

УДК 623.618:519.686

Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, К.І. Хударковський

*Харківський університет Повітряних Сил імені Івана Кожедуба, Харків*

## ДОСВІД І КОНЦЕПЦІЇ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ БОРОТЬБИ У ПРОВІДНИХ КРАЇНАХ СВІТУ

*В статті проведений аналіз концепцій інформаційної боротьби (інформаційної війни) у провідних країнах світу та її компонентів, визначені роль і умови досягнення інформаційної переваги у сучасній збройній боротьбі та особливості ведення інформаційної війни у країнах Європи та США.*

**Ключові слова:** інформаційна боротьба, інформаційна війна, інформаційна операція.

### Вступ

**Постановка проблеми.** На сьогоднішній день традиційні концепції ведення війни набувають глибоких змін. Уходять в минуле стратегії ведення війни на виснаження та знищення. Їм на зміну приходять концепції непрямих дій, гібридної війни, стратегічного паралічу та інші, які враховують нові фактори уразливості сторін.

В цих концепціях виділяються три сфери ведення війни: фізична, ментальна і моральна.

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізовувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів [1].

**Аналіз останніх досліджень і публікацій.** З початку століття інформаційні технології активно використовувалися в чотирьох війнах і двох військових конфліктах. Це друга арабо-ізраїльська війна в 2006 році, Сектор Газа в 2009 і 2012 роках, у Грузії проти Південної Осетії в 2008 році, а також війна НАТО проти Лівії в 2011 році та конфлікти в Сирії та Ірані [2].

Вперше інформаційна боротьба (ІБ) в XXI столітті була застосована США проти Іраку в 2003 році. Інфраструктурою інформаційної війни (ІВ) США і країн Європи є створювана ними глобальна мережа GIG (Global Information Grid), на будівництво якої було передбачено біля \$ 200 млрд. Її основне завдання – забезпечити командирів цілісною “картинкою зверху”.

Під час другої арабо-ізраїльської війни, на двох фронтах – на північному і південному, методично наносили авіаційні та ракетні удари, Ізраїль досягав поставлених цілей, однак на третьому фронті – на інформаційному, він зазнав поразки. Ця війна стала

другою війною XXI століття, у якій використовувалася зброя на нових фізичних принципах. Тут же відбулося поєднання бойової фази та інформаційної операції. Ізраїль, що завдав військової поразки своїм ворогам, програв інформаційну війну. В ізраїльській пресі інформація про розвиток подій у наземних боях ставала з кожним днем детальніше і прозоріше. Тому, створилася унікальна ситуація – великі коментарі до операцій, що ведуться, підведення підсумків після їхнього закінчення, а іноді й до їхнього початку, спочатку зробили засоби масової інформації (ЗМІ) власником фактора впливу, а потім перетворили пресу в інструмент контролю воєнних дій [2].

Третя інформаційна війна – війна у Грузії проти Південної Осетії в серпні 2008 року. Необхідно визнати, що Росія програла цю інформаційну війну на всіх її етапах. Фактично, вона не могла виграти цю війну, оскільки системи інформаційних озброєнь були нерівні. Англомовний інформаційний простір набагато більше російськомовного, а аудиторія CNN непорівнянна з аудиторією російських телеканалів. Зіграв свою роль і людський фактор.

Візуальний ряд, поданий необхідним чином, і відповідні йому за змістом тексти створювали в масовій західній свідомості антиросійську картину. А президент Грузії постійно виступав на фоні прапора ЄС і обов'язково говорив про те, що “Росія здійснила агресію” не тільки проти грузинського народу, але й проти США, НАТО та ОБСЄ.

Інформаційну війну у війні проти Лівії можна розділити на шість етапів [2]. Під час першого етапу, ще до фази відкритих збройних зіткнень, формувалися образи “ми” і “вони”, акцентувалася увага на ідеологічні символи, що виправдують прямий вплив. Психологічні операції проводилися з високою інтенсивністю як в інтересах формування позитивної суспільної думки у населення Лівії, так і для обробки особового складу лівійських збройних сил. Засоби масової інформації виступили як основні виконавці військово-політичних інтересів Франції. Їхня діяльність, проведена в умовах уже дестабілізованої в лівійській державі обстановки, мала на меті сформува-

ти необхідну думку у світового співтовариства (зокрема країнах ЄС), здійснити інформаційно-психологічний вплив на різні групи лівійського суспільства, міжнародні організації, держави арабського регіону, спонукати західні держави до втручання у внутрішню політику Лівії з можливим використанням силових методів.

