Інформаційна безпека держави

УДК 354.42

О.М. Косогов

Військова частина А1906

ПІДХІД ДО ПОБУДОВИ ДЕРЖАВНОЇ СИСТЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В ОСОБЛИВИЙ ПЕРІОД

На основі аналізу сутності протидії інформаційним загрозам державі в особливий період запропоновано підхід до побудови державної системи протидії інформаційним загрозам як узгодженої, цілеспрямованої, керованої з єдиного центра діяльності органів державної влади й місцевого самоврядування, що спрямована на забезпечення інформаційної безпеки людини, суспільства та держави в умовах реальної небезпеки розв'язання інформаційної агресії. Виділено основні складові зазначеної системи та основні завдання центральних органів виконавчої влади в галузі протидії інформаційним акціям (операціям, кампаніям).

Ключові слова: *інформаційна безпека, загрози інформаційній безпеці, державна система протидії, особливий період.*

Вступ

Постановка проблеми. Аналіз літератури. Сучасний світ характеризується, у першу чергу, бурхливим розвитком інформаційних технологій та комунікативних засобів, що породжує ситуацію необмежених можливостей реалізації інформаційних процесів для досягнення мети також необмеженої кількості завдань практичної діяльності. У зв'язку із цим, як на державному рівні, так і на рівні окремих суб'єктів інформаційної діяльності, існує та неухильно зростає проблема забезпечення інформаційної безпеки.

З точки зору забезпечення інформаційної безпеки особи, суспільства, держави негативний характер інформаційного впливу викликає потребу всебічного захисту та реабілітації цільової аудиторії, яка зазнає такого впливу, захисту власних інформаційних ресурсів, а також проведення упереджувальних заходів для його унеможливлення або зниження рівня ефективності.

Наукове опрацювання цього питання, зокрема в інтересах Збройних Сил України, є важливим з таких причин.

По-перше, в передових у воєнному відношенні державах світу останнім часом накопичено значний науковий, технічний та практичний досвід проведення інформаційно-психологічних операцій, акцій, атак і актів при вирішенні завдань у ході воєнних конфліктів, коли об'єктами інформаційно-психологічного впливу виступали збройні сили (формування) противника, – такий досвід необхідно вивчати та враховувати в практичній діяльності Збройних Сил України.

По-друге, за цілою низкою ознак можна стверджувати, що ключова роль у війні Росії проти України належить інформаційній складовій у формі надпотужної інформаційної кампанії щодо провокування розколу в українському суспільстві та забезпечення встановлення контролю над південно-східними регіонами України. В цих умовах гостро постає проблема захисту національного інформаційного простору від зовнішніх інформаційних загроз [2].

По-третє, наукова дискусія стосовно вирішення проблеми забезпечення інформаційної безпеки, у тому числі з її інформаційно-психологічною складовою, активно продовжується як у міжнародному вимірі, так і загальнодержавному в Україні, починаючи з термінології, – це викликає потребу подальших наукових досліджень цієї проблематики.

По-четверте, активне реформування Збройних Сил України потребує адаптації наукових розробок, зокрема з питань протидії інформаційно-психологічному впливу, до механізмів реалізації функцій і завдань Збройних Сил України у їх перспективній структурі та складі.

Аналіз спеціалізованої літератури, наприклад [3-5], показує, що на сьогодні у нашій державі та її Збройних Силах триває інтенсивний процес її формування, а саме у Міністерстві оборони України розроблені концептуальні документи та плани щодо розгортання такої системи, у Збройних Силах України створюються відповідні підрозділи. Разом з тим, забезпечення інформаційної безпеки держави в особливий період, в умовах якого цільовою аудиторією такого впливу розглядається особовий склад військ (сил) та органи військового управління, а об'єктами інформаційно-технічного впливу – засоби управління військами та зброєю [5], вивчено недостатньою мірою.

© О.М. Косогов

Тому розробка науково обґрунтованих підходів до створення дієвої системи протидії загрозам національній безпеці держави в інформаційній сфері в особливий період є актуальним науково-практичним завданням.

Метою статті є формулювання підходу до побудови державної системи протидії інформаційним загрозам в особливий період.

Основний матеріал

Система органів державної влади, будучи основним фактором, що регулює суспільні відносини в інформаційній сфері, поряд з основним і пріоритетним об'єктом зовнішньої агресії є центральною ланкою забезпечення інформаційної безпеки й основним інструментом відбиття та припинення будь-яких зазіхань іноземних держав на суверенітет, територіальну цілісність і громадянську єдність суспільства, на його життєво важливі інтереси й перспективи розвитку. Оскільки в інформаційному просторі такі зазіхання можуть приймати форми інформаційної акції, операції або інформаційної кампанії, на державу в особі системи її органів влади покладається найважливіший обов'язок своєчасного виявлення загроз інформаційній безпеці, мобілізації сил і засобів громадянського суспільства для захисту державних інтересів та протидії агресії в кожній з її форм, а також організації протидії акціям інформаційної агресії на ранніх стадіях виникнення конфлікту.

Державна система протидії інформаційним загрозам – система узгодженої, цілеспрямованої, керованої з єдиного центра діяльності органів державної влади й місцевого самоврядування, що спрямована на захист державних інтересів і забезпечення інформаційної безпеки людини, суспільства й держави в інформаційній сфері в умовах реальної небезпеки розв'язання учасниками інформаційного протиборства інформаційної війни.

Державна система протидії загрозам національній безпеці держави в інформаційній сфері може складатися з наступних основних компонентів.

