УДК 1:316.774

Є. М. Мануйлов, доктор філософії, професор;
О. В. Прудникова, доктор філософських наук, доцент

ІНФОРМАЦІЙНО-КУЛЬТУРНА БЕЗПЕКА УКРАЇНИ В УМОВАХ «ГІБРИДНОЇ ВІЙНИ»

Досліджено сутнісні характеристики інформаційно-культурної безпеки України. Визначено основні загрози інформаційно-культурній безпеці нашої держави. Показана корелятивність розвитку інформаційної культури та становлення інформаційної безпеки України в умовах «гібридної війни». Узагальнено основні підходи до розуміння інформаційної зброї та особливостей її застосування проти нашої держави у сучасних умовах.

Ключові слова: *інформаційна безпека, інформаційно-культурна безпека, інформаційні загрози, інформаційна війна, інформаційна зброя, гібридна війна.*

Актуальність проблеми. На початку XXI ст. українська держава стала об'єктом «гібридної війни», основою якої є потужна інформаційно-пропагандистська складова. В цих умовах значно зростає роль інформаційної культури наших співвітчизників, оскільки розвиненість даного суспільного феномену дозволяє активно протидіяти маніпулятивним та пропагандистським атакам з боку ворога. В той же час виникла нагальна потреба посилити інформаційну безпеку на державному рівні, перейти від формального ставлення до цієї проблеми до розбудови дієвої системи інформаційного захисту нашої країни. Безсумнівно, розвиток інформаційної безпеки корелюється та обумовлює становлення інформаційної культури в країні. Разом з тим варто дбати про баланс безпекової компоненти та демократичного розвитку інформаційної сфери у державі.

Виходячи з наведеного, ми ***поставили за мету в нашому дослідженні*** визначити сутнісні риси та особливості інформаційно-культурної безпеки України в умовах «гібридної війни», а також розкрити визначальну роль інформаційної культури у забезпеченні інформаційного суверенітету української держави.

Аналіз наукових джерел і публікацій. Поняття «гібридна війна» одним із перших став застосовувати американський дослідник М. Маклюен, який у своїх наукових працях детально аналізував роль інформації в сучасному світі. Вчений сформулював важливий висновок про те, що засоби масової комунікації стали новими «природними ресурсами», що збільшують багатство

суспільства. Він запропонував світу новаторську тезу: істинно тотальна війна – це війна за допомогою інформації. На основі багаторічних досліджень він довів, що сучасні війни зазвичай ведуться в інформаційному просторі та за допомогою інформаційних видів озброєнь [1, с. 202].

Гібридна війна – це війна із поєднанням принципово різних типів і способів ведення війни, які скоординовано застосовуються задля досягнення спільних цілей. Типовими компонентами гібридної війни є використання:

– класичних прийомів ведення війни (із військовослужбовцями в уніформі, військовою технікою та ін.);

– нерегулярних збройних формувань (повстанців, терористів, партизан та ін.);

– засобів і прийомів інформаційної та кібернетичної воєн [2, с. 230].

Виходячи з наведеного, можна стверджувати, що чим вищий рівень розвитку інформаційної культури суспільства, яке протистоїть агресії, тим менше шансів у ворога перемогти у «гібридній війні». Це пов'язано з тим, що агресор намагається вплинути на культурні, правові, політичні, ціннісні основи життєдіяльності суспільства та особистості, його завданням є змінити (деформувати) світогляд людини на свою користь за допомогою засобів масової комунікації.

З цього приводу дослідник О. Саєнко зауважує, що головним завданням інформаційно-психологічного впливу є зміна установок особистості. Для цього в ході «гібридної війни» усе, що сьогодні поширюється російськими засобами масової інформації на території України, особливо у східних областях, є відвертим перекручуванням картини дійсності. Використовуються нові, а точніше, брудні, методи та способи ведення цієї війни: підкуп, шантаж, залякування, викрадення людей, захоплення державних об'єктів, органів місцевої влади та об'єктів критичної інфраструктури, організація та проведення терористичних актів. Усе це супроводжується резонансними акціями насильства до непокірних та проявами мародерства. Механізм інформаційно-психологічного впливу ґрунтується на маніпуляції свідомістю мас і внесенням у свідомість цілеспрямованої дезінформації. Механізм духовного насильства над людиною, групою, масою спрямований на спотворення повідомлення про реальність, щоб, незважаючи на їх неправдивість, особа сприймала їх як вірогідні й вчиняла б відповідно до цієї деформованої інформації [3].

