ментів тексту, що також не рекомендовано в ЕВ, оскільки сприймати такий текст з екрана доволі важко. Поширеною помилкою є недотримання правил складання: брак пробілів після крапки перед наступним словом і після ком.

Висновки. Підсумовуючи, зауважимо, що ЕНВ такого потужного провідного освітнього закладу технічного спрямування, яким є НТУУ "КПІ", вимагають серйозного доопрацювання відповідно до вимог, що висуваються до цього виду видань, зафіксованих у нормативних документах, зокрема ДСТУ 7157:2010. Крім того, хаотична ситуація, що склалася в оформленні та представленні ЕНВ, потребує нагального вироблення в освітньому середовищі спільних вимог до ЕНВ, що й відображено в Положенні про електронні наукові та навчальні видання НТУУ "КПІ". Відомо, що аналогічні документи розробили фахівці Львівської політехніки та інших навчальних закладів, але з урахуванням власної специфіки. Було б доцільно, аби наявні положення склали основу загальнодержавного нормативного документа, стандарту, який би регламентував діяльність у царині електронного навчального простору і містив єдині вимоги до ЕНВ. Такий підхід сприятиме спрощенню роботи з цифровими підручниками, допоможе авторам, яким доводиться самотужки визначатися із термінологією, форматом та виглядом електронного навчального видання, зробить освітній процес більш ефективним та результативним завдяки використанню серед студентства високоякісного продукту сучасних технологій — ЕНВ.

Список використаної літератури

1. *Bohn R. E.* How Much Information? 2009. Report on American Consumers / R. E. Bohn, J. E. Short. — 2009. — Mode of access: http://hmi.ucsd.edu/pdf/HMI_2009_ConsumerReport_Dec9_2009.pdf. — Title from the screen.
2. *Bush V.* As We May Think // Atlantic Montly. — 1945. — № 7. — P. 101—108.
3. *Вершинская О. Н.* Информационно-комуникационные технологии и общество / О. Н. Вершинская. — Москва : Наука, 2007. — 203 с.
4. *ДСТУ 3017—95.* Видання. Основні види. Терміни та визначення. — Чинний від 1996—01—01 : [затв. наказом Держстандарту України від 23.02.95 № 58]. — Київ : Держстандарт України, 1995. — 47 с.
5. *ДСТУ 7157:2010.* Інформація та документація. Електронні видання. Основні види та вихідні відомості. — Чинний від 2010—07—01. — Київ : Держспоживстандарт України, 2010. — 18 с.
6. *Електронні* видання : довід. / Уклад. Т. Ю. Киричок. — Київ : НТУУ "КПІ", 2010. — 400 с.
7. *Энциклопедия* по печатным средствам информации. Технологии и способы производства / Гельмут Кипхан; Пер. с нем. — Москва : МГУП, 2003. — 1280 с.
8. *Эпштейн В. Л.* Антропоцентрическое информационное взаимодействие (вопросы терминологии) // Проблемы управления / В. Л. Эпштейн. — 2003. — № 1. — С. 28—33.
9. *Nelson T. H.* Complex information processing: a file structure for the complex, the changing and the indeterminate, Proceedings of the 20th National Conference, p. 84—100, August 24—26, 1965, Cleveland, Ohio, United States.
10. *Чепмен Н.* Цифровые технологии мультимедиа, 2-е издание : Пер. с англ. / Н. Чепмен, Д. Чепмен. — Москва : Издательский дом "Вильямс", 2006. — 624 с.

В статье рассмотрено состояние современных электронных учебных изданий, определены недостатки, сделан акцент на особенностях цифровых учебников (мультимедийность, гипертекстовость), которыми сегодня пренебрегают авторы. Обращено внимание на необходимость внедрения единых унифицированных требований к электронным учебным изданиям, разработки соответствующего стандарта.

The article deals with modern situation with electronic educational media, define the problems of their implementation. It was emphasized on the features of electronic media (multimedia, hypertext), which are neglected by authors today. It has been paid attention to necessity to introduce uniform requirements for electronic educational media and to create the standard.

Надійшла до редакції 15 вересня 2015 року

УДК 316.485.26:004

Оксана Сенченко,
аспірант кафедри видавничої справи та редагування НТУУ "КПІ"

Інформаційні війни як фактор трансформації соціальних систем

У статті здійснено аналіз загострення протиріч і посилення протиборств між різними соціальними системами, охоплюючи державні і недержавні суб'єкти, спричинених умовами ускладнення соціальної, економічної, політичної і культурної реальності. Розглянуто теоретичні розробки і практичні результати використання інформаційних засобів для трансформації соціальних систем, де лідерство безперечно і неподільно належить США.

Ключові слова: *військова дезінформація, інформаційна війна, інформаційне протиборство, інформаційна стійкість, кіберпростір, кібервійна, контррозвідка, оперативна безпека, операції в інформаційно-комунікаційних мережах, психологічні операції, радіоелектронна боротьба, соціальні системи, телекомунікаційні технології, фізичний вплив, фізична безпека.*

Вступ

Інформаційне протиборство (ІП) не є новим для людської цивілізації. Ще античні автори детально описували витончені агітаційні кампанії, за допомогою яких політики минулого намагалися деморалізувати супротивників, ввести їх в оману, змусити підкорятися своїй волі [1; 2]. Для реалізації цих завдань потрібно було вивчати суспільні системи країн — жертв агресії, їхнє матеріальне і духовне становище, розвиток промисловості та сільського господарства.

У XIX ст. видатний український письменник М. Гоголь зазначав: "...Мені хочеться знати, якого роду взагалі дух суспільства, і в якому стані його зіпсованість, і чим воно хворіє, якого роду люди його наповнюють, які класи переважають і які думки торжествують, якого роду розпуста найбільш в ходу нині?.. Прийшло нам рятувати нашу землю; гине вже земля наша не від нашестя двадцяти мов, а від нас самих. Поки не подумаємо про впорядкування душевного майна, — не встановиться впорядкування і земного майна... Настануть часи голоду і бідності, як у всьому народі, так і порізно у всякому...". Вже тоді Микола Васильович відчував потребу захисту інформаційного простору держави і розумів багатовекторність інформаційних війн.

