and tactics of the struggle in the information field.*

Keywords: *informational-psychological influences, informational warfare, informational weapons, informational field, strategy, cybernetic warfare, cyber actions.*

Отримано *23 жовтня 2019 року*, затверджено редколегією *28 листопада 2019 року*