Людина або суспільство з низьким рівнем інформаційної культури не в змозі повноцінно протистояти маніпулятивним технологіям «гібридних воєн». Ілюстрацією наведеної тези стали процеси, що відбувалися в окремих областях України на початку 2014 р., де частина мешканців сприйняли ідеї

«фашизації», «мовного насильства» тощо, які цілеспрямовано розповсюджувалися російськими спецслужбами та ЗМІ на теренах нашої держави.

Отже, маніпулятивна інформація є деструктивною за своєю суттю, адже руйнує особистість, оскільки пропонує і нав'язує поєднання готових моделей із арсеналу масової культури. Ще однією неодмінною умовою вдалої маніпуляції є небажання реципієнтів мислити: більшість аудиторії бездумно і пасивно споживає величезний інформаційний потік, не витрачаючи на його аналіз ані інтелектуальних, ані духовних сил. До цього додається втрата людиною здатності до критичного мислення, хоча у даному випадку воно було б доречним і навіть необхідним [4, с. 55].

Вочевидь, під час «гібридних воєн» вкрай важливими стають такі характеристики суб'єктів інформаційної культури, як здатність до критичного мислення, навички зіставлення та селекції інформації, пошук джерел інформації тощо.

Важливо усвідомлювати, що у «гібридній війні» застосовуються різноманітні психоінформаційні технології, які постійно ускладнюються та вдосконалюються. На думку П. Шевчука, основними напрямами та способами маніпулятивних психоінформаційних технологій РФ відносно України були (й залишаються надалі):

– поступове зниження міжнародного іміджу України з метою послаблення її геополітичного значення;

– відповідне дозування та спотворення інформації з метою дестабілізації ситуації в державі та впровадження власної політики «керованого хаосу»;

– формування стереотипу меншовартості та вторинності українців, а також відповідне руйнування почуття нації та народу;

– домінування російської мови, культури та традицій для утвердження самоідентифікації при одночасному витісненні української мови та культури [5].

Виходячи з наведеного, держава повинна постійно вдосконалювати систему інформаційної безпеки, відповідно дбаючи про розвиток інформаційної культури громадян, вдосконалюючи освітньо-виховні програми, здійснюючи просвітницьку і контрпропагандистську діяльність у суспільстві та за його межами.

На переконання І. Боднар, головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав'язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєвоважливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у ба-

жаному для іншої сторони напрямі. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні [6, с. 69].

У цьому контексті зауважимо, що інформаційно-культурне протистояння України під час «гібридної війни» має характер ціннісно-цивілізаційний, коли фактично зіштовхуються аксіологеми «західного» та «східного» світів. У процесі цієї боротьби об'єктивно трансформується сутність і характер інформаційної культури, вона стає більш активістською, політизованою, критичною, а її носії частіше вступають у публічні дискусії, беруть участь у громадянських акціях тощо. Можна зробити висновок про те, що рівень інформаційної культури під час «гібридної війни» обумовлює соціальну активність людини, її громадянсько-політичну позицію.

Продовжуючи наведену логіку, зазначимо, що захист та розвиток національної інформаційної культури у «гібридній війні» напряму залежить від міцності інформаційної безпеки держави. Синтезуючи різноманітні підходи до розуміння природи інформаційної безпеки як підґрунтя розвитку інформаційної культури, науковці виокремлюють такі її базові характеристики: по-перше, це стан захищеності інформаційного простору; по-друге, це стан захищеності національних інтересів України в інформаційному середовищі; по-третє, це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі; по-четверте, це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства і держави від реальних та потенційних загроз в інформаційному просторі; по-п'яте, це невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки [7, с. 36].

