

parliamentarianism as a new political culture of the future era of non-violence, if approaching non-violence as a phenomenon that carries the nuclei of a new history.

Key words: parliament, parliamentarianism, society, state, democracy, culture of parliamentarianism.

УДК 327.8: 15

Б. М. КАЛІНІЧЕНКО

ВИЗНАЧАЛЬНІ НАПРЯМИ ФОРМУВАННЯ СТРАТЕГІЇ ПРОТИСТОЯННЯ ІНФОРМАЦІЙНИЙ ВІЙНИ

З'ясовано характерні особливості ведення інформаційної війни на сучасному етапі, а також сформульовано визначальні напрями формування стратегії протистояння її засобам. Наведено приклади удосконалення засобів інформаційної війни на рівні керівництва провідних країн світу. Показано специфіку деструктивного впливу інформаційних технологій в умовах анексії Криму та окупації частини Донбасу Російською Федерацією. Проліковано можливості держави щодо зміцнення національної безпеки в умовах зовнішньої агресії, підкріпленої технологіями інформаційної війни.

Ключові слова: політична стратегія, інформаційна війна, асиметрична стратегія, національна безпека, інформаційний простір, інформаційні технології.

Kalinichenko Bogdan. Defining directions of the formation strategy of resisting the information war

The characteristic features of information warfare at the present stage have been elucidated, and the defining directions for the formation of a strategy to counter its means have been formulated. Examples of improving the means of information warfare at the leadership level of the leading countries of the world are given. The specificity of the destructive influence of information technologies in the context of the annexation of the crimea and the occupation of a part of donbass by the russian federation is shown. The possibilities of the state to strengthen national security in the conditions of external aggression, supported by information warfare technologies, are traced.

© КАЛІНІЧЕНКО Богдан Михайлович — кандидат політичних наук, доцент кафедри державної служби, публічного адміністрування та політології Черкаського національного університету імені Богдана Хмельницького

Key words: political strategy, information war, asymmetric strategy, national security, information space, information technology.

Інформаційне протистояння як наукове поняття набуло поширення у середині 70-х років ХХ ст. Родоначальником терміна «інформаційна війна» вважають фізика Т. Рону, який у 1976 році у розпал «холодної війни» назвав інформацію найслабшою ланкою збройних сил. Уперше цей термін був ним використаний у звіті «Системи зброї та інформаційна війна», підготовленому в 1976 р. для компанії «Боїнг» й офіційно застосованому в директиві Міністра оборони США № 3600 від 21 грудня 1992 року.

Проблеми, пов'язані з осмисленням явища «інформаційної війни» досліджували такі західні вчені як Г. Екклз, Г. Самерз, М. Лібікі, Р. Шафранські та ін. Серед українських дослідників слід відзначити праці таких вчених, як О. Дубас, В. Недбай, М. Рижков, Г. Почепцов, М. Требін, Р. Павленко, О. Соснін, В. Хорошко, В. Смолянюк, В. Балабін, Н. Гнасевич, О. Рудакевич та ін. У працях зазначених вчених з'ясовано багато проблем, пов'язаних із застосуванням засобів ведення інформаційних воєн. Разом з тим, у зв'язку з мінливим характером об'єкта дослідження, інформаційна війна потребує постійної уваги, насамперед задля вироблення адекватних засобів забезпечення від її деструктивного впливу. Зважаючи на це, метою пропонованої статті є розгляд визначальних напрямів формування стратегії протистояння інформаційній війні.

Для більш глибокого розуміння сутності поняття «інформаційна війна» розглянемо визначення термінів «інформація» та «інформаційна війна». У Законі України «Про інформацію» (1992) дається таке визначення першого з вищезазначених термінів: «інформація — будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді». Інформаційна війна визначається в науковій літературі як комплекс заходів інформаційного забезпечення, інформаційної протидії та інформаційного захисту, які здійснюються за єдиним задумом і планом з метою отримання

інформаційної переваги над супротивником. Застосування потенціалу інформаційних воєн, як правило, означає «протиборство між державами в інформаційному просторі»¹. Поширення інформаційних воєн пояснюється можливістю забезпечення досягнення політичних цілей завдяки проведенню глобальних (стратегічних) політико-психологічних операцій з метою формування відповідної вигідної суб'єкту системи поглядів шляхом обробки населення країни (території) впливу та інших країн.