На другому етапі з початком ракетно-бомбових ударів основний акцент інформаційної війни був перенесений на оперативнотактичний рівень. Основними компонентами інформаційної війни на даному етапі стали інформаційно-пропагандистські акції, радіоелектронна боротьба, виведення з ладу елементів цивільної і військової інфраструктур.

Коли конфлікт перейшов у тривалу фазу, почався третій етап інформаційної війни, завдання якого було викрити противника в морально-неприйнятних формах ведення конфлікту, а також залучити на свою сторону нових союзників. Обидві сторони прибігали до дезінформації, намагаючись посягти невір'я у власні сили та паніку.

Четвертий етап – початок штурму Тріполі. Тут використовувався механізм, що, імовірно, не використовувався із часів початку війни в Іспанії в 1936 році, коли кодова фраза по радіо означала одночасний виступ бойових сил по всій території країни. Головною подією п'ятого етапу в інформаційній війні при штурмі Тріполі був епізод, коли “Аль-Джазіра” і CNN показали кадри “перемоги” повстанців, зняті в Катарі. Це стало сигналом до атаки для заколотників і диверсантів. “Сплячі осередки” повстанців відразу почали встановлювати блок-пости, вриватися в командні пункти і квартири офіцерів, що не зрадили Каддафі.

Завершальний етап – формування вигідного трактування подій, що відбулися.

У збройних силах провідних країн світу ІБ трансформується в окремий інтегрований вид стратегічного (оперативного) забезпечення операцій, який призначений для досягнення інформаційної переваги над противником завдяки комплексному використанню всіх складових за єдиним задумом і планом.

Нажаль, на сьогоднішній день у Збройних Силах України, як і в державі в цілому, функціонує недостатньо ефективна система ведення інформаційної боротьби.

**Постановка завдання.** Метою цієї статті є аналіз концепцій інформаційної боротьби (інформаційної війни) у провідних країнах світу для впровадження позитивного досвіду у вітчизняну систему ведення інформаційної боротьби.

## **Викладення матеріалів досліджень**

Сьогодні інформаційна боротьба є видом стратегічного (оперативного) забезпечення операцій (бо-

йових дій) Збройних Сил (ЗС) України. Складовими ІБ є комп'ютерно-телекомунікаційна боротьба, радіоелектронна боротьба (РЕБ), розвідка, стратегічне та оперативне маскування, захист від психотропного впливу, морально-психологічне забезпечення, інформаційно-психологічні операції (ІПО), забезпечення безпеки своїх військ, порушення нормального функціонування або повне знищення інформаційних систем противника [3 – 10].

Аналіз публікацій у вітчизняній і зарубіжній літературі з проблеми інформаційної боротьби [3 – 6] свідчить, що в ній застосовується два види технологій: інформаційно-технічна і інформаційно-психологічна. Головними об'єктами інформаційно-технічної складової є науково-технічні засоби, а інформаційно-психологічної – люди.

Інформаційно-технічні технології – це комплексне застосування засобів розвідки, управління, зв'язку, навігації, РЕБ, а також технології дії на комп'ютерні системи, комунікаційні мережі і захист цих мереж.

Інформаційно-психологічні технології – це широкомасштабне застосування способів і засобів інформаційної дії на психіку особового складу військ і населення протилежної сторони на користь досягнення стороною, що здійснює вплив, політичних, дипломатичних, воєнних, економічних і інших цілей. Ці технології передбачають використання спеціальних методів й засобів, що призводять до порушення систем державного та військового управління противника, інформаційного впливу на його державне та військове керівництво, політичну еліту (персонально), особовий склад військ, формують сприятливу громадську думку у власній державі та інших країнах світу щодо подій, які відбуваються в зоні воєнного конфлікту, і сприяють досягненню воєнно-політичних і воєнно-стратегічних цілей у війні.