Необхідність вдосконалення системи захисту інформаційно-культурного простору нашої держави, а особливо її культурно-ціннісної складової обумовлена тим, що методи «гібридної війни», перш за все, спрямовані на світоглядні орієнтири особистості, її світосприйняття. Так, для пошуку каналів впливу на суспільну свідомість агресор використовує набір «сюжетних ліній», які розраховані на різні соціальні групи, етнонаціональні й релігійні спільноти тощо.

На думку Є. Магди, Росія використовує широкий спектр методів «гібридної війни»:

– «криве дзеркало» – перекручування та пересмикування фактів та дискурсів;

– «легітимний вигнанець» – можливість використання особи колишнього Президента Віктора Януковича для тиску та піддання сумнівам легітимність нинішньої влади;

– «спекуляції на історії» – вочевидь не новий інструмент, сутність якого полягає у педалюванні дискусійних моментів українсько-російської історії;

– «заперечення очевидного» – має на меті зберігати обличчя, створювати видимість відсутності агресії;

– «килимове бомбардування дезінформацією» – призводить до зростання панічних настроїв, зневіри, появи численних ліній розколу в українському суспільстві, що врешті має призвести до дестабілізації ситуації всередині країни;

– «перетягування Заходу» – намагання створити проросійську коаліцію помножуються на активне лобіювання інтересів Росії діючими та колишніми європейськими політиками. До цього варто також додати активну інформаційну компанію, яка спрямована на формування позитивного образу Росії в Європі;

– «показна миротворчість» – так само має на меті створити ілюзію Москви як мирно налаштованої та непричетної до конфлікту сторони. Водночас має запевнити в наявності інтересів Росії на території України та права їх відстоювати;

– «гримаси демократії» – використовуються для нагнітання внутрішньополітичного напруження в Україні;

– «економічні лещата» – мали б підштовхнути Україну до економічного краху. Виснажена та об'єктивно залежна від російських ринків економіка й нині знаходиться на межі, втім спостерігаються і позитивні тенденції;

– «фактор газу для Європи» – випробувана стратегія звинувачення України у минулих реальних та майбутніх потенційних проблемах із зимовими поставками газу [8, с. 140].

З нашої точки зору, розвиток інформаційної культури в Україні під час «гібридної війни» передбачає формування у громадян інтелектуально-світоглядної готовності до відстоювання національних цінностей, захисту української національної ідеї.

У цьому контексті головними напрямами та принципами інформаційної політики в Україні, які мають сприяти розвитку демократичної інформаційної культури, є такі:

– забезпечення доступу громадян до інформації;

– створення національних систем і мереж інформації;

– зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;

– забезпечення ефективного використання інформації;

– сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;

– створення загальної системи охорони інформації;

– сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України;

– сприяння задоволенню інформаційних потреб українців за кордоном [9, с. 38–40].

На переконання фахівців, організатори «гібридної війни» ставлять за мету отримати в першу чергу інформаційно-культурне та інтелектуальне домінування над противником, яке має забезпечити подальшу перемогу над певною країною. Саме тому агресору набагато легше перемогти державу з низьким рівнем освіти та культури, в тому числі й інформаційної. Як зауважує Ю. Нестеряк, солідаризуючись з позицією М. Лібікі, «боротьба культур», не будучи формою озброєного протиборства, ставить своїм завданням культурну експансію, яка також полегшує застосування психологічної зброї і, що найголовніше, дає змогу точніше спрогнозувати результати цього застосування. Ще однією рисою конфліктів нового покоління стало прагнення до інтелектуального домінування, на відміну від фізичного домінування в минулому. Бажання перемогти супротивника не воюючи чи позбавити його можливості чинити опір призвело до ще однієї форми інформаційної війни – економічного домінування. Об'єднання методів інформаційної та економічної війн, на думку науковців, зумовлює такі форми протиборства, як блокування відомостей про економічну потужність та інформаційний імперіалізм, який полегшує транснаціональним корпораціям, що втратили національні ознаки, боротьбу за економічне домінування [10, с. 66].

