УДК 351.862:354.61; 351.86(477)

Ю. Г. ДАНИК, О. О. ТРУШ, В. В. КЛИВЕЦЬ

ПЕРСПЕКТИВИ РОЗВИТКУ КОМУНІКАЦІЙНО-ДІАГНОСТИЧНИХ ТЕХНОЛОГІЙ МОНІТОРИНГУ КІБЕРНЕТИЧНО-ПСИХОЛОГІЧНОГО СТАНУ ІНФОРМАЦІЙНОГО ПРОСТОРУ ВИЗНАЧЕНОГО РЕГІОНУ

***Р**озглянуто основні аспекти та перспективи розвитку комунікаційно-діагностичних технологій моніторингу кібернетично-психологічного стану інформаційного простору визначеного регіону в інтересах забезпечення національної безпеки.*

Ключові слова: комунікаційно-діагностичні технології, кібернетично-психологічний могніторинг, інформаційний простір.

***T**he basic aspects and perspectives of development komunikatsionno-diagnostic technologies for monitoring cybernetic-psychological state of the information space of a certain region in the interests of national security.*

Key words: komunikatsionno-diagnostic technologies, cybernetic-psychological monitoring, information space.

Аналіз змісту глобального кібернетично-психологічного протиборства, яке стало невід'ємною складовою проявів сучасних економічних, політичних, етнічних, релігійних тощо конфліктів і криз та майже всіх більш-менш значущих світових подій і процесів, дозволяє стверджувати, що існуючі технології діагностики комунікацій на принципах аналізу технічних показників обсягів інформації або контролю її змісту на основі контррозвідувальної діяльності виявилися неспроможними упередити, а відтак, і захистити національні інтереси, у першу чергу високотехнологічно розвинених країн, від кібернетично-психологічних втручань. Деструктивна роль таких втручань і кіберзлочинний показник подібних впливів збільшується з кожним кроком розвитку науково-технічного прогресу.

На цей час важко знайти справді ефективні приклади упередження зазначених втручань у функціонування систем прийняття та реалізації управлінських рішень на рівнях комунікації, які стосуються як окремої людина, так і суспільства, держав і міжнародних структур безпеки в цілому. Основними причинами цього є відсутність (на сьогодні – невизначеність) державних кордонів у глобальному кіберпросторі, правові, етичні, моральні норми взаємовідносин у кіберпросторі знаходяться на найнижчому і неврегульованому стані.

Недосконалість комунікаційно-діагностичних технологій захисту і неврегульованість міжнародного правового режиму із зазначеної проблематики дозволяє деяким міжнародним суб'єктам отримувати воєнно-політичні переваги

використовуючи стратегію і тактику застосування кібернетично-психологічного втручання у функціонування систем управління об'єктів, що вибрані цілями впливу.

Саме через ці обставини ми пересвідчуємося в чисельних випадках цинізму, антиморальності та просто кіберзлочинності, які заполонили кіберпростір, що в разі залишення його без захисту та оборони може перетворитися на середовище формування найбільшої загрози, з якою зіштовхнулася цивілізація, кожна держава чи особа і навіть окрема людина.

Прийнято вважати, що від рівня інформованості залежить формування психічних особливостей, які стосуються моралі, поведінки груп людей чи певних прошарків, а зрештою і всього суспільства.

Трансформація психічних процесів, яка обумовлена наслідками високотехнологічного розвитку людства стає дедалі відчутнішою в усіх проявах його діяльності, насамперед управлінської. На здатності відображати об'єктивну дійсність, в якій готуються і відбуваються процеси управління та здійснюються управлінські відносини, – визначається як кібернетичний простір. Цей простір іноді помилково ототожнюють із віртуальним комп'ютерно-мережевим простором, який є лише однією зі складових кібернетичного простору.

