УДК 355.01

Г. А. Дробаха, М. О. Єрмошин, Є. Б. Смірнов

ПИТАННЯ НОРМАТИВНО-ПРАВОВОГО УРЕГУЛЮВАННЯ ПРОТИДІЇ НЕГАТИВНОМУ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОМУ ВПЛИВУ НА ГРОМАДЯН КРАЇНИ

Розглянуто існуючий стан питань нормативно-правового урегулювання протидії негативному інформаційно-психологічному впливу в Україні та зарубіжних країнах. Виявлено недоліки наявної нормативно-правової бази та визначено можливі напрямки її вдосконалювання.

Постановка проблеми. Головним об'єктом застосування технологій інформаційно-психологічних впливів на громадян країни є, безумовно, політичні конфлікти і породжені ними конфліктні стосунки. В умовах широкого застосування сучасних технологій інформаційно-психологічного впливу у міжнародних відносинах сама лише декларація незалежності й офіційне світове визнання суверенітету не є достатнім захистом від втручання у справи країни [7]. Країни, особливо ті, які нещодавно отримали власну державність і набули незалежності, мають потребу у розробленні і закріпленні на державному рівні (у нормах права) комплексу заходів щодо захисту від небажаного інформаційно-психологічного впливу.

Розроблення такої нормативної бази повинне ґрунтуватися на сучасних досягненнях у цій галузі з урахуванням світового досвіду, оцінюванні існуючих моделей впливу і розповсюдженості інформаційно-психологічних технологій впливу, ретельній перевірці придатності її застосування до країни.

Аналіз останніх досліджень і публікацій. Сьогодні у світі поширеними є англосаксонська, романо-германська, східноазійська та ближньосхідна моделі впливу на громадян країни. В основі англосаксонської моделі лежить доволі історично молода ідеологія і світогляд протестантства та три американські ідеологічні концепції – "експорт демократії", "силове примирення" та "оксамитові революції", які, по суті, є переробкою і розвитком протестантського світогляду. Романо-германська модель ґрунтується на досвіді співіснування різноманітних народів у межах Європи та історичній культурно-релігійній традиції католицизму. В основі східноазійської традиційної моделі – конфуціанство та філософське вчення Лао-Цзи. Основою ближньосхідної моделі є історичний досвід поширення впливу ісламського світу. Кожній із цих моделей відповідає та чи інша технологія інформаційно-психологічного управління конфліктами.

Так, англосаксонська модель передбачає розпалювання конфлікту на міжетнічних та міжконфесійних суперечностях аж до виникнення локального воєнного конфлікту у визначеному регіоні. Паралельно цей "штучно підігрітий" конфлікт широко висвітлюється світовими ЗМІ з метою впливу на масову свідомість населення та політичних еліт як у зоні конфлікту, так і за його межами. Масоване інформаційно-психологічне оброблення населення призводить до втрати ним критичності; у зв'язку з "міфічною загрозою" у регіонах конфлікту створюються ідеологічні фракції, що забезпечують схвалення населенням пропозиції про військове втручання у конфлікт та внутрішні справи учасників конфлікту. Далі, нерідко під виглядом миротворчих операцій розпочинається військове втручання із залученням сил союзників по воєнно-політичних блоках та країн-сателітів.

Романо-германська модель психологічного управління конфліктами передбачає тонке маніпулювання сприйняттям конфліктуючими сторонами політичного образу конфлікту. Для кожної сторони конфлікту готується свій, відмінний від інших, образ конфлікту, причому кожен із лідерів конфліктуючих сторін у цьому образі вбачає те, що бажає побачити. Для світової спільноти готується вибірка інформації, в якій увага концентрується на різниці у поглядах, на нестикуваннях у висловах різних політичних лідерів. Це, так би мовити, інтелектуальна гра на виявлення відсутності логіки, на питаннях моралі, довіри у стосунках. Сторона, що дискредитована таким чином в очах європейської спільноти (яку змушують почуватися винною), намагається відновити свою репутацію і стає більш поступливою.