Отже, «гібридна війна» поєднує в собі методи інформаційної, психологічної, економічної воєн та культурної експансії. Якщо у класичних війнах боротьба велася за ресурси та території, то у некласичних «гібридних війнах» ворог ставить за мету, перш за все, підкорити суспільну свідомість певної країни, перекодувати ціннісно-культурні настанови народу, спотворити його історичну пам'ять.

Для реалізації наведених завдань у «гібридних війнах» активно застосовується інформаційна зброя. Україна, ставши об'єктом інформаційного нападу, не стала винятком.

Фахівці стверджують, що інформаційна зброя – це інформація (дані), які є засобом ведення інформаційних воєн і призначення яких полягає в зміні системних якостей об'єкта інформаційного впливу за допомогою прихованих

установок на здійснення задуманих користувачем інформаційної зброї дій. Напрями і приклади використання інформаційної зброї такі:

– порушення, пошкодження або модифікація інформаційних ресурсів і знань людей про самих себе та про середовище, яке їх оточує;

– здійснення впливу на суспільну думку та позицію політичної еліти;

– завдання шкоди протилежній стороні дипломатичними засобами;

– пропагандистські, психологічні та підривні акції у сфері культури й політики;

– дезінформація;

– чутки, які створені навмисно;

– упровадження у ЗМІ своїх прибічників для проведення підривних акцій;

– проникнення в комп'ютерні мережі та системи управління базами даних, зараження комп'ютерних систем вірусами, навмисне введення різного роду помилок у програмне забезпечення об'єкта;

– інформаційна підтримка дисидентських та опозиційних рухів [11, с. 332].

Необхідно зазначити, що інформаційна зброя особливо ефективно діє проти тієї країни, яка знаходиться у кризовому стані, у суспільній свідомості якої панує ціннісна амбівалентність, соціально-політична невизначеність. Застосування інформаційної зброї стає особливо дієвим, коли у державі спостерігається протистояння між політичними силами, наявною є криза моральної та правової свідомості, є слабкою патріотично налаштована еліта, домінує низький рівень інформаційної культури серед громадян.

На думку науковців, інформаційна зброя представлена двома видами: інформаційно-технічна та інформаційно-психологічна. Інформаційно-технічна зброя – це зброя, яка впливає на інформаційні ресурси, мережі і системи державного і військового управління. Вона поділяється на:

– алгоритмічну, яка призначена для виведення з ладу або зміни алгоритму функціонування програмного забезпечення інформаційних систем, ресурсів і мереж;

– програмну, яка призначена для руйнування, спотворення (довільним чином) кодів програм, блокування та підміни (фальсифікації) масивів інформації, а також нейтралізації тестових програм і систем захисту інформаційних ресурсів;

– апаратну, яка призначена для тимчасового або повного виведення з ладу окремих компонентів радіоелектронних систем, компонентів радіоелектронного обладнання (у т. ч. систем їх електроживлення), а також дезорганізації функціонування підсистем обміну інформацією та впливу на середовище розповсюдження сигналів [12, с. 143–144].

У свою чергу, інформаційно-психологічна зброя – це зброя, яка впливає на психіку, свідомість, підсвідомість, морально-психологічний стан людини, соціальних груп та суспільства в цілому. Вона поділяється на:

– пропагандистську, яка призначена для здійснення інформаційно-психологічного впливу, спрямованого на закріплення бажаних уявлень, звичок, переконань у людини (соціальної групи), або навпаки – руйнування небажаних уявлень, звичок та переконань;

– психофізичну, яка призначена для здійснення інформаційного і (або) енергетичного впливу на психічні функції і на роботу фізіологічних органів і систем людини;

– нейролінгвістичну, яка призначена для управління людською свідомістю та поведінкою за допомогою лінгвістичних конструкцій, набору певних символів, кольорів, звуків, архетипів, візуальних зображень тощо;

– психотропну, яка призначена для впливу на мозок людини, збудження або зниження процесів мислення і сприйняття інформації за рахунок використання механізму зміни біохімічних характеристик процесів, що відбуваються у нервовій системі людини;

– психотронну, яка призначена для впливу спеціальними технічними засобами на свідомість та підсвідомість людини з метою зниження її волі, пригнічення, тимчасового виведення з ладу, зомбування тощо;

– психогенну, яка призначена для внесення змін у нервово-психічну діяльність мозку людини;

– психоаналітичну, яка призначена для впливу на підсвідомість людини терапевтичними засобами, зокрема у стані гіпнозу та глибокого сну з навіюванням їй необхідних установок тощо [12, с. 144].