Значно раніше, в VI столітті до нашої ери, відомий китайський філософ і теоретик війн Сунь Цзи першим узагальнив досвід інформаційного впливу на супротивника. Вчений пояснив важливість володіння інформацією і прийомами дезінформації для маніпулювання діями ворога: "Якщо я покажу супротивнику яку-небудь форму, а сам цієї форми не матиму, я збережу цілісність, а супротивник розділиться на частини" [3].

Наведемо деякі з його настанов ведення інформаційної війни:

— роздрібнюйте все добре, що є в країні вашого супротивника;

— втягуйте видатних діячів супротивника у злочинні дії;

— підривайте престиж керівництва супротивника й виставляйте його в потрібний момент на ганьбу громадськості;

— перешкоджайте всіляко нормальному постачанню військ і підтриманню в них порядку;

— робіть все можливе, щоб знецінити традиції ваших ворогів і підірвати їхню віру до власних богів;

— будьте щедрими на пропозиції й подарунки для купівлі інформації та спільників.

Наведені відомості яскраво свідчать, що інформаційні війни точаться у світі принаймні останні дві з половиною тисячі років [4].

У нинішній час, що має визначення "століття інформаційних технологій", невід'ємними компонентами систем управління державою, економікою, фінансами і обороною є інформаційні та комунікаційні системи. Їхнє впровадження веде до створення єдиного світового інформаційного простору, що вимагає високого науково-технічного і промислового потенціалу, а також відповідного культурно-освітнього рівня суспільства.

Очевидно, якщо одна зі сторін протиборства має потужніші інформаційні можливості, вона ефективніше й скоріше досягне мети. Водночас країни-аутсайдери процесу інформатизації можуть опинитися в умовах соціальної й економічної нестабільності. Така ситуація здебільшого призводить до протистояння розвинених держав і решти світу. Саме тому провідні зарубіжні країни використовують технології інформаційної боротьби для досягнення світового панування [5].

Проведений аналіз воєн і збройних конфліктів переконливо доводить, що інформаційна інфраструктура країни — жертви агресії є однією з основних цілей під час ведення бойових дій, а сторона, що програє інформаційне протиборство, неминуче зазнає поразки не лише в сучасній високотехнологічній війні, а й у локальних збройних зіткненнях.

Отже, інформаційна безпека зокрема є невід'ємною частиною національної безпеки загалом будь-якої держави, а інформаційне протиборство — складовою частиною збройного протистояння.

Нині провідні держави світу приділяють значну увагу розвиткові теорії та практики інформаційного протиборства, створенню його сил і засобів [6].

Сьогодні проти України ведеться інформаційна війна. З одного боку це інформаційна агресія Російської Федерації (РФ), з іншого — Сполучених Штатів Америки (США) і країн Європейського Союзу (ЄС). Очевидно, що під таким впливом відбувається трансформація українського суспільства, одна частина якого обирає шлях до РФ, а інша — до ЄС і США. Переглядається історія.

Для завойовників, що претендують на світове панування, насамперед потрібно знищити державність. Чому? Відповідь на це запитання міститься у фундаментальній праці "Нетократія. Нова правляча еліта і життя після капіталізму" [7]. Нетократія, тобто влада мережі, розглядається в контексті підготовки до встановлення нового світового ладу. Наведемо цитату з цього доктринального документа: "Перехід від старої до нової парадигми здійснюється поетапно.

На першому етапі руйнування держави призводить до утворення все більшої кількості субкультур, "племен" із вужчою ідентичністю і лояльністю.

На другому етапі держава, що занепала, замінюється наддержавними утвореннями в політиці, економіці та культурі.

Нинішня ситуація виносить на порядок денний стару як світ ідею створення глобальної держави" [8].

Майже 400 найпотужніших мозкових центрів США ведуть роботу з моніторингу стану й моделювання ситуації в соціальних системах різних країн світу, зокрема і в Україні. Вони спираються на базові дані, які збирають численні "незалежні" організації, враховують економічну ситуацію, фінансують екстремістські структури, під прапором демократії використовують людей, які вболівають за країну, і організовують революції [9].

Термін "інформаційна війна" уперше використано в директиві міністра оборони США від 21 грудня 1992 р. DOD S 3600.1. Це поняття було вжито у вузькому значенні й розглядалося як різновид радіоелектронної боротьби. У подальшому до обігу увійшов термін "стратегічна інформаційна війна (інформаційне протиборство)", яка визначалася як протистояння з використанням державного глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій і зміцнення впливу на власний інформаційний ресурс [10].

США — лідер розробки і використання інформаційної зброї

Розвиток інформаційних і телекомунікаційних технологій змінив не лише засоби збройної боротьби, а стратегію й тактику ведення сучасних воєн, виникли концепції, що враховують чинники інформаційної вразливості сторін. Останнім часом у наукових публікаціях щодо інформаційної зброї навіть застосовується термін "зброя масових руйнувань". Роль лідера у її використанні, безперечно, належить Сполученим Штатам Америки, які сформулювали основи стратегії інформаційного протиборства ще 1992 р. [11].

Динаміка розвитку інформаційних і телекомунікаційних технологій, що прискорюється, надання широких можливостей для підвищення ефективності інформаційної інфраструктури постіндустріального суспільства створюють чимало проблем у різноманітних сферах світової політики, передусім у галузі міжнародної та національної безпеки. Зростає залежність військової діяльності від якості функціонування інформаційно-комунікаційних мереж та інформації, яка в них циркулює.