Однак слід зазначити, що для провідних країн світу сьогоднішня економічна криза стала поштовхом для пошуку нових підходів розв'язання зазначеної проблеми. Для відвернення загрози втрати державного суверенітету і територіальної цілісності була залучена найбільш організована складова державного інтелектуального потенціалу – військова, яка виявилася більш придатною, ніж перевантажені негативним досвідом холодної війни спецслужби та медіаструктури. Підтвердженням цього є оприлюднені дані про значне скорочення протягом найближчих двох років кількості особового складу БіБіСі та Мі-6 у Великобританії та значної кількості співробітників їх аналогів в інших країнах.

Адже форми і способи діяльності таких структур стрімко і невпинно відходять у минуле [1]. Вони вже не можуть слугувати знаряддям для підтримання балансу сил у відверненні викликів і загроз в умовах нової епохи інформаційно-психологічного протиборства, а утримання їх стає надмірно витратним для бюджетів країн, які проводять політику жорсткої економії у в усіх напрямках зовнішньополітичної діяльності (неофіційним гаслом Давосу-2011 стало твердження, що кожен бореться зі своїми проблемами сам і виживе той, хто застосовуватиме більш раціональну модель розвитку на кшталт жорстких за змістом, але ефективних по суті проектів, що реалізовуються, наприклад у Китаї та Індії).

У цьому сенсі цілком природним видається те, що концептуальними документами у сфері оборони США, РФ, Китаю, Туреччини, Польщі, а також Північної Кореї, Ірану й інших країн кібернетично-психологічні форми і способи було визнано як найбільш ефективні стратегічні дії для розв'язання політичних, економічних і інших міждержавних проблем. А на заміну психологічній, інформаційній та інформаційно-психологічній операціям, наприклад у США наприкінці 2010 р., було прийнято на озброєння нову форму кібернетично-психологічних дій – воєнні операції з інформаційно-психологічної підтримки дій в інтересах оборони та військ (сил). Іншими словами – це операції, які повинні

постійно, практично легально (але приховано по суті) проводитися воєнними та іншими структурами держави в інтересах реалізації національних інтересів країни у сфері оборони. Загалом це приклад удосконалення відомої шведської моделі побудови системи кібернетичної та її складової інформаційної безпеки країни, де основну функцію виконує управління інформаційної оборони Міністерства оборони Швеції у протиборстві із глобальними кібернетично-психологічними втручаннями у сферу оборони цієї країни [2].

Світ зрозумів, що в сучасних високотехнологічних умовах сфера оборони все більше залежить від стану безпеки інформаційного простору країни, який є одним зі складових кібернетичного простору. Кібернетичний простір – це простір, в якому готуються і відбуваються процеси управління та здійснюються управлінські відносини. Його основними складовими є такі: інформаційний простір, комунікаційний простір, соціотехнічний простір і віртуальний комп'ютерно-мережаний простір.

Це відбулося, коли США відмовилися спочатку від термінів "інформаційна боротьба і інформаційна війна", створивши в червні 2010 р. Об'єднане командування бойових дій у кіберпросторі у складі Об'єднаного стратегічного командування.

Основними завданням інформаційної безпеки США відповідно до нової Національної стратегії із захисту кіберпростору є "... упередити кібернапади на критичну інфраструктуру, знизити вразливість нації до таких нападів, а також мінімізувати втрати під час відновлення..." [3].

У збройних силах ФРН основні завдання з впливу на інформаційні мережі противника покладено на Управління інформаційних і комп'ютерних операцій Командування стратегічної розвідки. У збройних силах Ізраїлю діяльність щодо використання інформаційних технологій здійснюють міністр оборони, начальник генерального штабу і начальник розвідувального управління.

Оприлюднений огляд масштабних навчань, проведених у рамках ЄС "Кібернетична коаліція-2010", свідчить, що з метою колективної інформаційної безпеки провідні країни світу відпрацьовували на практиці нові форми і способи застосування військових структур в інтересах реалізації національних інтересів країн у сфері оборони, зміст яких полягає в застосуванні сил і засобів у режимі бойового чергування для захисту національних інформаційних інтересів від кібернетично-психологічних впливів та адекватного реагування на дії агресора.