Як інформаційно-технічна, так й інформаційно-психологічна зброя значно гальмують становлення демократичної, національно-орієнтованої інформаційної культури в сучасній Україні, руйнуючи комунікативні системи в різних сферах життєдіяльності суспільства, розмиваючи культурно-історичні коди існування нації, підриваючи «інформаційно-культурний імунітет» народу.

Універсальність, скритність, багатоваріантність форм програмно-апаратної реалізації, радикальність впливу, достатній вибір часу і місця застосування, нарешті, економічність роблять інформаційну зброю надзвичайно небезпечною, оскільки вона:

– легко маскується під засоби захисту, скажімо, інтелектуальної власності;

– дозволяє навіть вести наступальні дії анонімно, без оголошення війни [13, с. 30].

На сучасному етапі розвитку людства інформаційна зброя є одним з основних засобів ведення воєн, її «непомітність», потужність, багатоканальність, технічна інноваційність роблять її вкрай небезпечною. В умовах ведення «гібридної війни» проти України постає нагальна потреба нейтралізації ін-

формаційної зброї ворога задля посилення інформаційно-культурної безпеки нашої держави.

Висновки. Отже, інформаційно-культурна безпека нашої країни має ґрунтуватися на скоординованій діяльності державних інституцій та структур громадянського суспільства. Вона передбачає захист національних ціннісно-культурних пріоритетів розвитку вітчизняного інформаційно-культурного поля. Необхідно зазначити, що в умовах «гібридної війни» значно зростає роль інформаційної культури як чинника забезпечення державного суверенітету країни. Підняття рівня інформаційної культури українського суспільства об'єктивно сприятиме посиленню «імунітету» у наших громадян проти інформаційної зброї. Розвиток інформаційно-культурної безпеки України потребує приділення більшої уваги з боку держави вітчизняній освіті, кінематографу, мистецтву, літературі, іншим підсистемам гуманітарної сфери.

ЛІТЕРАТУРА

1. Маклюен Г. М. Внешние расширения человека / Г. М. Маклюен ; пер. с англ. В. Николаева ; закл. ст. М. Вавилова. – М. ; Жуковский : КАНОН-пресс-Ц : Куликово поле, 2003. – 464 с.
2. Артюшенко О. М. Українське суспільство в умовах гібридної війни / О. М. Артюшенко // Гілея : наук. вісн. – 2015. – Вип. 102. – С. 230–233.
3. Саєнко О. Г. Механізм інформаційно-психологічного впливу в умовах гібридної війни [Електронний ресурс] / О. Г. Саєнко // Вісн. Нац. акад. Держ. прикордон. служби України. Серія : Психологія. – 2015. – Вип. 1. – Режим доступу: http://nbuv.gov.ua/UJRN/Vnadpn_2015_1_11.
4. Гойман О. О. Маніпулювання масовою свідомістю в умовах сучасної гібридної війни / О. О. Гойман // Грані. – 2015. – № 1. – С. 50–56.
5. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти [Електронний ресурс] / П. Шевчук // Демокр. врядування. – 2014. – Вип. 13. – Режим доступу: http://lvivacademy.com/visnik13/zmist.html.
6. Боднар І. Р. Інформаційна безпека як основа національної безпеки / І. Р. Боднар // Механізм регулювання економіки. – 2014. – № 1. – С. 68–75.
7. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : [навч. посіб.] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с.
8. Магда Є. В. Виклики гібридної війни: інформаційний вимір / Є. В. Магда // Наук. зап. Ін-ту законодавства Верхов. Ради України. – 2014. – № 5. – С. 138–142.
9. Брижко В. До питання сучасної інформаційної політики / В. Брижко // Вісн. Акад. управління МВС. – 2009. – № 2. – С. 27–47.
10. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз / Ю. В. Нестеряк // Публ. управління: теорія та практика. – 2014. – Вип. 1. – С. 62–67.