Завдяки стрімкому поширенню інформаційних і телекомунікаційних технологій відбувається концентрація сил (політичних, економічних, військових) у кількох світових

центрах впливу, які за певних умов можуть виявитися потенційними опонентами Америки. Закономірно, що підтримку лідерства у цій сфері американське військово-політичне керівництво розглядає як найважливіший компонент глобальної інформаційної переваги, плануючи, відповідно, істотні технологічні трансформації [12].

Розвиток теорії інформаційних війн у США

Сьогодні "найдосконалішу" теорію інформаційного протиборства розроблено у США, політичні сили цієї держави мають значний вплив на українське суспільство. Отже, доцільно дослідити аспекти формування ідеології та структур ведення інформаційних війн світового лідера у цій галузі.

Доктринальне опрацювання питань ведення інформаційного протиборства в США почалося після закінчення війни в Перській затоці (1991), в якій американські збройні сили вперше застосували новітні інформаційні технології. У директиві Міністерства оборони (МО) TS 3600.1, що набула чинності 21 грудня 1992 р., було сформульовано основні положення стратегії інформаційного протиборства. Вона визначалася як самостійний вид оперативного забезпечення (комплексна інформаційна дія на системи державного і військового управління супротивника) і складалася з п'яти основних елементів: психологічні операції; протидія розвідці супротивника і гарантування безпеки дій військ; введення супротивника в оману; радіоелектронна боротьба; знищення пунктів управління ворога і його систем зв'язку [13].

У січні 1995 р. корпорація "RAND" отримала замовлення на проведення дослідження щодо визначення ролі й місця інформаційного протиборства в національній військовій стратегії США. Результати робіт було викладено у звітах MR-661-OSD "Stranegic information Warfare. A new face of War" (1996), MK-964-OSD "Strategic information Warfare Rising" (1998) і MR-963-OSD "The Day After — in the American Strategic infrastructure" (1998) [14]. Подальші дослідження із цих питань було оформлено як офіційне видання так званих єдиних доктрин. У лютому 1996 р. Комітет начальників штабів (КНШ) ввів у дію "Доктрину боротьби з системами управління" [15].

У грудні 1998 р. набула чинності "Об'єднана доктрина інформаційних операцій", згідно з якою інформаційна операція — це комплекс заходів із маніпулювання даними для досягнення й утримання глобальної переваги над супротивником через вплив на інформаційні процеси, що відбуваються в системах управління [16].

У документі наголошувалося, що ефективність заборони, проектування сили й інших стратегічних концепцій значною мірою залежать від здатності впливати на рішення урядів інших країн. Наприклад, під час криз інформаційні операції покликані допомогти утримати супротивника від проведення акцій, що завдають збитків США та їхнім союзникам.

У доктринах було визначено мету, завдання й основні принципи інформаційного протиборства, обов'язки керівних органів і посадовців щодо його планування та організації в мирний час і в умовах кризового стану. Крім того, викладено вимоги до розвідувального забезпечення інформаційних операцій, а також до підготовки особового складу, що забезпечує їхнє планування і проведення. Ефективне інформаційне протиборство мало забезпечити можливість нав'язати супротивникові хибне бачення оперативного становища, змусити до ведення військових дій в несприятливих для нього умовах. Це досягається головним чином через проведення комплексу заходів, що дозволяють, з одного боку, зруйнувати процес ухвалення рішень супротивника, а з іншого — обробляти інформацію у власній системі управління ефективніше і швидше, ніж це робить ворог.

Республіканці, що прийшли до влади на початку XXI ст., значно посилили увагу до проблеми протиборства в інформаційному просторі. Їхні зусилля було спрямовано передусім на розробку стратегії інформаційного контролю і створення в Міністерстві оборони спеціального підрозділу, який би відповідав за ведення такої боротьби [17].

У лютому 2003 р. президент Дж. Буш-молодший схвалив "Національну стратегію безпеки кіберпростору", яка, по суті, була першою доктринальною ініціативою, що визначила потребу координації та зосередження зусиль усіх федеральних відомств у справі захисту національного інформаційного простору [18]. У документі, зокрема, наголошувалося і на необхідності посилити координацію Міністерства оборони і національного розвідувального співтовариства в реагуванні на кіберзагрози. Особливий акцент зроблено на тому, що американське керівництво залишає за собою право відповідати на кібератаки із застосуванням усіх засобів і можливостей військового компонента національної інформаційної інфраструктури.

Для розвитку цього доктринального документа у жовтні 2003 р. опубліковано "Дорожню карту інформаційних операцій" [19], в якій було визначено, що національна інформаційна інфраструктура — це оперативний центр тяжіння. Також зазначено, що Міністерство оборони координує зусилля федеральних відомств у боротьбі з кібератаками супротивника на автоматизовані центри державного і військового управління. Реалізуючи окреслені завдання, було розпочато опрацювання і введення основних положень стратегії інформаційного протиборства до складу військової доктрини, а також формування структур для управління операціями в інформаційному просторі.

Комітет начальників штабів, зі свого боку, у лютому 2006 р. ухвалив документ "Інформаційні операції", в якому викладено погляди американського військового керівництва на їхню підготовку і проведення [20]. Відповідно до засад документа, інформаційні операції є комплексом заходів впливу на людські й матеріальні ресурси супротивника, що передбачає ускладнення або блокування ухвалення правильного рішення з його боку й одночасний захист власних інформаційно-комунікаційних мереж і комп'ютерних систем.

Такі операції охоплювали п'ять основних складників: радіоелектронну боротьбу (electronic warfare), психологічні операції (psychological operations), операції в інформаційно-комунікаційних мережах (computer network operations), військову дезінформацію (military deception), оперативну безпеку (operations security). Було визначено й допоміжні елементи інформаційних операцій, потрібні для досягнення успіху у мирний і воєнний час, зокрема: інформаційна стійкість (information assurance), фізичний вплив (physical attack), контррозвідка (counter intelligence), фізична безпека (physical security), збір і використання даних видової розвідки (combat camera), зв'язок із громадськістю (public affairs), цивільно-військові операції (civil-military operations), підтримка з боку структур Міністерства оборони публічної дипломатії (defense support to public diplomacy).