Загалом огляд результатів навчань показав, що інноваційні підходи з використання потенціалу військової структури інформаційно-психологічних дій дозволяють провідним країнам світу реалізовувати їх національні інтереси не тільки силовими способами, а дедалі більш ефективними кібернетичними впливами, серед яких визначна роль належить кібернетично-психологічним впливам і економити при цьому бюджетні кошти за рахунок інтеграції значної кількості завдань армійських структур до загальнодержавних систем кібернетичної безпеки та її складової інформаційно-психологічної безпеки.

Такий підхід дозволяє органічно розвивати в загальному комунікаційному просторі держави як воєнні так і цивільні системи комунікації. Він надає можливість

узгоджено і заздалегідь планувати розподіл бюджетних коштів для забезпечення розвитку всіх елементів інформаційної інфраструктури і для їх захисту і для активного залучення з метою сприяння реалізації національних інтересів як у мирний час, так і особливий період.

Україна не залишається осторонь від впливу глобальних кібернетично-психологічних втручань, метою та результатом яких можуть бути не тільки локальні, але й глобальні деструктивні геополітичні зміни.

Як правило, подібні кібернетично-психологічні втручання здійснюються за різними сценаріями, які є більш за все унікальними, хоча іноді і повторюються. Але вони базуються на суттєвих, загальних закономірностях і повторюваних зв'язках соціальних явищ і процесів, а передовсім зв'язках між соціальною дійсністю людей як спільноти та соціальними діями окремих індивідів.

Залежно від рівня кібернетично-психологічних втручань, їх можна класифікувати як такі дії:

– на рівні соціальних інститутів (діалектична єдність людини, вождя, лідера й соціального середовища; визначальна роль особистості чи колективу, суспільства; постійне вдосконалення (деградація) колективу; провідна роль колективу (окремого чи елітного підрозділу) в системі колективів чи системі організації захисту та оборони національних інтересів);

– такі, що визначають розвиток складових соціальної структури суспільства: постійне збільшення (зменшення) кількості населення, прискорене збільшення кількості міського населення; прискорене зростання частки населення, зайнятого у певній сфері торгівлі, обслуговування, військовій; спрямовані на самовдосконалення систем.

Особливість кібернетично-психологічних втручань у тім, що в них чітко простежується об'єктивність. Водночас, хоча дія кібернетично-психологічних втручань є об'єктивною, вона зв'язана із суб'єктивним фактором і реалізується (на відміну від законів природи) лише через діяльність людей.

Класичною стратегією таких дій є ситуація навколо сайту Wikileaks та його засновника Дж. Ассанжа. На сайт Wikileaks (від англ. wiki й leak – витік) було оприлюднено анонсовану за тиждень до цього частину листування дипкорпусу США – 251 287 одиниць документів від несекретних до секретних матеріалів включно. Основна частина документів – записи бесід американських дипломатів із політиками, чиновниками та приватними особами різних країн, звіти про найважливіші події в країнах перебування та аналіз поточної ситуації в цих країнах. Усього ж планувалося оприлюднити більше 3 млн документів.

Зокрема, архів, оприлюднений Wikileaks, складається з 251 287 документів (261 276 536 слів), найстаріший з яких датовано 28 грудня 1966 р., а найсвіжіший – 28 лютого 2010 р. Ці документи – переважно депеші, послані американськими дипломатами вищого рангу в Держдепартамент, а також – відправлені з канцелярії Держсекретаря в американські представництва, включно з представництвами при НАТО й ООН.

Зміст сайтів формує погляди для подальшого прийняття рішень на підставі: інструкцій, які надсилає Вашингтон; розвідувальних даних, які збираються; способів передачі обробленої інформації; даних про які довідалися дипломати у країнах, в

яких вони працюють; звітів зустрічей з міністрами й політиками; думок дипломатів про своїх співрозмовників тощо.

