

УДК 354.42

О.М. Косоков

Військова частина А1906

МЕХАНІЗМИ ПОПЕРЕДЖЕННЯ ЗАХОДАМ ІНФОРМАЦІЙНІЙ КАМПАНІЇ НА РАННІХ СТАДІЯХ ЇЇ ПІДГОТОВКИ

На основі аналізу форм інформаційної боротьби визначаються шляхи вирішення проблем щодо раннього попередження та нейтралізації загроз національній безпеці України в інформаційній сфері.

Ключові слова: інформаційна безпека держави, інформаційна операція, інформаційна кампанія, попередження загроз.

Вступ

На сьогодні формування світового геополітичного простору та внутрішньодержавних відносин відбувається в умовах інформаційного протиборства. Для нашої держави ця проблема особливо актуальна: зважаючи на певну невизначеність геополітичного статусу, політичну нестабільність, нестійкість вітчизняного інформаційного простору, Україна перебуває під систематичним інформаційним тиском.

З огляду на підвищення спроможності арсеналу сил, засобів і методів інформаційного протиборства, дії, що проводяться в ході інформаційної кампанії (інформаційної операції), необхідно виявляти та припиняти на ранніх стадіях підготовки їх реалізації. У наукових роботах багатьох дослідників [1 – 3] достатньо глибоко аналізуються механізми проведення інформаційних операцій. Однак аналізу проблем протидії таким операціям більшість робіт не містить, а ті, що є, переважно стосуються технічних питань.

Отже, **метою статті є** розроблення системи заходів протидії інформаційним кампаніям на ранніх стадіях їх підготовки.

Основний матеріал

Інформаційна кампанія – це сукупність узгоджених та взаємопов'язаних за метою, завданнями, місцем і часом інформаційних операцій, ударів, акцій та атак, що проводяться послідовно і одночасно за єдиним замислом і планом для сприяння вирішенню завдань реалізації національної політики в декількох сферах життєдіяльності держави [4].

Основний об'єкт впливу інформаційної кампанії – це в цілому держава противника, а кінцевою метою її проведення може бути встановлення повного контролю над зовнішньою та внутрішньою політикою протилежної країни.

Інформаційна кампанія носить, як правило, довготерміновий перманентний характер, вона може тривати роками до досягнення своєї кінце-

вої мети. Вона може посилюватися або затухати залежно від початку чи закінчення інформаційних операцій, ударів або окремих інформаційних акцій, які її складають. У рамках однієї інформаційної кампанії можуть одночасно або послідовно проводитися декілька інформаційних операцій, кожна з яких має власну сферу спрямованості (зовнішньополітичну, внутрішньополітичну, економічну, військово-технічну тощо) та мету, яка разом з тим є частковою метою всієї кампанії.

Інформаційна операція – це сукупність узгоджених та взаємопов'язаних за метою, завданнями, об'єктами і часом інформаційних ударів, акцій, атак та заходів, що проводяться як послідовно, так і одночасно за єдиним замислом та планом для сприяння вирішенню завдань реалізації національної політики в обраній сфері життєдіяльності держави.

У мирний час метою інформаційних операцій може бути вплив на морально-психологічний стан вищого державного керівництва країни-супротивника і певних соціальних груп населення в інтересах схилення їх до прийняття рішень та дій у потрібному для протилежної держави напрямі. У воєнний час цілі інформаційних операцій полягають у дезорганізації системи державного управління та систем управління військами і зброєю, знищенні інформаційної інфраструктури противника, завоюванні інформаційної переваги над ним та створенні сприятливих умов в інформаційному просторі для дій своїх військ, а також у забезпеченні захисту власної інформаційної інфраструктури та інших складових інформаційного середовища від дій противника.

Об'єктами інформаційних операцій можуть бути населення протилежної держави, певні соціальні групи, особи, що приймають державні рішення, керівництво і населення провідних країн світу та суміжних з Україною держав, а в ході воєнного конфлікту додатково – особовий склад військ противника, населення країн-учасників воєнного конфлікту, системи державного і військового управління противника, елементи його інформаційної інфраструктури. Тривалість інфо-

рмаційної операції може бути від декількох тижнів до декількох місяців.

Інформаційна операція може мати як чітко виражену психологічну або технічну спрямованість, так і поєднувати одночасно заходи психологічного та технічного впливу. Інформаційну операцію психологічної спрямованості традиційно називають інформаційно-психологічною операцією (ІПСО). Теоретично ІПСО ведеться шляхом організації лише заходів інформаційно-психологічного впливу. Але, враховуючи те, що в реальних умовах інформаційного протистояння в особливий період у рамках однієї операції окрім заходів інформаційно-психологічного впливу мають організовуватися і заходи активного, у тому числі інформаційно-технічного, впливу на супротивника, фактично будуть вестися не інформаційно-психологічні, а інформаційні операції, тому вважати ІПСО окремою формою інформаційної боротьби недоцільно.