11. Шпига П. С. Основні технології та закономірності інформаційної війни / П. С. Шпига, Р. М. Рудник // Проблеми міжнар. відносин. – 2014. – Вип. 8. – С. 326–339.
12. Левченко О. В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби / О. В. Левченко // Сучасні інформ. технології у сфері безпеки та оборони. – 2014. – № 2 (20). – С. 142–146.
13. Дугінець Г. В. Інформаційні війни як інструмент впливу на національний суверенітет в умовах глобалізації / Г. В. Дугінець, С. М. Косячевська // Екон. простір. – 2014. – № 92. – С. 23–33.

ИНФОРМАЦИОННО-КУЛЬТУРНАЯ БЕЗОПАСНОСТЬ УКРАИНЫ В УСЛОВИЯХ «ГИБРИДНОЙ ВОЙНЫ»

Мануйлов Е. Н., Прудникова Е. В.

Исследованы сущностные характеристики информационно-культурной безопасности Украины. Определены основные угрозы информационно-культурной безопасности нашего государства. Показана коррелятивность развития информационной культуры и становления информационной безопасности в Украине в условиях «гибридной войны». Обобщены основные подходы к пониманию информационного оружия и особенностей его применения против нашего государства в современных условиях.

Ключевые слова: *информационная безопасность, информационно-культурная безопасность, информационные угрозы, информационная война, информационное оружие, гибридная война.*

INFORMATION AND CULTURAL UKRAINE SECURITY IN TERMS OF «HYBRID WARFARE»

Manuilov E. M., Prudnykova O. V.

Studied the essential characteristics of information and cultural Ukraine security. It is alleged that the higher the level of information culture of society that opposes aggression, the less chance the enemy to win the «hybrid warfare». This ratio is because the aggressor is trying to influence the cultural, legal, political and value foundations of society and the individual, his aim is to distort a person's world with the help of the media. There are very important characteristics during the «hybrid warfare» such as information culture capacity for critical thinking, skills comparison and selection of information, search for sources of information and so on.

Determined the main threats for the information and cultural security of our country. It is noted that the main threat to national security information – a threat to the impact on

the other side of the country information infrastructure, information resources, society, consciousness, subconscious personality to impose the desired state (for another side) of values, attitudes, interests and decisions in vital areas of public and state activities, manage their behavior and development in the desired direction for another party.

Shown the correlativity of information culture and establishment of information security Ukraine in a «hybrid warfare». Proved that the Ukraine information and cultural opposition during the «hybrid warfare» has a value-civilizational nature when the values of «western» and «eastern» worlds factually collide. In the course of this struggle objectively transformed the nature and character of information culture, it becomes more militant, politicized, critical media and its increasingly entering the public debate, participate in civic events and so on. It is concluded that the level of information culture during the «hybrid warfare» causes social activity of man, its civic and political position.

It is alleged that need in improving protection system information and cultural space of our country, especially its cultural value component due to the fact that the methods of «hybrid warfare» primarily aimed at the ideological orientation of the individual, its world view. So, to search channels impact on public consciousness aggressor uses a set of «scene lines» that are designed for different social groups, ethnic-national and religious communities etc. «Hybrid warfare» combines the techniques of information, psychological, economic wars and cultural expansion. If in the classic wars struggle was wagged for resources and territory, then in the non-classical «hybrid warfare» enemy seeks to conquer the public consciousness of a country, encode values and cultural guidance, distort its historical memory. For implementation the above objectives in «hybrid warfare» actively used information weapons. Overviewed basic approaches to understanding information weapons and especially its use against our country in the modern world. It is noted that the information weapon is particularly effectively acts against the country, which is in crisis in the public mind which dominates ambivalence of values, socio-political uncertainty. The use of information weapon is particularly effective when there is a state of confrontation between the political forces, crisis of moral and legal consciousness, weak patriotic elite, domination by low information culture among citizens.

Key words: *information security, information and cultural security, information threats, information warfare, information weapons, hybrid warfare.*