У положеннях директиви Міністерства оборони D 3600.1, введеної в дію 14 серпня 2006 р., уперше чітко визначено основні завдання і функції інформаційних операцій, що означають комплексне застосування засобів радіоелектронної боротьби, операцій в інформаційно-комунікаційних мережах, психологічних дій, військової дезінформації та оперативної безпеки [21]. У документі зазначено, що інформаційні операції проводяться "з метою інформаційного впливу, введення в оману, порушення роботи комп'ютерних систем, спотворення, дезорганізації баз даних і позбавлення супротивника можливості їхнього використання, вилучення інформації з комп'ютерних систем і баз даних супротивника

при одночасному забезпеченні захисту власної інформаційної інфраструктури". Документ регламентував застосування принципу розподілу інформаційних операцій на три категорії: атака на комп'ютерні мережі (computer network attack), захист комп'ютерних мереж (computer network defense), забезпечення доступу до комп'ютерних мереж супротивника й їхнє використання у власних інтересах (computer network exploitation). Аналогічними директивами було забезпечено усі види збройних сил [22].

Адміністрація демократів, що прийшли до влади на початку 2009 р., продовжила активно розвивати стратегію інформаційного протиборства. Після інаугурації президент Б. Обама віддав розпорядження про проведення ретельного аналізу заходів федеральних відомств з організації комплексного ефективного захисту національних інформаційно-комунікаційних мереж, а також про розробку стратегії боротьби в інформаційному просторі. Згідно з офіційною заявою президента США "кібершпигунство і злочини в інформаційно-комунікаційних мережах мають тенденцію до зростання. Тому кібербезпека — найвищий пріоритет національної безпеки країни в XXI столітті" [23].

Ця заява збіглася з виходом у світ документа "Огляд політики в кіберпросторі", котрий президентові представили члени спеціальної комісії, які проводили аналіз стану справ у сфері захисту інформаційного простору. Огляд містив рекомендації з удосконалення безпеки національної інформаційної інфраструктури [24]. Зокрема, стверджувалося, що федеральні відомства занадто забюрократизовані й роз'єднані у діях у галузі кібербезпеки. Наголошувалося, що потрібно негайно виробити правові норми у сфері кібербезпеки для національної юрисдикції, відповідальності держав і порядок силового реагування на кіберзагрози.

Положення доповіді засвідчили, що підходи уряду США до збереження кібербезпеки не відповідають темпам зростання загроз. Відзначалося, що національна безпека майже повністю залежить від функціонування інформаційно-комунікаційних мереж, які забезпечують життєдіяльність усієї національної інфраструктури, насамперед федеральних відомств, що відповідають за оборону і безпеку. Відповідно до рекомендацій американських фахівців, пропонувалося створити пост координатора із кібербезпеки, який звітував би безпосередньо президенту.

Ці пропозиції майже повністю збіглися з рекомендаціями експертів з вашингтонського Центру стратегічних і міжнародних досліджень, визначеними у грудні 2008 р. у доповіді "Забезпечення безпеки кіберпростору для 44 президента США" [25].

У березні 2010 р. стало відомо про основні напрями реалізації програми підвищення ефективності протидії кібератакам на американські інформаційно-комунікаційні мережі та бази даних. Роботи велися відповідно до "Ініціативи всеосяжної національної кібербезпеки" (The Comprehensive National Cyber Security Initiative) під керівництвом Ради національної безпеки США [26]. До її виконання залучено всі федеральні відомства США, а також уряди штатів, відповідальні за безпеку інформаційного простору.

До "Ініціативи" увійшли документи, розроблені ще за часів правління республіканської адміністрації: Президентська директива із забезпечення національної безпеки № 54 (National Security Presidential Directive 54) і Президентська директива із забезпечення внутрішньої безпеки № 23 (Homeland Security Presidential Directive 23), видані в січні 2008 р.

"Ініціатива" передбачає подальше вдосконалення моніторингу роботи федеральних інформаційно-комунікаційних мереж, а також введення в дію програми "Надійне інтернет-з'єднання", націленої на зменшення кількості точок підключення комп'ютерних систем федеральних відомств і установ до зовнішніх інформаційно-комунікаційних мереж для своєчасного виявлення випадків вторгнення. Витрати на реалізацію завдань цього документа становитимуть від 40 до 100 млрд дол. Усього в ньому передбачено 12 основних напрямів робіт, пов'язаних із захистом національного інформаційного простору і фіксацією спроб несанкціонованого проникнення.

Одним із важливих завдань, визначених в "Ініціативі", є якнайповніший захист баз даних від вірогідних кіберзагроз. Його запропоновано вирішувати через розширення технічних і оперативних можливостей федеральних відомств, відповідальних за національну безпеку. Ще один напрям "Ініціативи", що реалізується, — комплекс заходів з якісного поліпшення системи підготовки фахівців у галузі інформаційної безпеки. Заплановано підвищити ефективність координації фінансування з федерального бюджету наукових досліджень і дослідно-конструкторських розробок у цій сфері.

Передбачено формування стратегічних підходів для ефективної протидії усім видам кіберзагроз. Для цього потрібно провести комплекс заходів: від модернізації державних структур, що відповідають за інформаційну безпеку, до визначення місця і ролі федерального уряду в цьому процесові задля забезпечення безперервного контролю над функціонуванням національних інформаційно-комунікаційних мереж і управління ними як єдиним комплексом.