У більшості підходів до інформаційної війни зазвичай чітко визначена її складова, пов'язана з обороною. Поняття її початку і закінчення застосовується лише для окремих операцій, лінія фронту не визначена, а наступ описується окремими моделями. Успіх проведених інформаційних операцій не має прямого зв'язку зі співвідношенням військових потенціалів сторін. Забезпечення інформаційної безпеки у сфері державного та муніципального управління ґрунтується на детальному аналізі їх структури та змісту, а також інформаційних процесів і особливостей їх використання за допомогою відповідних технологій. При цьому визначальними чинниками при розробці засобів інформаційної зброї стають індивідуальні особливості людини та соціуму. Для того, щоб змодельювати поведінку людини (суспільства), необхідно знати саме ці особливості та переваги. Варто зазначити, що інформаційна боротьба стає тим чинником, що впливає на саму війну, її початок, хід і результат. Це підтверджується агресією Росії проти України. Виходячи з цього, розробка концепції системи інформаційно-аналітичного забезпечення в умовах міждержавного протистояння є актуальною проблемою для безпеки України.

Інформаційна війна проявляється у таких аспектах: 1) тенденційне викладення фактів, упереджене висвітлення певної інформації, що стосується тих чи інших подій за допомогою цілеспрямовано підібраних (зазвичай, вирваних із контексту) правдивих даних; при цьому спеціально сформована інформація подається дозовано, з урахуванням зростаючого напружен-

ня; 2) дезінформування «від зворотного», що відбувається шляхом надання правдивих відомостей спотвореному вигляді чи в ситуації, коли вони сприймаються об'єктом як неправдиві. Внаслідок ужиття подібних заходів виникає ситуація, коли об'єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно, не готовий протистояти негативному впливу; 3) термінологічне «мінування», яке полягає у викривленні первинної, правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативно-прикладного характеру (йдеться, наприклад, про спотворення Росією, у зв'язку з анексією Криму та окупацією частини Донбасу, принципів міжнародного права, пов'язаних із застосуванням права вето, відшкодуванням заподіяної шкоди, ідентифікацією військовополонених, застосуванням миротворчих сил ООН та ін.); 4) «сіре» дезінформування, що передбачає використання синтезу правдивої інформації з дезінформацією та «чорне» дезінформування, яке передбачає використання переважно неправдивої інформації.

Зазначені аспекти дають змогу зрозуміти, що політичні технології досить часто використовуються в сучасних реаліях у створенні інформаційно-політичного протиборства та інформаційних атак в геополітичному масштабі. При стратегічному веденні такої війни традиційні кордони розмиваються, лінія фронту відсутня (або, принаймні, не обмежується лінією зіткнення в рамках певної території, поширюючись на всю країну щодо якої застосовується агресія).

Мартін Лібікі — один із провідних теоретиків у інформаційній галузі — визначає 7 форм інформаційної війни: 1) командно-управлінська (націлена на знищення каналів зв'язку між командуванням і виконавцями); 2) розвідувальна (збір важливої і захист власної інформації); 3) психологічна (пропаганда, інформаційна обробка населення, деморалізація); 4) хакерська (диверсійні дії та атаки проти ворога шляхом створення спеціальних програм); 5) економічна (інформаційна блокада й інформаційний імперіалізм); 6) електронна (спрямована проти

засобів електронних комунікацій — радіозв'язку, радарів, комп'ютерних мереж); 7) кібервійна (Лібікі відокремив кібервійну від хакерської війни, вбачаючи в «кібервоїні» істоту, яка селиться в систему і живе в ній)².