В основу розроблення концепцій та доктрин інформаційної війни більшості провідних західних країн, а також керівних документів НАТО покладені підходи щодо організації та проведення інформаційних операцій, які існують у ЗС США.

Проблеми інформаційної війни у США знаходяться в центрі уваги воєнно-політичного керівництва. Концепція “інформаційної війни” базується на тому, що інформація та інформаційні технології мають дуже важливе значення як для національної безпеки в цілому, так і для військових дій безпосередньо. На думку американських воєнних експертів, інформаційна війна складається з дій, що виконуються з метою досягнення інформаційної переваги в забезпеченні національної воєнної стратегії шляхом дії на інформацію та інформаційні системи противника із одночасним зміцненням і захистом власної інформації, а також інформаційних систем і інфраструктури [12].

Практична реалізація Концепції здійснюється шляхом проведення інформаційних операцій (ІО), під якими розуміється комплекс заходів, що проводиться за єдиним планом і задумом з метою здійснення впливу на інформацію і інформаційно-управляючі системи противника при одночасному захисті власної інформації і інформаційних систем [11–15].

Основні цілі і завдання ІО були сформульовані в директиві міністра оборони США “Інформаційна війна” (1992 р.) і розвинуті в директиві Об’єднаного комітету начальників штабів № 30-93 і “Польовому статуті ФМ 100-6 (інформаційні операції)”. У цих документах ідеї інформаційної боротьби були трансформовані в концепцію “боротьби із системами управління”, яка передбачала “комплексне проведення по єдиному плану психологічних операцій, заходів щодо радіоелектронної боротьби (РЕБ) і фізичного знищення пунктів управління і систем зв’язку з метою позбавлення противника інформації, виведення із ладу або знищення його систем управління”.

У документі “Єдина перспектива – 2020” визначено, що “головною рисою збройної боротьби в ХХІ столітті буде її перенесення в сферу інформаційного протиборства, а досягнення інформаційного панування стане обов’язковою умовою перемоги над будь-яким противником”.

Ведення інформаційної війни відповідно до керівних документів США здійснюється на двох рівнях – державному і воєнному [12].

Інформаційні операції на державному рівні повинні вирішувати завдання захисту національних інтересів США, попередження міжнародних конфліктів, припинення провокаційних і терористичних акцій, а також забезпечення безпеки національних інформаційних ресурсів.

На воєнному рівні інформаційні операції є комплексом заходів, що проводяться в масштабах збройних сил країни, їх видів, об’єднаних командувань в зонах, і є складовою частиною воєнних кампаній (операцій). Вони спрямовані на досягнення інформаційної переваги над противником і захист своїх систем управління. Досягнення інформаційної переваги над противником передбачає більш глибоке усвідомлення й розуміння ситуації на полі бою, більш точне з’ясування своїх переваг і недоліків противника, здатність їх реалізувати у своїх цілях, випереджальне прийняття й негайне доведення рішень, повністю адекватних обстановці, що склалась, та безперервний контроль їхнього виконання.

Реалізація інформаційної переваги, на думку американських фахівців, може бути досягнута при виконанні наступних умов:

– формування збройних сил (їхньої складу та структури), адаптованих до умов ведення мережецентричної війни, включаючи розробку науково обгру-

нтованих концепцій їхнього застосування, детально відпрацьованих і апробованих у процесі підготовки військ, бойових статутів і настанов;

– наявність підготовленого особового складу, що має відповідну освіту, технічну та тактичну підготовку та практичний досвід;

– наявність технічних засобів і умов для збору інформації, її колективного використання та організації взаємодії. Це передбачає оснащення військ спеціалізованою комп’ютерною технікою, системами збору, обробки й передачі даних, включаючи сучасні засоби відображення інформації, адаптовані для різних споживачів, а також розробку відповідного програмного забезпечення;

– створення умов для самосинхронізації дій військ, що передбачає досягнення єдиного розуміння обстановки в будь-який момент часу та забезпечення раціональної взаємодії в ході бойових дій.