У травні 2011 р. президент Б. Обама затвердив "Міжнародну стратегію для кіберпростору", яка декларує комплексний підхід військово-політичного керівництва до політики в глобальному інформаційному просторі [27]. У документі наголошено, що інформація і національна інформаційна інфраструктура загалом — це стратегічний ресурс, і в XXI ст. держава має вкрай обмежені можливості управління і контролю в кіберпросторі.

Особливий акцент американські фахівці роблять на міжнародній співпраці у сфері інформаційної безпеки національної інфраструктури. Провідна роль в її забезпеченні належить Міністерству оборони США.

Серед основних політичних пріоритетів розвитку національної інформаційної інфраструктури, разом із покращенням національної економіки, захистом інформаційно-комунікаційних мереж, посиленням законодавства в інформаційній сфері, розширенням міжнародної співпраці, створенням ефективної структури для управління Інтернетом і забезпеченням фундаментальних принципів свободи в мережі, важливе місце відведено військовому компоненту. Уперше в офіційних документах особливу увагу приділено інформаційному стримуванню потенційних супротивників. При цьому вважається, що структури колективної безпеки (приміром, НАТО) дозволять ефективно застосовувати стратегію інформаційного стримування щодо держав-опонентів і недержавних об'єднань; також акцентовано на потребі вироблення норм міжнародного права в царині інформаційної безпеки.

Для виконання настанов цього доктринального документа Міністерство оборони видало "Стратегію Міністерства оборони з операцій в кіберпросторі", яку в липні 2011 р. представив, виступаючи в Університеті національної оборони, заступник міністра оборони У. Лінн [28]. Він наголосив: "США залишають за собою право відповідно до законів війни відповісти на кібератаки пропорційно у той час і в тому місці, які ми виберемо".

У "Стратегії" зазначено, що Пентагон розглядатиме кіберпростір як сферу оперативної діяльності (на додаток до чотирьох основних) і виокремлено п'ять стратегічних ініціатив, виконання яких дозволить Міністерству оборони США захистити національну інфраструктуру:

1. Визнання кіберпростору пріоритетною сферою оперативної діяльності.

2. Застосування "активного захисту" інформаційно-комунікаційних мереж і комп'ютерних систем.

3. Ефективна взаємодія Міністерства оборони США з іншими федеральними відомствами і приватними компаніями у сфері інформаційної безпеки.

4. Налагодження активної співпраці з союзниками і партнерами в контексті колективного захисту від кіберзагроз.

5. Збільшення фінансових і матеріальних ресурсів, спрямованих на розвиток науково-технічної бази кібербезпеки, а також на підготовку висококваліфікованих спеціалістів.

Загалом, із доктринальних документів, в яких визначено основні складники стратегії інформаційного протиборства, випливає, що Вашингтон декларує потребу відповідати сучасним вимогам національної оборони й безпеки та потенціалу ведення інформаційного протиборства. Акцентовано на зростанні ролі інформаційної зброї як найважливішого елементу планів ведення війн нового покоління. Відзначено, що залежність ефективності бойових дій від новітніх цифрових технологій неминуче веде до посилення вразливості усієї національної інформаційної інфраструктури, роблячи її складники пріоритетною військовою метою для супротивника. Принципові засади усіх документів полягають у потребі надійного всебічного захисту інформаційного простору й інформаційної інфраструктури загалом.

Сфери застосування інформаційної зброї

Під інформаційною зброєю американські фахівці розуміють сукупність спеціально організованого і структурованого інформаційного трафіку, який разом з новітніми інформаційними і телекомунікаційними технологіями дозволяє цілеспрямовано видозмінювати (знищувати, спотворювати, блокувати, копіювати) інформацію, долати системи захисту, обмежувати доступ законних користувачів, здійснювати дезінформацію, дезорганізовувати роботу технічних засобів, носіїв інформації, комп'ютерних систем й інформаційно-комунікаційних мереж [29]. Це арсенал засобів несанкціонованого доступу до інформації й виведення з ладу електронних систем управління супротивника. Передбачається, що засоби інформаційно-психологічної дії в змозі не лише завдати шкоди здоров'ю, а й призвести до блокування на неусвідомлюваному рівні свободи волевиявлення людини, втрати здатності до політичної, культурної й іншої самоідентифікації, до маніпуляцій суспільною свідомістю і навіть руйнування єдиного інформаційно-духовного простору.

Виникнення інформаційної зброї, в офіційному трактуванні, принципово змінює механізм ескалації збройних конфліктів, оскільки навіть її вибіркове застосування щодо об'єктів військової та цивільної інформаційної інфраструктури супротивника може завершити конфлікт ще на початковій стадії, без активних бойових дій. Володіння інформаційною зброєю забезпечує політичну і військово-стратегічну перевагу над державами, які не мають цього інструменту боротьби.

Як і ядерна, інформаційна зброя може використовуватися і для політичного тиску, і для стримування конфлікту. Згідно з оцінками впливових експертів, ефект цільової інформаційної дії на супротивника доцільно порівняти із застосуванням зброї масового ураження (ЗМУ), і загроза піддатися такій дії може стати важливим чинником стримування потенційного агресора. Ефективність цього процесу безпосередньо залежить від рівня технологічного розвитку і масштабу використання комп'ютерної техніки в інформаційних системах держави. Наприклад, комп'ютерну систему можна знищити фізично, або викрасти стратегічно важливу інформацію, або пошкодити програмне забезпечення через вірусну чи хакерську атаки.

Один із провідних американських фахівців у сфері інформаційного протиборства, професор Університету національної оборони М. Лібицький вважає, що в майбутньому інформація буде основним засобом стримування збройних конфліктів [30]. На його думку, єдина розвідувально-інформаційна інфраструктура, що складається з мережі космічних, повітряних, наземних і морських датчиків різного призначення, надасть можливість контролювати будь-яку військову активність на планеті, а отже, застосовувати превентивні заходи. В таких умовах, на думку науковця, дії потенційного супротивника будуть абсолютно прозорі для протилежної сторони і міжнародного співтовариства загалом. Відповідно, ворог втратить можливість провести власне військові приготування, оскільки глобалізація світових інформаційно-комунікаційних мереж дасть змогу паралізувати і блокувати його системи управління, завдавши значного збитку військовому потенціалу. М. Лібицький вирізнив сім основних форм інформаційного протиборства [31]:

- боротьба з системами управління;
- інформаційно-розвідувальна;
- електронна;
- психологічна;
- хакерська;
- кібернетична;
- економічна.