Прикладом цілеспрямованого спотворення громадської думки є інформаційне супроводження агресії Росії проти України, що включає: дестабілізацію ситуації в державі чи її окремих регіонах; активізацію кампанії проти політичного курсу правлячої еліти держави та окремих її лідерів різними міжнародними установами; формування негативних суджень про воєнно-політичне керівництво України та про те, що хаотичні бойові дії призводять до невиправданих жертв серед сил АТО; поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до керівництва; ініціювання антидемпінгових кампаній та іншого роду скандальних судових процесів та ін. Тобто Росією в її інформаційній війні проти України застосовується широкий спектр засобів, які українські вчені В. В. Балабін, І. В. Замаруєва та І. В. Пампуха всебічно охарактеризували ще до початку конфлікту, аналізуючи необхідні складові воєнної безпеки держави³.

Зміна інформації з метою викривлення сприйняття реальності противником в умовах інформаційної війни досягається різними технологіями, включаючи комп'ютерні програми для редагування текстів, графіків, відео- і аудіоінформації з метою надання їм необхідної форми, яка буде представлена противнику. Поступ новітніх технологій дозволив розширити існуючі методи боротьби за політичний простір. Зазначені технології передбачають паралізування центрів управління протистоящою стороною з метою входження в системи прийняття рішень. Розвиток мережевих інформаційних структур та поява віртуального простору змусили переглянути організацію та захист політичного простору в сучасній геополітичній та інформаційній пропаганді. Театр ведення сучасної інформаційної війни прослідковується від секретного кабінету до домашнього комп'ютера, смартфона⁴.

Спростування, заперечення і знищення інформації — невід’ємні складові перешкоджання одержанню ворогом повної достовірної інформації. Щоб захиститися від інформаційної війни, необхідно застосовувати такі ж методики, які використовує противник: знати його інфраструктуру, знищувати її; забезпечувати належний захист інформації; попереджувати введення викривленої інформації в потоці правдивих фактів і даних; протидіяти спростуванню, запереченню і знищенню інформації і вчасно та якісно реагувати на всі прояви війни. Для цього необхідно насамперед мати національну концепцію інформаційної безпеки. В науковій літературі й політичній практиці зазначена протидія отримала назву «асиметричної стратегії», яка «в сучасних умовах означає постійний, активний системний тиск на «вразливі місця» супротивника, здатність організовувати свою діяльність і мислити відмінним від опонента чином задля максимізації власних переваг і використання вразливих місць, захоплення ініціативи чи забезпечення простору для маневрування»⁵.

Усі війни покликані змінити поведінку супротивника/опонента, але для цього в них є різний інструментарій. Кожен тип війни спрямований на власний тип простору. Звичайна війна — на фізичний, інформаційна — на інформаційний, смислова — на когнітивний. Сьогодні саме інформаційна війна найчастіше використовується і новини, які подаються в зумовленому її завданнями ракурсі, непросто відфільтрувати. Звідси необхідно на науковому і практичному рівнях виробити чіткі засоби протистояння пропаганді та технологіям, які ведуться проти суспільства. Розвинені країни саме на цьому останнім часом зосереджують свої зусилля. Так, у Великій Британії проблемами інформаційної боротьби займається департамент урядових комунікацій (The Government Communications Head-quarters). Під інформаційною боротьбою у цій країні розуміється цілеспрямована реалізація комплексу заходів щодо дезорганізації і встановлення контролю над системою державного та воєнного управління противника шляхом інформаційно-технічного й інформаційно-психологічного впливу на його інформаційні

ресурси, на суспільну та індивідуальну свідомість. Питаннями проведення інформаційних операцій у військовому відомстві займається група з координації військових інформаційних операцій, яка підпорядкована міністрові оборони. У Німеччині створений і активно функціонує Центр безпеки інформаційної техніки (штат 500 співробітників, річний бюджет 50 млн євро). За результатами його діяльності передбачається ведення наступальних і оборонних операцій інформаційної війни для досягнення національних цілей. Німецькі аналітики розглядають управління 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). 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. На думку американських політологів, технологія ведення інформаційних воєн несе основну загрозу для об'єкта впливу в тому, що країна-ціль може усвідомити цей вплив дуже пізно, а це дає певний вииграш тому, хто першим завдає удару. Звідси постає, що у ХХІ столітті фахівці з ведення інформаційного протиборства повинні бути зорієнтовані на створення фальшивої реальності. Бо, по суті, психологічні операції спрямовані на зміну ворожої орієнтації в короткому й довготривалому часових планах шляхом модифікування ворожого прийняття рішень та впливу на дії суперника.