Загалом джерелами інформації є 274 посольства і представництва США в усьому світі. Найбільш часто згадується Ірак – в 15,365 документах (з них біля половини – 6,677 – депеші з Іраку). Найбільше депеш послано з посольства в Анкарі – 7,918. Ще більше – з канцелярії держсекретаря США – 8,017. Тільки 15,652 повідомлень – з грифом "секретно"; менше половини (101,748) – з грифом "конфіденційно". Більше половини – 133,887 – з грифом "для службового користування".

Масштабне оприлюднення конфіденційної інформації здійснюється даним сайтом та активно репрезентується у світових ЗМІ його керівником – Джуліаном Ассанжем.

Дж. Ассанж так характеризує роботу зазначеного сайту: "Це класична система інформаторів. У нас є різні можливості допомогти їм поставляти нам інформацію. Ми використовуємо високотехнологічні методи забезпечення комп'ютерної безпеки при передачі інформації через мережу, і для того, щоб ховати "кінці у воду", переспрямовуємо інформацію на законних підставах через такі країни, як Бельгія та Швеція, щоб знаходитись під їх юридичним захистом".

Хронологія розвитку подій дозволяє відслідковувати імовірну послідовність кібернетично-психологічних впливів, відповідно до яких, і що цікаво навіть деяким чином апріорно, здійснювалася підготовка до протидії та безпосередньо сама протидія, саме:

– у першому кварталі 2010 р. вочевидь відбувалася латентна фаза протиборства Wikileaks – уряд США;

– у травні 2009 р. проведені навчання "Єврокоаліція – 2010" як запобіжник діям Wikileaks;

– у червні 2009 р. створено, а з листопада 2009 р. почало функціонувати Об'єднане кібернетичне командування.

Однак запобіжних заходів виявилося замало – перша частина публікацій, яка стосувалась військової компанії США в Іраку (так зване "Іракське досьє"), була оприлюднена сайтом у липні-серпні 2010 р. – понад 90 000 засекречених військових документів, що стосувалися воєнних дій США в Афганістані. Серед них був найбільш резонансним відеосюжет обстрілу американським гелікоптером "Апач" центру Багдада, коли під вогонь потрапили цивільні особи (серед них два фотокореспонденти "Ройтерс". Американські військові в процесі переговорів визнають це як "помилку"). Крім зазначеного в документах повідомлялось про численні задокументовані випадки загибелі мирного населення, злочини, що здійснювались коаліційними військами, тощо.

Цей комплекс публікацій Wikileaks був добре розрекламований світовою пресою й спричинив ефект бомби, що розривається на інформаційному полі. Новий пакет даних – це тисячі статей та інфографіки, що має наслідком увагу багатомільйонного інтернет-співтовариства, а відтак, виходять за його межі.

Подібні "викиди" або "витоки" різноманітних резонансних інформаційних матеріалів включно з секретними або конфіденційними – відомий спосіб інформаційно-психологічних дій, який відноситься до "м'якої" чи "сірої" пропаганди (ПР).

У Росії 1990-х рр. набули широкої популярності інтернет-викиди, які йшли від

охоронної спецслужби переслідуваного офіційною владою "Медіа-Моста" В. Гусинського ("Коготь-1" та "Коготь-2" тощо).

Попередньо у витоку інформації звинувачується співробітник військової розвідки США Бредлі Меннінг, якого будуть судити за співробітництво із сайтом WikiLeaks. За даними Der Spiegel, більша частина службового листування дипломатів відноситься до періоду після 2004 р., коли було запущено спільний проект міністерства оборони США та Держдепартаменту США Net-Centric Diplomacy. Він став частиною так званого Secret Internet Protocol Router Network (SIPRNet) – таємної бази даних Пентагону, що була доступна 2,5 млн співробітникам цього відомства по всьому світу.