Підтвердженням цьому є також іноземний досвід. Так, військові спеціалісти ряду провідних країн світу, в першу чергу США, все більше відходять від вживання терміну «інформаційно-психологічна операція» та повсюди впроваджують термін «інформаційна операція». При цьому вважається, що інформаційна операція є основоположною формою інформаційної боротьби, а інформаційно-психологічні дії проводяться у її рамках на тактичному рівні. Більш того, в останній редакції польового статуту ЗС США з організації і ведення інформаційних операцій FM 3-13 Inform and Influence Activities від 25 січня 2013 року термін «інформаційно-психологічна операція» взагалі не використовується [5].

Інформаційна акція – це сукупність узгоджених та взаємопов'язаних за метою, завданнями, об'єктами і часом заходів інформаційно-психологічного впливу на особовий склад збройних сил та населення противника та/або заходів інформаційно-технічного впливу, спрямованих на втручання в процес функціонування його інформаційних, телекомунікаційних або інформаційно-телекомунікаційних систем.

Інформаційна акція за основними показниками є подібною до інформаційної атаки, але має значно більші масштаби (спрямованість на груповий об'єкт впливу) і тривалість (декілька тижнів) та вагомість об'єктів і суб'єктів впливу.

У таких умовах важливе місце в системі інформаційної боротьби займає система заходів попередження інформаційної кампанії. У випадку відбиття інформаційних акцій в діяльність повинна вступати програма локалізації нанесеного збитку, відновлення потенціалу державної системи інформаційного протистояння, поповнення втрат у силах і засобах, а також перегрупування сил постійної готовності відповідно до нових виявлених напрямків можливої інформаційної кампанії.

Систему заходів протидії акціям інформаційної кампанії та інформаційних операцій на ранніх стадіях можна умовно розділити на три складові.

1. Попередження акцій інформаційної кампанії та інформаційних операцій.

2. Виявлення акцій інформаційної кампанії та інформаційних операцій.

3. Припинення акцій інформаційної кампанії та інформаційних операцій [6].

Попередження акцій інформаційної кампанії та інформаційних операцій містить у собі:

схилення можливих противників до відмовлення від реалізації власних агресивних планів і намірів відносно держави за допомогою арсеналу сил і засобів інформаційної боротьби;

дискредитацію в очах потенційних противників найнебезпечніших для безпеки держави напрямків інформаційної кампанії;

безперервний пошук і усунення вразливостей у державній системі інформаційного протистояння та забезпечення інформаційної безпеки;

виявлення та ліквідацію умов, сприятливих для реалізації іноземними державами своїх агресивних намірів у формі розв'язання інформаційної кампанії;

безперервний пошук нових джерел інформаційно-психологічної напруженості, відстеження переміщення й розростання (зменшення) уже виявлених зон інформаційно-психологічних конфліктів (моніторинг розподілу конфліктогенного потенціалу в інформаційній сфері), а також їхніх зон впливу й оцінку загроз безпеки держави, пов'язаних з можливим залученням до одного з таких конфліктів;

моніторинг процесів укрупнення геополітичних суб'єктів, створення нових союзів і коаліцій навколо держави, в яких основною метою об'єднання суб'єктів геополітичної конкуренції є спільна конкурентна боротьба за право переважного впливу на певні частини інформаційного простору та процеси, що протікають у них. Визначення реальних цілей створення таких коаліцій та причин, що спонукали різномірних геополітичних суб'єктів до такого об'єднання;

моніторинг просторового розподілу і зосередження сил та засобів потенційних супротивників (суперників) із числа іноземних держав і інших суб'єктів геополітичної конкуренції поблизу життєво важливих об'єктів інформаційної інфраструктури держави;

виявлення та припинення умов для виникнення усередині держави й на його кордонах нових суб'єктів геополітичної конкуренції, здатних самостійно виходити із власними ініціативами на міжнародний рівень, процесів ініціювання та підтримки ззовні проявів сепаратизму;

оцінка та аналіз рівня присутності й впливу (фінансового, технологічного, інформаційного,

ідеологічного) іноземних структур над національними ЗМІ, метою якого може бути встановлення повного або часткового зовнішнього контролю над національними інформаційними ресурсами й психологічною сферою суспільства;