Сучасні економічні відносини все більше набувають форми обміну знаннями, а не обміну товарами. За цих умов на чільне місце виступає доступ до інформаційних ресурсів, знань. Серйозну роль починають відігравати стратегічна розвідка, військові операції, дослідження і розробка нової інформаційної зброї. У розвинутих країнах здійснюється розробка засобів інформаційного протиборства з можливим противником як в

умовах воєнних конфліктів різної інтенсивності, так і в мирний час на стратегічному, оперативному, тактичному рівнях і в польових умовах з метою захисту національної інформаційної сфери від агресії і несанкціонованого втручання. У цих країнах концепція інформаційної війни є складовою воєнної доктрини, що обумовлює спеціальну підготовку особового складу і окремих підрозділів для проведення інформаційних операцій⁶.

Україна наразі має розробити стратегію інформаційної політики, якої немає і не було за всі роки незалежності, створити доктрину інформаційної безпеки та працювати над кібербезпекою. На сучасному етапі ефективна державотворча інформаційна політика у підсумку має сприяти вирішенню питання консолідації національного інформаційного простору України як інформаційної основи для розвитку українського народу, делегітимізації анексії Російською Федерацією суверенних українських територій та агресивних дій Росії щодо України. Необхідною умовою успішної реалізації зазначених напрямів є організація комплексу заходів у різних площинах — офіційній, дипломатичній, науковій, культурно-освітній, громадській.

Підґрунтям офіційного та дипломатичного рівнів інформаційної політики є науковий рівень, на якому для широкого загалу з наукових позицій обґрунтовується законність перебування вказаних територій у складі України, їх інтегрованість в українську історію, висвітлюються особливості й наслідки радянської та нинішньої імперської політики Росії стосовно України, розкривається специфіка суспільно-політичних процесів, пов'язаних з Революцією гідності та її наслідками для українського суспільства й держави. Результати таких наукових досліджень мають закласти фундамент для вироблення єдиного для українців концепту національної пам'яті, який стане основою для зміцнення національної свідомості й консолідації української нації.

Надзвичайно важливо в сучасних умовах звертати увагу на медіаграмотність в Україні. Ми живемо в добу інформації, яка поволі перетворюється в добу дезінформації. Зважаючи на інформаційний простір, який надає можливість оперативного

донесення інформації до користувача, потрібно вміти фільтрувати та грамотно визначати, що є важливим, а що ні, у що варто вірити, а що краще перевірити. Тому людині життєво необхідні критичне мислення і компетентність, що означає навички щодо перевірки сумнівної інформації. На національному рівні існує потреба забезпечення захисту національного інформаційного простору через ухвалення дієвих нормативно-правових актів, спрямованих на захист інформації в інформаційно-комунікаційних системах. Потреба в цьому зумовлена поширенням інтернет-послуг, їх доступністю для надто великої кількості користувачів. Це пов'язано також і з тим, що останніми роками виробляється багато досить досконалих засобів безконтрольного зняття та поширення інформації. Робиться це також за допомогою новітніх інформаційних технологій, що потужно розвиваються і вдосконалюються.

Забезпечити інформаційну безпеку неможливо через тотальну утаємниченість чи певні обмеження. Варто застосовувати апробовані засоби координації роботи з інформаційної безпеки, методики захисту особистості, суспільства, держави в інформаційному середовищі. Найважливішим напрямом протидії інформаційній експансії геополітичних супротивників України є створення інформаційно-психологічних підрозділів для забезпечення психологічної безпеки особистості, суспільства, держави. Їх основне завдання — розробка і здійснення стратегічних та оперативних заходів із попередження і нейтралізації негативного інформаційно-психологічного впливу на державному, регіональному і місцевому рівнях.