Більшу частину оприлюднених матеріалів присвячено проблематиці Близького та Середнього Сходу, частково Росії і окремим країнам Європи. Зокрема, очікувано, що велика увага ЗМІ в оприлюднених документах була зосереджена на найбільш "пікантних" фактах, а саме: зневажливій оцінці з боку диппредставників США щодо лідерів окремих країн; особливості приватного життя високопосадовців та негативно – радикальні оцінки внутрішньополітичного становища в деяких країнах.

Таким чином, варто зазначити, що більшість з оприлюднених даних навряд чи може вважатись надзвичайно актуальними або такими, що може призвести до значних політичних конфліктів. Наприклад, по відношенню до негативних оцінок внутрішньополітичного стану в Росії сенатор Ради Федерації М. Капура справедливо відмічає, що "з приводу криміналу в нашій країні, то в тих же самих США про це кажуть щонайменше 20 років".

Крім того, такі оцінки є типовими для американської преси, і сенсацією тут є хіба що сам факт демонстрації особливостей мислення дипломатів. Водночас вбачається важливим, що більшість оприлюднених матеріалів у тій чи іншій формі містять значно більше інформації про оціночні характеристики та психологічні портрети політичних лідерів, ключових чиновників тощо, ніж власне фактологічної інформації про стан у тій чи іншій країні.

Водночас деякі дані стали причиною виникнення напруги на міжнародному рівні. Так, Російська Федерація зажадала офіційних пояснень від НАТО щодо існування відсутності потенційних військових планів НАТО, пов'язаних із можливою агресією РФ у напрямку Прибалтійських країн. Офіційне підтвердження існування таких розробок вже змусило МЗС РФ та Міністерство оборони РФ загострювати свою позицію щодо цього питання, констатуючи, що РФ буде "адекватно реагувати" на наявність подібних проявів.

Сутність кібернетично-психологічного впливу здебільшого була зосереджена на найбільш "пікантних" фактах, а саме:

– зневажливій оцінці з боку диппредставників США щодо лідерів окремих країн;

– особливостях приватного життя високо посадовців;

– негативно-радикальних оцінках внутрішньополітичного становища в деяких країнах.

Однак вірогідною є версія, що більшість матеріалів сайту Wikileaks було передано самими спецслужбами США, однак це означає наявність потужного внутрішнього конфлікту між урядовими інституціями в США, в який активно втягнуто весь силовий блок разом із розвідувальним співтовариством.

Така версія додатково підтверджується і тим, що видається вкрай

малоймовірним, що у випадку небажання спецслужб допустити витік такої інформації, в них би не знайшлось реальних механізмів завадити цьому (оскільки вся оприлюднена інформація передана сайту Wikileaks виключно в електронному вигляді) навіть шляхом фізичного усунення тих, хто здійснював практичні дії або навіть був просто причетний до зазначеного.

Тим більше, що провідні країни світу активно розробляють кіберзброю, а нещодавній успіх вірусу Бйіхпеї, що, на думку експертів, був спрямований проти іранської ядерної програми і не міг бути створений лише групою ентузіастів, доводить ефективність цих зусиль [4].

Іншою версією може бути зацікавленість різноманітних безпекових організацій, що активно пропагують засоби криптографічного захисту та комплексні системи кіберзахисту для урядів і державних інституцій. Варто відзначити, що автор сайту Wikileaks свого часу був пов'язаний як із хакерським середовищем, так і з розробкою систем криптографічного захисту.

Ще однією актуальною версією можна вважати опосередкований початок передвиборної компанії в США.