Мета статті – проаналізувати можливість використання досвіду зарубіжних країн щодо нормативно-правового урегулювання протидії негативному інформаційно-психологічному впливу на громадян країни.

Виклад основного матеріалу. Досвід США –

країни з найбільш розвиненою у світі інформаційною та телекомунікаційною інфраструктурою, що стала за останні кілька років об'єктом для вчинення терористичних актів та кібернетичних атак, є досить цікавим і повчальним з точки зору аналізу тенденцій у державній, бюджетній, інвестиційній, науково-технічній і кадровій політиці вирішення комплексу проблем, пов'язаних із забезпеченням інформаційної безпеки національної інфраструктури [6].

Розроблені у цій країні заходи інформаційної безпеки характеризуються глобальністю і цілісністю. Заходи інформаційної безпеки охопили всю інфраструктуру країни, яка тим чи іншим чином може стати об'єктом інформаційного впливу. Управління і фінансування цих заходів – централізоване, використовуються як приватні, так і державні ресурси, широко застосовуються сучасні наукові розробки. Новітні інформаційно-психологічні технології здатні спричиняти колосальні збитки будь-якій країні, можуть одночасно підірвати фінансову систему і систему управління країни. Тому система інформаційно-психологічної протидії має бути орієнтована на випередження, адже орієнтація на дії "за фактом" впливу має "завелику ціну".

Відповідно до закону про патріотизм (USA Patriot Act), що прийнятий Конгресом США 26 жовтня 2001 р., критична інфраструктура визначається як сукупність фізичних або віртуальних систем і засобів, важливих для США такою мірою, що їх виведення з ладу або знищення можуть призвести до згубних наслідків у галузях оборони, економіки, охорони здоров'я та безпеки нації.

25 листопада 2002 р. було прийнято закон про внутрішню безпеку (Home Security Act, HR 5005). Був створений спеціальний комітет (House Homeland Security Committee), який здійснює постійний нагляд за його виконанням в особі членів Палати представників. Відповідно до цього закону з метою забезпечення безпеки громадян від загроз з боку міжнародного тероризму створено Міністерство внутрішньої безпеки (Department of Homeland Security), на яке покладаються функції щодо запобігання терористичним актам, зниження вразливості інфраструктури та ліквідації наслідків від терористичних актів, а також координації дій інших міністерств і відомств у ліквідації наслідків техногенних, антропогенних і природних катастроф на території США.

Структура нового міністерства передбачала наявність апарату міністра і чотирьох основних підрозділів (директоратів): аналізу інформації та захисту інфраструктури (Information Analysis and Infrastructure Protection), безпеки кордонів і транспорту (Border and Transportation Security), мобілізаційної готовності та екстреного реагування (Emergency Preparedness and Response), науки і технологій (Science and Technology).

1 березня 2003 р. до штату Міністерства внутрішньої безпеки були передані такі підрозділи міністерств і відомств уряду США: управління безпеки критичної інфраструктури Міністерства торгівлі (Infrastructure Assurance Office – CIAO), національний центр захисту інфраструктури ФБР Міністерства юстиції (National Infrastructure Protection Center – NIPC), національний центр моделювання та аналізу інфраструктури при Інституті проблем захисту інформаційної інфраструктури Міністерства енергетики (National Infrastructure Simulation and Analysis Center – NISAC), федеральний центр захисту інформаційних ресурсів Адміністрації загальних служб (Federal Computer Incident Response Center of the General Services Administration – FedCIRC), управління безпеки енергетичних систем Міністерства енергетики (Energy Assurance Office of the Department of Energy – EAO), національна система зв'язку Міністерства оборони (National Communication System – NCS).

Напередодні підготовки війни в Іраку американська адміністрація прийняла три нових директивних документи в інтересах внутрішньої безпеки: Національну стратегію боротьби з тероризмом (The National Strategy for Combating Terrorism), Національну стратегію кібернетичної безпеки (The National Strategy to Secure Cyberspace) та Національну стратегію фізичного захисту критичної інфраструктури (The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets).