Зростання впливу інформаційних чинників, що обумовлено інформатизацією суспільства, об'єктивно вимагає ефективного функціонування системи інформаційно-психологічного забезпечення національної безпеки, об'єктами впливу якої мають бути інформаційно-психологічне середовище суспільства, інформаційні ресурси, психіка і поведінка політичної еліти, системи формування суспільної свідомості й думки та прийняття політичних рішень. Така система забезпечить захист психіки населення і військовослужбовців України від деструк-

тивного інформаційно-психологічного впливу, протидіятиме спробам маніпулювати процесами сприйняття інформації з метою відстоювання національних інтересів України в інформаційному просторі. Політика цілеспрямованого впливу на суспільну думку передбачає знання настроїв широких народних мас, реального стану справ. Постійний моніторинг ставлення українського суспільства до найважливіших проблем національної безпеки дасть змогу захистити психіку населення від негативного інформаційно-психологічного впливу⁷.

Маніпуляція суспільною думкою є однією із серйозних проблем сучасного політичного життя. Розширення її масштабів веде до деградації суспільства. Від маніпуляції слід відрізнити цілеспрямоване управління суспільною думкою, особливо в умовах надзвичайних ситуацій, для того щоб уникнути паніки серед населення. Стратегія формування позитивної для України суспільної думки в умовах збройного конфлікту має стати довгостроковою програмою дій в інформаційному середовищі. Зазначена стратегія повинна включати: оперативне розповсюдження достовірної, повної та об'єктивної інформації; підготовку і розповсюдження у ЗМІ готових інформаційних, довідкових і роз'яснювальних матеріалів із метою цілеспрямованого просування інформації, в якій зацікавлені державна влада і силові структури; оцінку реакції суспільства на діяльність державної влади і силових відомств; соціальну взаємодію різних суб'єктів, що у своїх діях керуються визначеними державною стратегією принципами і стандартами.

Таким чином, інформаційна війна сама по собі є не менш складною, ніж традиційна війна. Вона передбачає застосування різних стратегій, засобів, зброї та оборонних технологій. Глобальна інформатизація веде до створення єдиного інформаційного простору. Наше життя повністю залежить від інтенсивності інформаційного обміну. Ще декілька років тому комп'ютерні мережі та мережі передачі даних вважалися полем битви майбутнього, тепер — це сьогодення⁸. Протидія інформаційній агресії, інформаційному терору стає можливою і результативною у разі використання насамперед таких важе-

лів, як: більш широке залучення усіх засобів масової інформації до боротьби з негативними проявами в суспільстві, особливо тими, що спричиняють загрози національній безпеці⁹; неухильне забезпечення прав громадян на свободу слова, доступ до інформації; попередження будь-якого, не передбаченого правом, втручання державних органів влади, органів місцевого самоврядування у діяльність засобів масової інформації, застереження від можливих дискримінацій в інформаційній сфері¹⁰; посилення інформаційного суверенітету України та забезпечення належного захисту національного інформаційного простору; удосконалення державного регулювання та встановлення цивілізованого контролю за діяльністю інформаційної сфери шляхом поліпшення політико-правових, фінансово-економічних та організаційних засад її функціонування.

1. Рижков М. Інформаційна війна. *Політична енциклопедія*. Редкол.: Ю. Левенець (голова), Ю. Шаповаленко (заст. голови) та ін. Київ: Парламентське видавництво, 2012. С. 298. 2. Libicki M. Conquest in cyberspace. *National security and information warfare*. Cambridge, 2007. P. 88; 3. Балабін В. В., Замаруєва І. В., Пампуха І. В. Концептуальні засади захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби як складової воєнної безпеки. *Вісник КНУ імені Тараса Шевченка. Військово-спеціальні науки*. 2009. № 22. С. 30–33. 4. Лібікі М. Що таке інформаційна війна? URL: <http://viysko.com.ua/technologie-vojen/martin-libiki> — shho-take-informacijna-vijna/. 5. Горбатенко В. Асиметрична стратегія як відповідь на виклики системі європейської безпеки. *Studia Politologica Ucraino-Polona*. Випуск 6. Житомир-Київ-Краків: Вид. О. О. Євенок, 2016. С. 62. 6. Аналітична доповідь Національного інституту стратегічних досліджень до позачергового Послання Президента України до Верховної Ради України «Про внутрішнє і зовнішнє становище України у сфері національної безпеки». Київ: НІСД, 2014. С. 45–51. 7. Хорошко В. О., Хохлячова Ю. Є., Чирков Д. В. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України № 387/2015. Київ: ПВП «Задруга», 2013. С. 15. 8. Медвідь Ф. М. Національна безпека України в умовах формування європейської системи колективної безпеки. *Україна в нових реаліях: політичні, економічні та правові орієнтири розвитку*: зб. наук. праць за мате-