Перед ЗС вперше поставлено завдання здійснення впливу на противника ще в загрозовий період (до початку активних бойових дій) з тим, щоб забезпечити вигідну для США спрямованість процесів управління і прийняття рішень протиборчою стороною.

За поглядами командування ЗС США, інформаційні операції включають радіоелектронну боротьбу, психологічні операції (Псо), оперативне маскування, боротьбу із системами управління, програмно-математичні дії і спеціальні інформаційні операції.

Інформаційні операції проводяться на всіх рівнях воєнних дій – стратегічному, оперативному і тактичному та поділяються на наступальні та оборонні [12].

Подальше уточнення цілей і завдань інформаційної боротьби в інтересах забезпечення переваги в інформаційній сфері було здійснено у доктрині “Інформаційні операції” (2006 р.). В цьому документі викладені погляди воєнного керівництва на їх підготовку і проведення, уточнені цілі, завдання та основні принципи інформаційного протиборства. В документі під інформаційною операцією розуміється комплекс заходів із впливу на людські та матеріальні ресурси противника для того, щоб ускладнити або зробити неможливим прийняття вірного рішення з одночасним захистом своїх інформаційно-комунікаційних мереж та комп’ютерних систем. Вказана доктрина спільно із документами JP 6-0 “Сумісні системи комунікації”, JP 3-0 “Сумісні операції”, JP 3-13.1 “Електронне протиборство” складають ядро військово-правової основи ведення інформаційної війни [15].

Воєнно-політичне керівництво Великобританії також приділяє суттєву увагу проблемам інформаційної боротьби. Цими проблемами займається департамент урядових комунікацій (The Government Communications Head-quarters). Уявлення британсь-

ких військових аналітиків про ІВ аналогічне американським – ІВ визначається як дія на інформаційні системи противника при одночасному захисті власних [12, 16].

Під інформаційною боротьбою у Великобританії розуміється цілеспрямована реалізація комплексу заходів щодо дезорганізації і встановлення контролю над системою державного і воєнного управління противника шляхом інформаційно-технічного і інформаційно-психологічного впливу на його інформаційні ресурси, на суспільну і індивідуальну свідомість, підсвідомість населення і особового складу збройних сил (особливо на осіб, що ухвалюють найбільш важливі рішення у сфері управління), а також забезпечення власної інформаційної безпеки [16]. Її головною метою визначено забезпечення інформаційної переваги над противником і ефективне його використання для досягнення перемоги в збройному конфлікті, а також для забезпечення національних інтересів. При цьому інформаційна перевага повинна досягатися за рахунок залучення інформаційних ресурсів всіх державних інститутів.

Діяльність воєнних структур у рамках інформаційної боротьби визначається концепцією “Боротьба із системами управління”. Її основними елементами є протидія розвідці противника і забезпечення безпеки дій своїх військ, введення противника в оману, радіоелектронна боротьба, психологічні операції, фізичне знищення противника [16].

Питаннями проведення інформаційних операцій у військовому відомстві займається група координації воєнних інформаційних операцій, підпорядкована міністру оборони.

Стратегічне планування проведення інформаційних операцій здійснює Об’єднаний оперативний штаб і штаб об’єднаного угруповання військ (сил) на театрі воєнних дій [16].

У Німеччині створений і активно функціонує центр безпеки інформаційної техніки із штатом у 500 співробітників та річним бюджетом 50 млн. євро [12].

Погляди німецьких фахівців на характер і способи ведення інформаційної війни в цілому співпадають з прийнятими у США та Великобританії. Передбачається ведення наступальних і оборонних операцій інформаційної війни для досягнення національних цілей. Характерною особливістю є більш глибока систематизація даних. При визначенні загроз і можливих наслідків країни та недержавні об’єднання розглядаються окремо, кримінальні угруповання виділені в окрему категорію.

На відміну від американських, німецькі аналітики розглядають керування засобами масової інформації як дієвий елемент інформаційної війни. Крім того, вони окремо розглядають економічну інформаційну війну.