Нові стратегії вперше офіційно визнають "повну залежність інфраструктури США від інформаційних систем і мереж", їх уразливість і націлюють уряд, промисловість, бізнес і суспільство у цілому на створення так званої Єдиної національної системи реагування на кібернетичні напади (National Cyberspace Security Response System) як сукупності територіальних, відомчих та приватних центрів аналізу і розподілу інформації (ISAC) у різних секторах народного господарства та економіки країни. З цією метою у структурі МВБ створено національний підрозділ кібернетичної безпеки (National Cyber Security Division), головним елементом якого має стати

новостворений за рахунок об'єднання трьох груп негайного реагування (CC/CERT, NCS, NIPC) Центр екстреного реагування на комп'ютерні події у США (US-CERT – US Computer Emergency Response Team).

Основне завдання інформаційної безпеки формулюється як посилення заходів щодо забезпечення цілісності, надійності і готовності критичної фізичної та інформаційної інфраструктур як всередині, так і за межами країни.

У законі про внутрішню безпеку також визначено додаткові заходи, спрямовані на посилення відповідальності за злочини у сфері інформаційної безпеки.

Крім законодавчого вирішення проблеми у США неабияке значення надається фінансовому та науковому вирішенню питань інформаційно-психологічної безпеки.

Для створення нових технологій у галузі забезпечення інформаційної безпеки уряд США залучає кращих учених, інженерів і фахівців з таких провідних організацій, як Національна академія наук, Національний інститут стандартів і технологій, Інститут проблем захисту інформаційної інфраструктури. Починаючи з 2004 р. фінансування всіх дослідницьких проектів у США, пов'язаних з інформаційною безпекою, незалежно від відомчої належності здійснюється в рамках єдиної національної програми "Кібернетичне страхування" (Cyber Trust).

Ідеологічними питаннями займаються у США три потужні центри – RAND Corporation, Массачусетський і Стенфордський університети. Вони розробляють програми, спецоперації, заходи, доктрини, стратегію і тактику американського просування, які згодом американською піар-машиною тиражуються по всьому світу, приймаються на озброєння політиками.

Проте "переоснащення" системи інформаційної безпеки країни не одразу привело до бажаного результату. Крім того, стало зрозумілим, що потрібно модифіковувати саму модель впливу, а не лише технологічні засоби її реалізації. Так, постійне звертання до світової спільноти, поширення інформації про конфлікти у тих чи інших регіонах та посередництво у них США уможливило виявлення алгоритму дій цієї країни та вироблення критичного ставлення до них і як наслідок – зниження ефективності інформаційно-психологічного впливу США.

Після обрання Барака Обами президентом стали частіше застосовувати "soft power" – "м'яку силу", тобто економічний і культурний вплив. Широко популяризуються американський стиль, американський спосіб життя, американські стандарти, американська музика і цілий набір штампів суспільства. Ця гуманітарно-ідеологічна експансія відбувається через фонди, релігійні секти, правозахисні центри, що пропагують американські цінності. Проте й керівництву Обами довелося визнати зниження ефективності існуючої моделі інформаційно-психологічних впливів.

Як зазначила Хіларі Клінтон, її країна перебуває у стані інформаційної війни і програє її "Аль-Джазіра". Китайці створили глобальну телевізійну мережу, що транслює передачі різними мовами. Росіяни створили англомовний канал. А вплив її країни скорочується.

Деяке скорочення дійсно спостерігається, але воно викликане потребами зміни технологій. Так, на зміну монополії "Голосу Америки", що значно скоротив зону свого радіомовлення у Східній Європі, прийшли CNN та Інтернет.

Країни, які нещодавно набули незалежності чи відновилися після занепаду, мають дещо спрощену систему інформаційно-психологічної безпеки. Їх система захисту рефлексивного типу, тобто така, що дає реакцію "за фактом" здійснення впливу, має досить обмежені можливості прогнозування та попередження. У країнах СНГ інформаційний захист будується майже за однією схемою – це прийняття Доктрини безпеки та окремих керівних документів периферійного рівня.