ріалами II Міжнародної науково-практичної конференції, 17 травня 2011 року / Національний університет ДПС України, НДІ фінансового права. Київ: Алеута, 2011. С. 93. **9.** Смолянюк В. Ф. Національні інтереси України: еволюція в політичному часі. *Інститут президентства України в системі державної влади України*: матеріали наукової конференції. Київ: ВПЦ «Київський університет», 2014. С. 93. **10.** Гнасевич Н. В., Рудакевич О. М. Вплив політичної пропаганди в інформаційно-психологічних операціях: принципи, форми та засоби впливу. *Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід*: матеріали II Міжнародної науково-практичної конференції, м. Тернопіль, Тернопільський національний економічний університет, 21–22 квітня 2017р. Тернопіль: Економічна думка, 2017. С. 37.

Kalinichenko Bogdan. Defining directions of the formation strategy of resisting the information war

The characteristic features of information warfare at the present stage have been elucidated, and the defining directions for the formation of a strategy to counter its means have been formulated. Examples of improving the means of information warfare at the leadership level of the leading countries of the world are given. The specificity of the destructive influence of information technologies in the context of the annexation of the Crimea and the occupation of a part of Donbass by the Russian Federation is shown. The possibilities of the state to strengthen national security in the conditions of external aggression, supported by information warfare technologies, are traced.

The growth of the influence of informational factors caused by the informatization of society objectively requires the effective functioning of the information-psychological security of the national security, the objects of influence of which should be the information-psychological environment of society, information resources, the psyche and behavior of the political elite, the system of formation of social consciousness thinking and making political decisions. Such a system will ensure the protection of the mentality of the population and servicemen of Ukraine from destructive information and psychological influence, will counteract attempts to manipulate the processes of perception of information in order to defend the national interests of Ukraine in the information space. The policy of purposeful influence on public opinion involves knowledge of the mood of the broad masses of the people, the real state of affairs. Constant monitoring of the attitude of Ukrainian society towards the most important problems of national security will help protect the psyche of the population from negative informational and psychological influence.

Manipulation of public opinion is one of the serious problems of modern political life. Expansion of its scale leads to the degradation of society. From manipulation it is necessary to distinguish purposeful management of public

opinion, especially in conditions of emergency, in order to avoid panic among the population. The strategy of forming a positive public opinion for Ukraine in an armed conflict must become a long-term program of action in the information environment. The said strategy should include: prompt dissemination of reliable, complete and objective information; preparing and disseminating in the media of ready information, reference and explanatory materials for purposeful promotion of information in which interested state authorities and power structures; an assessment of the reaction of society to the activities of state power and law enforcement agencies; social interaction of different subjects, which in their actions are guided by certain principles and standards of the state strategy.

Thus, the information war itself is no less difficult than the traditional war. It involves the use of various strategies, weapons, weapons and defense technologies. Global informatization leads to the creation of a single information space. Our life depends entirely on the intensity of the information exchange. A few years ago, computer networks and data networks were considered the battlefield of the future, now it's a present. Countering informational aggression, information terror becomes possible and effective in case of use of such instruments as: wider involvement of all mass media in combating negative manifestations in society, especially those that pose threats to national security; the steady guarantee of citizens' rights to freedom of speech, access to information; prevention of any non-stipulated law, interference of state authorities, local governments in the activities of mass media, warnings against possible discrimination in the information sphere; strengthening the information sovereignty of Ukraine and ensuring the proper protection of the national information space; improvement of state regulation and establishment of civilized control over the activity of the information sphere by improving the political-legal, financial-economic and organizational principles of its functioning.

Key words: political strategy, information war, asymmetric strategy, national security, information space, information technology.