З погляду на проміжні результати діяльності Wikileaks така версія однак з певним уточненням є небезпідставною. Метою такої глобальної операції може бути не лише спроба здійснити деструктивні впливи на нинішню адміністрацію, яку значна кількість американських експертів називає занадто м'якою та неефективною, але й максимально уповільнити та ускладнити процеси, пов'язані зі спробою змін у геополітичних і геостратегічних процесах у північно-східних регіонах Європи та Азії. Можливо знайти й опосередкований вплив зазначених процесів і на події в північній Африці та на Близькому Сході. Скоріш за все вони матимуть резонанс і на Далекому Сході, і в Південно-східній Азії, таким чином охоплюючи фактично регіони як хартленду, так і рімленду по найбільш критичним їх точкам. Водночас це надає й можливість дискредитувати як окремі персоналії адміністрацій з кожного боку і тим самим відповідним чином впливати на них та управляти їх діями, так і продемонструвати подвійність стандартів у цих відношеннях на інституційному рівні; відкрити найбільш складні питання як внутрішньої політики держав, так і зовнішньої, тобто спровокувати кібернетично-психологічні впливи на ключових акторів світової політики [5].

Отже, інформаційно-психологічна експансія із геополітичним прицілом є реально існуючим явищем, відповідь на яку держави, які стали мішенню таких впливів, мають вживати ефективних заходів протидії.

Але ані на рівні державних документів, ані на рівнях організаційно-правовому та діяльнісно-практичному факти подібної інформаційно-геополітичної експансії, інформаційно-психологічної безпеки та протидії спеціальним інформаційно-психологічних операціям не отримали поки що належного осмислення.

З огляду на зазначене інноваційні комунікаційно-діагностичні технології моніторингу кібернетично-психологічного стану національного інформаційного простору повинні забезпечити можливість для органів державного управління (як місцевого самоврядування, так і центральних) оперативно визначати ті показники, що раніше не проявлялися і їх ніякими іншими способами визначити було

неможливо, наприклад, щодо рівня сприйняття та реакції управлінських систем на зовнішній вплив, його наслідки на короткострокову перспективу та вірогідні глобальні результати в інформаційній сфері, а також оцінки впливу управлінських рішень на стан кібернетично-психологічної обстановки.

Сучасні технології дозволяють ефективно й оперативно вирішувати подібні завдання. Цю унікальну, за своїми можливостями, особливість сьогодення, необхідно використати для активізації тих складових систем безпеки, на які покладається функція моніторингу стану інформаційного простору та кібернетичного простору в цілому.

Особливе значення має розвиток технологій виявлення ознак зовнішнього кібернетично-психологічного втручання на початкових етапах деструктивних змін у національному кібернетичному просторі, що дозволить ідентифікувати першопричини економічних, політичних етнічних, психологічних криз і звести до мінімуму можливість діагностичної помилки як на короткострокову перспективу, так і на вірогідні глобальні результати.

Застосування комунікаційно-діагностичних технологій моніторингу кібернетично-психологічного стану інформаційного простору може стати ефективним інструментом для тестування соціотехнічних систем з виявлення уражених об'єктів, щоб установити весь патологічний ланцюжок з урахування нових його важливих таких показників:

– енергетичний баланс інформаційного простору з визначенням у сформованій ситуації його резервів адаптації;

– історичні особливості визначеного регіону, пов'язані зі спадкоємною схильністю до певних традицій (войовничість, сепаратизм, тяжіння до переселення тощо);

– приховані психологічні причини захворювань масової свідомості у визначеному регіоні (непевність, страх, образа, закомплексованість, депресія, стрес тощо);

– наявність у соціотехнічних системах управління будь-якого виду вірусів для їх локалізації й зменшення рівня активності;

– відсутність у регіональних соціотехнічних системах управління комунікаціями елементів, які необхідно включати (виключати) негайно або в перспективі для підтримання їх захищеності та спроможності ефективно функціонувати;

– рівень неприйняття в конкретному регіоні на тих чи інших кібернетично-психологічних втручань, виявити її причину, а також протестувати будь-який вид втручань;

– ступінь ефективності й сумісності будь-яких кібернетично-психологічних втручань, а також можливість їхньої побічної дії без застосування в реальному інформаційному просторі.