пошук і припинення спроб створення негативного психологічного фона відносно діяльності (або окремих її напрямків) системи органів державної влади й місцевого самоврядування;

виявлення спроб встановлення інформаційної блокади;

демонстрація (пропаганда) власної сили (могутності) держави в інформаційному просторі (у вигляді, наприклад, оперативно-тактичних навчань сил спеціальних інформаційно-психологічних операцій з використанням інформаційної зброї) з метою стримування потенційних агресорів;

зосередження сил швидкого реагування (постійної готовності) в областях інформаційного простору, що стали об'єктом уваги сил інформаційних операцій збройних сил, спецслужб і інших організацій іноземних держав, що беруть участь в інформаційному протиборстві;

протидія розвідувальної й іншої діяльності іноземних спецслужб у національному інформаційному просторі;

забезпечення власної інформаційної безпеки;

інформування Президента України, Уряду України, а також органів державної влади, що уповноважені на ведення інформаційного протиборства, про виявлені загрози розв'язання інформаційної кампанії та ступеня загрози безпеці держави.

Виявлення акцій інформаційної кампанії та інформаційних операцій містить у собі:

безперервний пошук (моніторинг) зовнішніх загроз інформаційній безпеці держави, можливих ознак, слідів і зовнішніх проявів здійснення акцій інформаційно-психологічної кампанії або операцій інформаційно-психологічної війни;

виявлення напрямків експансії іноземних держав в інформаційній (інформаційно-психологічній) сфері, протидія спробам іноземних держав за допомогою інформаційно-психологічної експансії створити умови для організації прихованого управління соціальними й політичними процесами держави ззовні;

виявлення інших спроб створення умов для організації прихованого управління системою соціальних, економічних, політичних відносин держави, системою державної влади й місцевого самоврядування - до таких спроб, наприклад, може належати створення умов для спонукання державної влади до здійснення тих або інших дій не стільки у власних, скільки - у чужих інтересах, а також - інформаційно-психологічні провокації;

аналітична реконструкція (по виявлених ознаках, слідах, зовнішнім проявам і логіко-структурним зв'язкам) акцій інформаційно-

психологічної кампанії або секретних операцій інформаційно-психологічної війни, визначення їхніх цілей, завдань, планів на стратегічному, тактичному й оперативному рівні, послідовності реалізації заходів, задіяних сил і засобів, а також можливі наслідки цієї кампанії. Як правило, діяльність сил інформаційно-психологічних операцій або вплив на них у тій або іншій формі проявляються (відображаються) в інформаційно-психологічному просторі (наприклад, у матеріалах ЗМІ та масових комунікацій), отже, можуть бути виявлені й ідентифіковані насамперед відповідними аналітичними методами;

інформування Президента України, Уряду України органи державної влади, що уповноважені на ведення інформаційного протиборства, про джерела, цілі, масштаби виявленої інформаційно-психологічної кампанії (інформаційно-психологічної війни) і ступеня загрози безпеці держави.

Припинення акцій інформаційно-психологічної кампанії й операцій інформаційно-психологічної війни на ранніх стадіях містить у собі:

знищення джерел інформаційно-психологічної кампанії (війни);

нейтралізацію джерел інформаційно-психологічної кампанії (війни);

локалізацію масштабів і ступеня небезпеки інформаційно-психологічної кампанії (війни).

Знищення джерел інформаційно-психологічної кампанії (ураження сил і засобів інформаційно-психологічних операцій агресора звичайною й інформаційною зброєю, ураження командних пунктів і центрів управління агресією) може бути повним (якщо в результаті впливу на нього джерело припиняє своє існування) або частковим (якщо уражаються сили й засоби інформаційно-психологічної кампанії, що задіяні супротивником у конфлікті) і виражатися в припиненні супротивником інформаційної кампанії або війни відносно даної держави або, у випадку часткової поразки джерел, - приводити до зміни інтенсивності кампанії, активності сил і засобів супротивника, а також планів реалізації агресивних дій на оперативному, тактичному й стратегічному рівнях.

Нейтралізація джерел інформаційно-психологічної кампанії може бути повною або частковою. *Повна* нейтралізація джерела інформаційно-психологічної кампанії (війни) містить у собі: паралізацію джерела кампанії (війни); спонукання супротивника до відмови від агресивних дій (або ведення війни); приховане управління джерелом кампанії (війни); проникнення в кадровий склад сил і засобів інформаційно-психологічних операцій агресора. *Часткова* нейтралізація джерела інформаційно-психологічної кампанії (війни) містить у собі: дестабілізацію діяльності джерела кампанії (війни); уповільнення активності джерела кампанії (війни); дезінформацію вій-

ськово-політичного керівництва сил інформаційно-психологічних операцій агресора; розкладання особового складу сил інформаційно-психологічних операцій; спонукання керівництва сил інформаційно-психологічних операцій агресора до зміни цілей і завдань кампанії, а також основних її напрямків; відволікання сил і засобів агресора на негідний об'єкт і т.д.