Боротьба з системами управління супротивника передбачає їхнє фізичне знищення і відсікання командних структур, руйнування комунікацій, що зв'язують системи управління з підрозділами. Цінність таких інформаційних операцій полягає в тому, що вони можуть виявитися особливо ефективними на ранніх стадіях розвитку конфлікту і сприяти досягненню швидкої перемоги над супротивником [32].

Інформаційно-розвідувальні операції припускають оперативний збір, опрацювання і доведення до кінцевого споживача максимально повної інформації про супротивника в режимі реального або близького до реального часу. Створення багаторівневої системи збирання даних дає можливість отримувати якнайширшу панораму ситуації в районі бойових дій і полегшує розподіл інформації між користувачами [33].

Електронна боротьба знижує інформаційні можливості супротивника. Відповідно, вона поділяється на:

- радіоелектронну (зокрема, через створення активних і пасивних перешкод), яка вважається головним напрямом;
- криптографічну (спотворення і ліквідація інформації);
- боротьбу з комунікаційними системами супротивника [34].

Психологічні операції є комплексом заходів із поширення спеціально підготовленої інформації для впливу на емоційний стан, мотивацію, аргументацію дій, ухвалення рішень і поведінку опонентів у напрямі, сприятливому для США й їхніх союзників. За масштабами вони можуть бути стратегічними, оперативними і тактичними й охоплюють чотири основні компоненти: підривання цивільного духу, деморалізацію збройних сил, дезорієнтацію вищого політичного та військового керівництва, війну культур. Основним інструментарієм ведення таких операцій є національні й транснаціональні засоби масової інформації, а також глобальні інформаційно-комунікаційні мережі, здатні впливати на світогляд, політичні погляди, правосвідомість, менталітет, духовні ідеали і ціннісні настанови окремої особистості й суспільства загалом [35].

Хакерська боротьба передбачає застосування програмних засобів (програмно-математична дія на інформаційно-комунікаційні мережі) і спрямована на використання, спотворення, підміну або знищення інформації, що міститься в базах даних комп'ютерів та інформаційно-комунікаційних мереж, а також на зниження ефективності функ-

ціонування або виведення з ладу комп'ютерів і комп'ютерних систем. Конкретні прийоми хакерської боротьби мають найрізноманітніший характер. Їхньою метою може бути і повне виведення з ладу комп'ютерних систем, й ініціація періодичних або визначених у часі порушень у роботі, вибіркове спотворення даних, інформаційного трафіку, доступ до таємної інформації, несанкціонований моніторинг роботи комп'ютерної системи тощо [36].

Кібернетична боротьба охоплює повний комплекс завдань і аспектів (організаційні, доктринальні, стратегічні, тактичні, технічні) ведення інформаційних операцій і нині є актуальною саме у військовій сфері. Поняття кібернетичної боротьби належить радше до організаційної форми інформаційного протиборства, ніж власне до боротьби з інформаційною інфраструктурою супротивника. Щобільше, цей різновид протистояння має на меті використання інформаційної інфраструктури супротивника для виконання власних завдань [37].

Економічна боротьба є комплексом методів і засобів інформаційної дії в економічній сфері. Розвиток технічних можливостей засобів зв'язку, трансляції й нагромадження інформації зумовив різке зростання мобільності капіталів, чутливості світових фінансово-економічних і соціальних процесів до інформаційних дій, а також до того, що економіка держави й її фінансова сфера стали важливою метою інформаційного впливу [38].

Необхідно "зняти" мотивацію націй до опору, позбавити їх історичної пам'яті, змінити сутність державної влади як системи управління, перетворивши її представників на "банду грабіжників", яка викликає роздратування й ненависть у населення. Ці дії також передбачають введення до управлінського апарату некваліфікованих людей без вищої освіти, котрі, проте, мають можновладних покровителів [39].

Керований хаос

Наукові досягнення виводять людей за межі ньютонівських концепцій в екзотичну теорію хаосу і самоорганізовану критичність. Нові напрями досліджень виникли упродовж останніх 30-ти років. У засадах цих концепцій викладено ідею, що структура і стабільність перебувають усередині видимого безладу і нелінійних процесів. Відколи наукові революції в минулому змінили сутність конфлікту, американські стратеги мають усвідомлювати зміни, що відбуваються [40].

Для населення країни, де впроваджено стратегію "керованого хаосу", очевидною є потреба зміни не лише політичної, а й економічної системи. Відповідно, до діла беруться радники США чи інших країн Заходу або власні експерти, які переконують уряд в тому, що реформи гальмують, оскільки ринок недостатньо вільний. Водночас вони посилаються на економічну "школу Чикаго", основоположником якої є М. Фрідман — ідеолог руху за необмежений капіталізм.

"Шокова терапія" Мілтона Фрідмана

Професор Чиказького університету запропонував використовувати широкомасштабний шок, кризу або керований хаос для миттєвого перетворення економіки на основі вільного ринку. Як тільки вибухає криза, запевняв М. Фрідман, потрібно діяти швидко, блискавично вносити незворотні зміни, поки охоплене кризою суспільство не оговтається і не повернеться до "тиранії статус-кво". За його словами, "лише криза — справжня або уявна — веде до реальних змін. Коли вона виникає, дії людей залежать від їхніх уявлень. І в цьому, вважаю, полягає наша головна функція: створювати альтернативи наявним стратегіям, підтримувати їхню життєздатність і доступність допоки політично неможливе не стане політично неминучим".