Таким чином, буде створено цілісну систему, яка дозволить таке:

– відслідковувати зміни в інформаційному середовищі щодо держави в інтересах реалізації її інформаційної політики;

– створити гнучку систему управління заходами щодо забезпечення інформаційної безпеки на державному рівні із залученням різних структур збройних

сил держави без безпосереднього їх підпорядкування;

– залучати інформаційний ресурс держави для організації та проведення заходів з забезпечення інформаційної безпеки у мирний час та в особливий період для запобігання та стримування збройних конфліктів і відсічі збройної агресії;

– раціонально використовувати загальнодержавні і відомчі ресурси в ході підготовки та проведення інформаційних заходів в інтересах оборони держави.

На такій теоретичній базі можлива розробка, координування та здійснення такого:

– інформаційно-освітніх програм;

– підготовка військ (сил) інших країн, залучення для рішення завдань по підтриманню мирного положення тощо;

– визначення компромісних умов для встановлення контактів між всіма зацікавленими партіями;

– проведення оцінки району дій з метою виявлення лідерів, основних груп, уразливих сторін місцевого населення та його сприйнятливості до психологічного впливу;

– надання допомоги іноземним державам у забезпеченні внутрішньої безпеки, впровадження психологічних заходів у всі аспекти здійснюємих програм з надання допомоги іноземним державам, включаючи внутрішній розвиток, гуманітарну сферу та зміцнення безпеки, розробка заходів з інформування міжнародної громадськості.

Практична реалізація зазначеного замислу можлива за наявності потужної організаційної складової. Тому, за ініціативи Європейської комісії, до 2013 р. планується створити Центр боротьби з кіберзлочинністю ЄС та Європейську систему попередження і спільного використання інформації.

До 2012 р. очікується формування Єдиної європейської мережі реагування на комп'ютерні інциденти, основу якої складатимуть комп'ютерні підрозділи (команди) швидкого реагування кожної країни-члена ЄС.

Слід зазначити, що досвід іноземних країн щодо захисту від кібернетичних загроз свідчить про комплексний підхід до цієї важливої складової національної та колективної безпеки.

Основними напрямами системного підходу з реалізації заходів щодо створення ефективних систем захисту національних інформаційних ресурсів та інфраструктури від кібернетичних загроз є такі:

– розробка та вдосконалення нормативно-правової бази, відповідних національних стратегій, концепцій, у тому числі узгодження спільних заходів на міждержавному рівні стосовно забезпечення глобальної безпеки у кібернетичній сфері;

– посилення координації дій органів державного та військового управління з метою забезпечення захисту національного кібернетичного простору;

– створення дієвих систем виявлення, запобігання та протидії зовнішнім кібернетичним загрозам з одночасною оцінкою їх можливостей щодо реагування на загрози;

– формування нових державних структур із забезпечення кібернетичної безпеки, у тому числі у складі збройних сил, призначених для ведення бойових дій у кіберпросторі.

Особливо актуальним для України є формування навичок нового мислення не тільки в середовищі еліти, а в усіх верств населення. Кожен член суспільства має

бути певною мірою освіченим у сфері кібернетичного протистояння, має розуміти значення і роль знань у розбудові нового кібернетичного суспільства, має вміти дати оцінку виконанню своїх професійних ролей, передбачати наслідки своїх кібернетично-психологічних втручань у суспільне життя.

Зараз в Україні зростає значення формування нового мислення, основними принципами якого мають стати відмова від ідеологізації, просування в напрямі до єдиного світового знання з метою вирішення спільних завдань.

Література:

1. Збірник документів і матеріалів навчань сил і засобів спецпропаганди КВО / Політичне управління КЧВО. – К., 1989.

2. Информационная безопасность США. – М. : ЗВО. – 2010. – № 10.

3. *Севастьянов А. А.* Апарат психологической обороны Швеции / А. А. Севастьянов. – М. : ЗВО. – 2003. – № 9.

4. http://www.newsru.com/world/29nov2010/wikileaks_2.html

5. http://www.lenta.ru

Надійшла до редколегії 25.10.2011 р.