У Доктрині інформаційної безпеки Російської Федерації [2] негативний інформаційно-психологічний вплив визначається як пропагандистські та психологічні дії, що спричиняють таке:

– зниження боєготовності та боєздатності військ, зниження службової активності, дезертирство серед військовослужбовців, симуляцію хвороб, ухилення від виконання наказів командирів, викривлення картини бойових дій і бойової обстановки;

– зниження морального духу, створення обстановки невпевненості і занепокоєння особового складу з приводу свого майбутнього, майбутнього Збройних сил та інших військових формувань держави, а у воєнний час – ослаблення волі до військового опору;

– нівелювання почуття гордості за свою державу, за свої Збройні сили та інші військові формування держави, нейтралізацію патріотизму військовослужбовців виконувати свій конституційний обов'язок щодо захисту Батьківщини;

– розкол військових колективів, протиставлення різних категорій військовослужбовців;

– неправильне сприймання військовослужбовцями існуючих загроз національній безпеці, дійсних планів та намірів імовірного противника.

На думку російських аналітиків [1], у більшості випадків визначення змісту інформаційно-психологічного протиборства не виходить за межі боротьби з хакерами та захисту комп'ютерних мереж. Аналітик Фонду стратегічної культури А. Циганок указує, що сьогоднішні інформаційні структури Росії є недостатніми. Так, Управління Президента РФ по міжрегіональних і культурних зв'язках ні за чисельністю, ні за колом своїх повноважень не може повною мірою здійснювати всю необхідну роботу з інформаційної протидії і ведення інформаційної війни. Рада безпеки РФ виявилася не готовою до інформаційного протиборства. До інформаційної війни не пристосовані ні Міністерство закордонних справ, ні підзвітний йому Росзакордонцентр. Практично жодна із цих структур не здатна виконувати повне коло завдань з інформування, дезінформування, порушення інформаційних мереж, захисту своїх мереж, подання необхідних інформаційних блоків у провідні інформаційні агентства тощо. Росія не має структур для ведення інформаційного протиборства. У Міністерстві оборони, Міністерстві закордонних справ є структурні підрозділи, що займаються роботою з інформацією у ЗМІ, але на загальнодержавному рівні такої структури, яка б координувала роботу різних відомств в інформаційному середовищі, немає. Крім того, немає конкретних осіб, що відповідають за цю роботу. Російські експерти вбачають у цьому організаційно-управлінську проблему відсутності цільового впливу на ЗМІ, суспільну думку країн СНГ та світу. З погляду І. Панаріна, система інформаційного протиборства повинна починатися з державної доктрини, яка б прописувала структуру, відповідальність за міжнародний імідж Росії і ведення інформаційної війни, її повноваження, фінансування, цілі та завдання.

Зосередженість на "периферійній" боротьбі з небажаним інформаційно-психологічним впливом притаманна і для Білорусі. Для неї характерні добре розроблені рекомендації (методики) щодо відбиття конкретних впливів, але розробка та реалізація стратегій, що працюють на випередження небажаного впливу чи цілеспрямованого формування іміджу Білорусі у країнах СНГ та світу, є досить слабкими.

Схожа ситуація склалась і в Україні. Так, нормативно-правові основи щодо організації протидії негативному інформаційно-психологічному впливу викладені у Конституції України та законах України "Про основи національної безпеки України", "Про інформацію", "Про об'єднання громадян", "Про політичні партії", "Про правовий режим надзвичайного стану", "Про правовий режим воєнного стану". У цих документах наведені положення, які визначають заходи стосовно захисту національного інформаційного простору та обмежень у розповсюдженні певної інформації в особливий період.

Зокрема, Законом України "Про правовий режим воєнного стану" [5] передбачено низку таких обмежень, як:

– заборона діяльності політичних партій та громадських організацій, якщо така їх діяльність загрожує суверенітету, національній безпеці України, її державній незалежності і територіальній цілісності;

– здійснення контролю за роботою підприємств зв'язку, поліграфічних підприємств, видавництв, телерадіоорганізацій;

– використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ і населення;

– регулювання роботи цивільних телерадіоцентрів;

– заборона роботи аматорських приймально-передавальних радіостанцій особистого і колективного користування та передача інформації через комп'ютерні мережі;

– вилучення у підприємств, установ і організацій усіх форм власності та в окремих громадян радіопередавального обладнання, телевізійної, відео- і аудіоапаратури, комп'ютерів тощо.