Французькі експерти дотримуються концепції інформаційної війни, що складається з двох головних компонентів – військового та економічного (цивільного) [12]. Військова складова передбачає обмежену роль інформаційних операцій, оскільки інформаційна війна розглядається, головним чином, у контексті конфліктів малої інтенсивності або у миротворчих операціях. При такому підході союзники не можуть бути потенційними противниками. Економічна (цивільна) концепція передбачає більш широкий діапазон застосування інформаційних операцій. Точка зору французьких експертів відрізняється більш широким і більш глибоким вивченням конфліктів в економічній сфері. Їх підхід допускає, що союзник може одночасно бути об’єктом інформаційної війни.

Значна увага проблемам інформаційної боротьби приділяється й у Росії, що підтверджує виступ на зборах Академії військових наук (м. Москва) 28 січня 2012 року начальника Генерального штабу ЗС РФ генерала армії М. Макарова та прийняття у грудні 2014 року нової Воєнної доктрини Російської Федерації [17, 18].

Головна особливість Воєнної доктрини Російської Федерації 2014 – це визначення місця інформаційної війни в домінуючих позиціях сучасного військового протистояння. Росія визнала, що інформація – це зброя, якою досягаються перемоги. Поряд із традиційними методами ведення збройної боротьби та засобами ураження, інформаційна зброя отримала визнання в російського військово-політичного керівництва. При цьому Російська Федерація включила інформаційну складову в перелік основних загроз національній безпеці, як у внутрішній, так і в зовнішній політиці.

## **Висновки**

Таким чином, у більшості провідних країн світу активно йде формування координуючих органів по контролю за створенням і застосуванням інформаційної зброї, об’єднання зусиль у наукових дослідженнях проблем інформаційної боротьби, забезпечення інформаційної безпеки, планування інформаційних операцій, розробка юридичної бази у сфері забезпечення інформаційної безпеки, впровадження єдиної термінології.

Особлива увага приділяється розробці питань інформаційно-психологічного впливу.

За експертними оцінками фахівців НАТО, найбільш розвинені країни світу в найближчі два-три роки дістануть можливість вести повномасштабні війни в інформаційній сфері. Основними завданнями в них будуть дезорганізація (порушення) функціонування ключових військових, промислових, адміністративних об’єктів і систем противника, а також інформаційно-психологічна дія на його військово-політичне керівництво, війська і населення, перш за

все, з використанням сучасних інформаційних технологій і засобів.

Досвід проведення антитерористичної операції на південному сході України свідчить про необхідність розробки сучасної нормативно-правової бази для ведення інформаційної боротьби Україною, у тому числі її Збройними Силами.

**Подальші дослідження.** В ході подальших досліджень передбачається удосконалення класифікації інформаційно-психологічних операцій за розширеним переліком ознак.