Локалізація масштабів і ступеня небезпеки інформаційно-психологічної кампанії (війни) містить у собі: ізоляцію вогнища кампанії щодо не зачеплених агресією областей інформаційно-психологічного простору; повну або часткову ізоляцію сил і засобів інформаційно-психологічної кампанії (війни) щодо джерел керуючого впливу, інформаційно-телекомунікаційних комунікацій супротивника, по яких ці сили забезпечуються всім необхідним для продовження кампанії; створення умов, що сковують і утрудняють дії сил і засобів інформаційно-психологічної кампанії (війни) противника; стабілізацію масштабів кампанії (недопущення розростання вогнища кампанії, проникнення деструктивних впливів за межі області інформаційно-психологічного конфлікту, втягування в конфлікт нових суб'єктів); стабілізацію інтенсивності джерела кампанії (заходи, що спрямовані на протидію зростанню активності джерела інформаційно-психологічної кампанії); мінімізацію наносимого агресією збитку.

У випадку, якщо виявлену акцію інформаційно-психологічної війни або операцію інформаційно-психологічної війни неможливо ліквідувати на ранніх стадіях наявними силами інформаційно-психологічних операцій органів державної влади, що перебувають у постійній готовності, в обов'язок системи протидії акціям інформаційно-психологічної кампанії (війни) входить інформування Президента України, Уряду України та органи державної влади, що уповноважені на ведення інформаційного протиборства, про виявлені загрози інформаційно-психологічної безпеки держави й локалізація активності агресора з метою одержання часу для мобілізації необхідних сил і засобів інформаційно-психологічної боротьби.

МЕХАНИЗМИ ПРЕДУПРЕЖДЕНИЯ МЕРАМ ИНФОРМАЦИОННОЙ КАМПАНИИ НА РАННИХ СТАДИЯХ ЕЕ ПОДГОТОВКИ

А.Н. Косоков

На основе анализа форм информационной борьбы определяются пути решения проблем раннего предупреждения и нейтрализации угроз национальной безопасности Украины в информационной сфере.

Ключевые слова: информационная безопасность государства информационная операция, информационная кампания, предупреждения угроз.

MECHANISMS OF PREVENTION MEASURES INFORMATION CAMPAIGNS IN THE EARLY STAGES OF ITS DEVELOPMENT

O.M. Kosogov

Based on the analysis of forms of information warfare defines the solutions to problems in regard to early prevention and neutralization of threats to national security of Ukraine in the information field.

Keywords: information security state information operation, information campaign warning of the threats.

Висновки

Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективно діючу систему протидії загрозам в кіберпросторі. До таких проблем в першу чергу відносяться: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складності із кадровим наповненням відповідних структурних підрозділів.

Пріоритетними напрямками державної політики щодо посилення інформаційної (зокрема кібернетичної) безпеки держави є реформування нормативно-правових документів у галузі інформаційної безпеки, дослідження питань захисту об'єктів критичної інфраструктури, сприяння недопущенню мілітаризації кіберпростору.

Список літератури

1. Ланде Д.В. Как организовать оборону: 12 шагов противодействия / Д.В. Ланде // Телеком – 2009. – № 6. – С. 46-51.
2. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій. Навч. пос. / В.М. Петрик, В.В. Остроухов та ін. – К.: Росава, 2006. – 208 с.
3. Горбулін В.П. Проблеми захисту інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченок. – К.: Інтертехнологія, 2009. – 136 с.
4. Левченко О.В. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату / О.В. Левченко // Наука і оборона. – 2013. – № 3. – С. 36-40.
5. Левченко О.В. Попередження акцій інформаційного впливу на ранніх стадіях їх підготовки / О.В. Левченко, О.М. Косоков // Перспективи розвитку сучасної науки. Мат. II Міжн. конф. (м. Київ, 7 – 8 травня 2015 року). – У 2-х част. – Херсон : Гельветика, 2015. – Ч. II. – С. 64-66.
6. Радковець Ю.І. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю.І. Радковець, О.В. Левченко, О.М. Косоков // Наука і оборона. – 2014. – № 1. – С. 38-41.

Надійшла до редколегії 16.06.2016

Рецензент: д-р техн. наук, проф. О.Б. Леонтьєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.