Воєнна доктрина України [2] серед основних завдань Збройних Сил України визначає необхідність здійснення заходів щодо забезпечення інформаційної безпеки.

У Доктрині інформаційної безпеки України [4] серед реальних та потенційних загроз інформаційній безпеці визначено:

– у зовнішньополітичній сфері – зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а

також мережу Інтернету;

– у сфері державної безпеки – негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

– у воєнній сфері – інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

– у внутрішньополітичній сфері – негативні інформаційні впливи, у тому числі із застосуванням спеціальних засобів впливу, на індивідуальну та суспільну свідомість людей.

Серед заходів, які має вжити держава з метою забезпечення інформаційної безпеки України, визначаються [4]:

– у зовнішньополітичній сфері – виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізація;

– у воєнній сфері – удосконалення форм і способів протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності держави.

Висновки

Як бачимо, нормативно-правове урегулювання захисту інтересів національної безпеки та територіальної цілісності в інформаційній сфері в Україні має більшість таких же самих недоліків, що і в російському законодавстві: недостатнє опрацювання питань щодо вирішення цієї проблеми, щодо централізованості управління, відповідальності та фінансування розроблення і підтримання цілісної системи протидії. Протидія інформаційно-психологічному впливу визнається проблемою, яку повинні вирішувати Збройні Сили України та інші силові структури, що не мають для цього необхідної матеріально-технічної і наукової бази. Існуюча система протидії не здатна контролювати та захищати більшість об'єктів інформаційної інфраструктури. Технології інформаційно-психологічної протидії, що використовують державні органи, максимум, на що здатні – обмежити поширення небажаної інформації всередині країни (наприклад, використання цензури на телебаченні, у виданнях та Інтернеті). Більш розвинені технології інформаційно-психологічного впливу є капіталомісткими і застосовуються великими комерційними корпораціями для маніпуляції свідомістю населення країни у власних інтересах (комерційних і політичних). Цілеспрямоване формування світової суспільної думки навколо процесів, у яких задіяна Україна, є надсильним державній системі інформаційної протидії як у матеріальному та технічному, так і ідеологічному плані. Навіть попри вельми сприятливу ситуацію для реалізації Концепції Державної програми формування позитивного міжнародного іміджу України на 2007–2010 роки, що склалася внаслідок очікуваного чемпіонату Європи з футболу, вона так і може залишитися документом без реалізації.

Список використаних джерел

1. Барановский А. Информационная война вокруг конфликта в Южной Осетии: анализ и выводы [Электронный ресурс]. – Режим доступа : http://www.osetinfo.ru/main/194

2. Воєнна доктрина України [затв. Указом Президента України від 15.06.2004 р. № 648]. – 16 с.

3. Доктрина информационной безопасности Российской Федерации (09.09.2000 р.) [Электронный ресурс]. – Режим доступа : http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

4. Доктрина інформаційної безпеки України [затв. Указом Президента України від 08.07.2009 р. № 514]. – 7 с.

5. Про правовий режим воєнного стану : закон України від 06.04.2000 р. № 1647-III [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws

6. Леваков А. Информационная безопасность в США: проблемы и решения [Электронный ресурс]. – Режим доступа : http://freelance4.narod.ru/IS_USA.htm

7. Об утверждении Инструкции о порядке организации и проведения идеологической работы в пограничных войсках республики Беларусь : приказ Государственного комитета пограничных войск Республики Беларусь от 16 января 2007 г. № 492 [Электронный ресурс]. – Режим доступа : http://old.bankzakonov.com/obsch/razdel77/timc1/lazv0008.htm

8. Карякин В. Наступила эпоха следующего поколения войн – информационно-сетевых войн [Электронный ресурс]. – Режим доступа : http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html

Стаття надійшла до редакції 19.05.2011 р.