Науковець дав назву цій тактиці: економічна "шокова терапія". Відтоді впродовж десятиріч, коли уряди здійснювали радикальні програми переходу до вільного ринку, лікування шоком "раптово і відразу" або застосування "шокової терапії" було лише питанням вибору методу [41].

"Сповідь економічного вбивці"

Багато мешканців України не вірять у невидиму війну Сполучених Штатів Америки проти різних країн, зокрема й нашої. Проте є чимало свідчень саме американських громадян про методи цієї боротьби, одним з яких є офіційне зізнання Дж. Перкінса щодо продажності, брехні та зрадництва в найвищих ешелонах влади. "Приголомшлива річ, — зауважував Дж. Е. Мек, професор Гарвардського університету, лауреат Пулітцерівської премії. — Один із рідкісних випадків, коли людина, яка працювала в глибинах урядових імперських структур, ясно й однозначно розриває їхню внутрішню сутність. Ця книга, що вимагає від автора моральної стійкості, проникає у найглибші глибини".

Йдеться про видання "Сповідь економічного вбивці" Дж. Перкінса, яке в перекладі з англійської мови 2005 р. побачило світ завдяки московському видавництву "Претекст". Книга вийшла в Америці в кінці 2004 р., відразу стала бестселером як перша у світі автобіографічна розповідь про діяльність таємної групи професіоналів-економістів вищого рівня — "економічних убивць", — які працюють із вищими політичними й економічними керівниками країн, що цікавлять уряд США, для реформування їхньої економіки на користь американської "корпоратократії", урядових організацій, банків і корпорацій.

У передмові до російського видання доктор економічних наук, професор, лауреат премії "Кращі економісти РАН" Л. Фітуні зазначав: "З надзвичайною відвертістю Перкінс зізнається в належності до певної структури, пов'язаної з Управлінням національної безпеки США, у межах якої діють економічні вбивці. Їхнє завдання — підштовхувати уряди суверенних держав до проведення рекомендованого комплексу соціально-економічних реформ, що обіцяють модернізацію економіки, розвиток сучасного ринкового господарства, залучення прогресивних технологій завдяки іноземним інвестиціям. Ключовим елементом будь-якого мегапроекту такого спрямування є надмірні зовнішні запозичення, що витрачаються на придбання насамперед американських товарів і послуг".

Найвиразніша інформація про злочинну дію американської корпоратократії міститься на обкладинці книги. Це цитата з "Library journal" (США): "Джон Перкінс був таємно завербований Управлінням національної безпеки Сполучених Штатів. Пройшов підготовку з найбільш закритого фаху в галузі економічних диверсій. Офіційно — він співробітник впливової й потужної транснаціональної консалтингової фірми, що продає по всьому світові особливий товар — економічні реформи й демократичні перетворення…

Їхнє завдання — поневолювати країни й народи, нав'язуючи мегапроекти-пастки, які нібито забезпечують прискорення розвитку, а насправді обертаються введенням доти суверенних держав до складу нової глобальної імперії" [42]. І, додамо, — розвалом їхнього національного виробництва й зубожінням народу. Фактично йдеться про терористичну діяльність проти багатьох націй задля необмеженого збагачення купки олігархічних родин.

Серед наявних можливостей застосування інформаційної зброї надзвичайно ефективними є ті, що пов'язані з глобальним моніторингом економічної діяльності й тотальним контролем інформаційного трафіку. На тлі подальшого інтенсивного розвитку мережі Інтернет у США всеосяжна інформаційна обізнаність може виявитися надто дієвим інструментом.