## Список літератури

1. Воєнна Доктрина України. Затверджено Указом Президента України від 15 червня 2004 року № 648 (в редакції Указу Президента України від 8 червня 2012 року № 390/2012) [Електронний ресурс]. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/648/2004>.
2. Современные информвойны [Електронний ресурс]. – Режим доступу: [http://duma.ks.ua/articles/policy/sovremennye\\_informvoynuy/](http://duma.ks.ua/articles/policy/sovremennye_informvoynuy/).
3. Руснак І.С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18–23.
4. Толубко В.Б. Підготовка і ведення інформаційної боротьби в Збройних Силах України: Навчальний посібник / В.Б. Толубко. – К.: НАОУ, 2004. – 280 с.
5. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, –технологічні аспекти): Монографія / В.Б. Толубко. – К.: НАОУ, 2003. – 320 с.
6. Певцов Г.В. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: Монографія / Г.В. Певцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський. – Х.: Цифрова друкарня № 1, 2013. – 272 с.
7. Певцов Г.В. Основні особливості ознак проведення інформаційно-психологічної операції Російської Федерації в АР Крим / Г.В. Певцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський, А.О. Феклістов, А.В. Антонов // Наука і техніка Повітряних Сил. – Х.: ХУПС, 2014. – Вип. 1(14). – С. 37–39.
8. Певцов Г.В. Реалізація підходів інформаційної війни Російською Федерацією в сучасному інформаційному просторі України / Г.В. Певцов, С.В. Залкін, С.О. Сідченко, К.І. Хударковський, А.М. Гордієнко // Наука і техніка Повітряних Сил. – Х.: ХУПС. – 2014. – Вип. 2(15). – С. 10–13.
9. Певцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері / Г.В. Певцов, С.В. Залкін, А.О. Феклістов // Системи обробки інформації: збірник наук. праць. – Х.: ХУПС, 2011. – Вип. 2(92). – С. 57–59.
10. Феклістов А.О. Сучасні погляди на місце інформаційних операцій в системах інформаційної боротьби / А.О. Феклістов // Системи озброєння та військова техніка. – 2010. – № 2(22). – С. 25–27.
11. Жуков В. Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. – 2001. – № 1. – С. 2–9.
12. Гриняев С. Н. Концепция ведения информационной войны в некоторых странах мира / С.Н. Гриняев // Зарубежное военное обозрение. – 2002. – № 2 – С. 11–15.
13. Кисляк С. Психологические операции вооруженных сил иностранных государств: учебное пособие [Електронний ресурс] / С. Кисляк. – 2011. – Режим доступу: [http://otherreferats.allbest.ru/war/00116946\\_0.html](http://otherreferats.allbest.ru/war/00116946_0.html).
14. Корсаков Г. Б. Информационное оружие супердержавы [Електронний ресурс] / Г. Б. Корсаков // “Пути к миру и безопасности”. – 2012. – Вип. 1 (42). – Режим доступу: [http://www.perspektivy.info/rus/desk/informacionnoje\\_oruzhije\\_superderz\\_havy\\_2012-04-19.htm](http://www.perspektivy.info/rus/desk/informacionnoje_oruzhije_superderz_havy_2012-04-19.htm).
15. Соколов М. С. Инициативы США в сфере обеспечения информационной безопасности [Електронний ресурс] / М.С. Соколов. – Режим доступу: [www.voennopravo.ru/files/Соколов%20М.С.doc](http://www.voennopravo.ru/files/Соколов%20М.С.doc).
16. Димлевич Н. Информационные войны в киберпространстве – Великобритания и Израиль [Електронний ресурс] / Н. Димлевич // Фонд стратегической культуры. – 2010. – Режим доступу: <http://www.fondsk.ru/news/2010/11/08/informacionnye-vojny-v-kiberprostranstve-velikobritaniya-i-izrail-873.html>.
17. Макаров Н. Сетевые войны Николая Макарова шагнули в космос и киберпространство / Н. Макаров. – 2012. – [Електронний ресурс]. – Режим доступу: <http://www.siliyan.ru/archives/9744>.
18. Гусаров В. Информационные акценты новой Военной доктрины Кремля [Електронний ресурс] / В. Гусаров. – 2015. – Режим доступу: <http://sprotyn.info/ru/news/11034-informacionnye-akcenty-novoy-voennoy-doktriny-kremlya>.

Надійшла до редколегії 2.02.2015

**Рецензент:** д-р техн. наук проф. О.М. Сотніков, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

## ОПЫТ И КОНЦЕПЦИИ ВЕДЕНИЯ ИНФОРМАЦИОННОЙ БОРЬБЫ В ВЕДУЩИХ СТРАНАХ

Г.В. Певцов, А.Н. Гордиенко, С.В. Залкин, С.А. Сидченко, К.И. Хударковский

В статье проведен анализ концепций информационной борьбы (информационной войны) в ведущих странах мира и их компонентов, определены роль и условия достижения информационного превосходства в современном вооруженном противоборстве и особенности ведения информационной войны в государствах Европы и США.

**Ключевые слова:** информационная борьба, информационная война, информационная операция.

## EXPERIENCE AND CONCEPTIONS OF CONDUCTING INFORMATION FIGHT IN LEADING COUNTRIES

H.V. Pevtsov, A.M. Hordiienko, S.V. Zalkin, S.O. Sidchenko, K.I. Khudarkovskiy

In the article the analysis of conceptions of informative fight (informative war) was conducted in the leading countries of the world and its components, a role and terms of achievement of informative superiority is certain in the modern armed opposing and feature of prosecution of informative war in the countries of Europe and USA.

**Keywords:** informative fight, informative war, informative operation.