Список використаної літератури

1. *Волковський Н. Л.* История информационных войн. Ч. 1. / Н. Л. Волковський. — Санкт-Петербург : Полигон, 2003. — 507, [2] с., [8] л. ил. — (Военно-историческая библиотека).
2. *Волковський Н. Л.* История информационных войн. Ч. 2. / Н. Л. Волковський. — Санкт-Петербург : Полигон, 2003. — 735 с., [8] л. ил. — (Военно-историческая библиотека).
3. *Сунь* Цзы. Трактат о военном искусстве / Сунь Цзы. — Москва : Воениздат, 1955. — 124 с.
4. *Зенгер Х. фон*. Стратагемы: о китайском искусстве жить и выживать. Знаменитые 36 стратагем за три тысячелетия / Х. фон Зенгер. — Москва : Прогресс : Культура, [1995]. — 379 с.
5. *Бжезинский З.* Великая шахматная доска: (господство Америки и его геостратегические императивы) / Збигнев Бжезинский. — Москва : Междунар. отношения, 1998. — 254, [1] с. — (Великое противостояние).
6. *Гродненский Н.* Четвертая мировая: США в войне за мировое господство / Николай Гродненский. — Минск : В. П. Ильин : Белорус. дом печати, 2004. — 347 с.
7. *Бард А.* Нетократия : новая правящая элита и жизнь после капитализма / Александр Бард и Ян Зодерквист. — [изд. 2-е, испр.]. — Санкт-Петербург : Стокгольм. шк. экономики в Санкт-Петербурге, 2004. — 252 с. — (Серия "Книги Стокгольмской школы экономики в Санкт-Петербурге").
8. *Вилко В.* Інформаційно-психологічне забезпечення Збройних сил США в локальних війнах і збройних конфліктах 1950—2000 рр. : (іст. аспект) : автореф. дис. ... канд. іст. наук / Вилко Володимир Миколайович ; Нац. акад. оборони України. — Київ, 2005. — 30 с.
9. *Петрик В.* Сучасні технології маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій : навчальний посібник / В. Петрик, В. Остроухов та ін. — Київ, 2006. — С. 196.
10. *Раскин А.* Информационное противоборство в современной войне / Раскин А. В., Тарасов И. В. // Информационные войны. — Москва, 2014. — № 4 (32). — С. 2—6.
11. *Владимиров А.* Технологии войны мирного времени: (Россия в условиях четвертой мировой) / А. Владимиров // Национальная безопасность и геополитика России. — Москва, 2003. — № 12. — С. 13—20.
12. *Попов И.* Война будущего: взгляд из-за океана: военные теории и концепции современных США / И. Попов. — Москва : Транзиткнига : АСТ : Астрель, 2004. — 443, [1] с. — (Великие противостояния : Америка против всех).
13. *Information* Warfare. Directive TS 3600.1. Washington D. C. : U. S. Department of Defense, 21 Dec. 1992.
14. *Почепцов Г.* Информационно-психологическая война / Г. Г. Почепцов. — Москва : Синтег, 2000. — 179 с. — (Серия "Информационные войны").
15. *Command* and Control Warfare. Joint Publication 3—13.1. Washington D. C. : Joint Chiefs of Staff, Feb. 1996.
16. *Joint* Doctrine for Information Operations. Joint Publication 3—13. Washington D. C. : Joint Chiefs of Staff, Dec. 1998.
17. *Graham B.* Bush Orders Guidelines for Cyber Warfare // The Washington Post. 7.02.2003.
18. *The* National Strategy to Secure Cyber Space. Washington D. C. : The White House, Feb. 2003.
19. *Information* Operations Roadmap. Washington D. C. : U. S. Department of Defense. 30 Oct. 2003.
20. *Information* Operations. Joint Publication 3—13. Washington D. C. : Joint Chiefs of Staff, 13 Feb. 2006.
21. *Information* Operations. Directive D 3600.1. Washington D. C. : U. S. Department of Defense, 14 Aug. 2006.
22. *Information* Operations. Directive 10—7. Washington D. C. : U. S. Department of Air Force, 6 Sep. 2006.
23. *Obama B.* National Framework for Strategic Communication. Washington D. C. : The White House, 2009.
24. *Cyber* Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington D. C. : The White House, May 2009.
25. *Securing* Cyberspace for the 44th Presidency. CSIS Commission on Cybersecurity for the 44th Presidency. Washington D. C. : CSIS, Dec. 2008.
26. *Butler R.* Deputy Assistant Secretary of Defense for Cyber and Space Policy. Testimony before the House of Representatives Committee on Armed Services Subcommittee on Strategy Forces. Washington D. C., 21 Apr. 2010; Lynn W. Deputy Secretary of Defense. Remarks. National Space Symposium. Colorado Springs, 14 Apr. 2010.
27. *Informational* Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. Washington. Washington D. C. : The White House, May 2011.
28. *Department* of Defense Strategy for Operating in Cyberspace. Washington D. C. : U. S. Department of Defense, July 2011.
29. *O'Neil M.* Cyberchiefs: Autonomy and Authority in Online Tribes. L. : Pluto Press, 2009; Technology, Policy, Law and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities / Ed. by W. Owens, K. Dam and H. Lin. Washington D. C. : The National Academies Press, 2010.
30. *Libicki M.* Cyberdeterrence and Cyberwar. — Santa Monica (Calif.) : RAND, 2009.
31. *Libicki M.* What is Information Warfare. — Santa Monica : RAND, 1995.
32. *Прокофьев В.* Тайное оружие информационной войны. — Мосва, 1999. — 152 с.
33. *Елизаров А.* Контрразведка. ФСБ против ведущих разведок мира. — Москва, 1999. — 288 с.
34. *Панарин И.* Психологическая безопасность войск. — Москва, 1996. — 135 с.
35. *Історія* інформаційно-психологічного протиборства. За редакцією Є. Д. Скулиша / Жарков Я. М., Компанцева Л. Ф., Остроухов В. В., Петрик В. М., Присяжнюк М. М., Скулиш Є. Д. — Київ : Науково-видавничий відділ Національної академії СБ України, 2012. — 209 с.
36. *Сучасні* технології та засоби маніпулювання свідомістю: ведення інформ. війн і спец. інформ. операцій : навч. посіб. / В. М. Петрик [та ін.]. — Київ : Росава, 2006. — 206, [1] с.
37. *Расторгуев С.* Философия информационной войны. — Москва : Московский психолого-социальный институт, 2003. — 496 с.
38. *Лисичкин В.* Третья мировая информационно-психологическя война / Лисичкин В., Шелепин Л. — Москва, 2000. — 304 с.
39. *Наоми* Кляйн. Доктрина шока. Становление капитализма катастроф. Пер. с англ. — Москва : Добрая книга, 2009. — 656 с.
40. *Карякин В.* Стратегии непрямых действий, "мягкой силы" и технологии "управляемого хаоса" как инструменты переформатирования политических пространств / Карякин В. В. // Информационные войны. — Москва, 2014. — № 3 (31). — С. 29—38.
41. *Friedman M.* Capitalism and Freedom. 1962, repr. — Chicago : University of Chicago Press, 1982. — P. 2.
42. *Перкинс Дж.* Исповедь экономического убийцы / Дж. Перкинс. — Москва : Pretext, 2005. — 319 с.

В статье произведен анализ обострения противоречий и усиления противостояний между различными социальными системами, включая государственные и негосударственные субъекты, вызванных условиями сложной социальной, экономичной, политической и культурной реальности. Рассмотрены теоретические разработки и практические результаты использования информационных средств для трансформации социальных систем, где лидерство безусловно и нераздельно принадлежит США.

The article analyzes the sharpening of the contradictions and strengthening confrontation due to the fact that we live in a complexity of social, economic, political and cultural reality. The growing complexity and diversity inevitably leads to the expansion and intensification of the contradictions between different social systems, including state and non-state actors of all kinds. The analysis of theoretical developments and practical results of the use of information tools for the transformation of social systems, where United Statesdefinitely takes the leadership.

Надійшла до редакції 15 вересня 2015 року