І. Підсистема протидії інформаційним акціям, операціям, кампаніям на ранніх стадіях їх планування та ведення.

На цю підсистему можуть покладатися такі завдання.

1. Попередження акцій інформаційної кампанії та інформаційних операцій, що містить:

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

безперервний пошук і усунення уразливостей у державній системі інформаційного протиборства та забезпечення інформаційної безпеки;

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

2. Виявлення акцій інформаційної кампанії та інформаційних операцій містить:

безперервний пошук (моніторинг) зовнішніх загроз інформаційній безпеці держави, можливих ознак, слідів і зовнішніх проявів здійснення акцій інформаційної кампанії або операції;

виявлення напрямків експансії іноземних держав в інформаційній сфері;

виявлення інших спроб створення умов для організації прихованого управління системою соціальних, економічних, політичних відносин держави.

3. Припинення акцій інформаційно-психологічної кампанії на ранніх стадіях містить:

нейтралізацію джерел інформаційно-психологічної кампанії;

локалізацію масштабів і ступеня небезпеки інформаційної кампанії.

ІІ. Підсистема оперативного реагування на раптово виявлені акції (заходи) інформаційної кампанії.

Метою створення цієї підсистеми є припинення акцій інформаційної кампанії (операції) у тих випадках, коли дії агресора є раптовими для державної системи протидії, а оперативна обстановка в країні не дозволяє відразу пустити в хід всю систему захисту національних інтересів і забезпечення інформаційної безпеки держави.

Підсистема оперативного реагування на раптово виявлені акції інформаційної кампанії (операції) може складатися з таких основних компонентів:

оперативного штабу, що здійснює керівництво силами й засобами системи оперативного реагування та взаємодією (координацією діяльності) з іншими державними структурами, що не входять у систему;

апарата оперативного штабу - спеціальної структури, створюваної з підрозділів органів державної влади, що беруть участь в інформаційному протиборстві, у результаті тимчасової передачі цих підрозділів до підсистеми швидкого реагування, а також перепідпорядкування їх керівників керівництву оперативного штабу системи - на час особливого періоду (правового режиму надзвичайного або воєнного стану). При цьому підрозділи органів державної влади, включаючись у підсистему швидкого реагування, приводяться до стану, що передбачений заздалегідь розробленим планом, а їх керівники займають відповідні місця у вертикальній системі підпорядкування, в тих випадках, коли ситуація вимагає прийняття негайних рішень;

сил оперативного реагування, що складаються із сил спеціальних, оперативних підрозділів розвід-

ки, контррозвідки та власної безпеки, слідчих органів, підрозділів безпосередньої підтримки сил інформаційно-психологічних операцій, підрозділів антикризового управління;

підрозділів роботи зі ЗМІ;

спеціальних захищених систем зв'язку та систем автоматизованого управління.

III. Підсистема сил та засобів інформаційних операцій.

Складається із визначених сил та засобів підготовки та ведення інформаційних операцій.

Ключову роль у побудові та функціонуванні державної системи протидії інформаційним загрозам відіграють центральні органи виконавчої влади.

Основними завданнями центральних органів виконавчої влади в галузі протидії інформаційним акціям (операціям, кампаніям) можуть бути:

розробка пропозицій з визначення державної політики України в галузі інформаційного протиборства, прогнозування, виявлення та оцінка джерел і характеру загроз застосування проти України засобів і методів інформаційного протиборства;

збір розвідувальної інформації про використовувані та перспективні інформаційні технології об'єктів інформаційної сфери конфронтуючої сторони;

захист воєнно-політичного керівництва України, а також індивідуальної, групової та масової свідомості її населення від застосування конфронтуючою стороною інформаційно-психологічних та інформаційно-технічних засобів і методів впливу;

організація протидії антиукраїнській пропаганді, проведеної, у тому числі, інформаційно-психологічними засобами й методами впливу;

захист інформаційної інфраструктури України від застосування конфронтуючою стороною інформаційно-технічних засобів і методів впливу;

розробка моделі загроз національним інтересам в інформаційній сфері, заснованої на проведенні глибоких і різнобічних наукових досліджень. Створення такої моделі могло б надати процесу пошуку, визначення й класифікації вже існуючих загроз і їх проявів (моніторингу загроз) цілеспрямований характер, а розробка методичних рекомендацій з виявлення загроз і відстеженню розвитку загрозливих ситуацій стала б для органів виконавчої влади, що займаються забезпеченням інформаційної безпеки, надійним інструментом, який багаторазово підвищує ефективність відповідних заходів;

створення й розробка стратегії проведення інформаційних операцій за мирного часу і в особливий період (при різних ступенях ескалації напруженості міжнародних відносин);

розробка нормативно-правової бази з питань забезпечення інформаційної безпеки України в особливий період;

створення системи оперативного реагування на раптові (зненацька виявлені) інформаційні атаки, здатної своїми діями скувати противника, змусити його відмовитися від всіх або хоча б частини своїх планів, перехопити ініціативу й створити найбільш сприятливі умови для нанесення контрудару;

створення системи забезпечення безпеки комп'ютерних систем управління Збройними Силами (ЗС) України.

Висновки

Державна система протидії інформаційним загрозам є системою погодженої, цілеспрямованої, керованої з єдиного центра діяльності органів державної влади й місцевого самоврядування, що спрямована на захист державних інтересів і забезпечення інформаційної безпеки людини, суспільства й держави в інформаційній сфері в умовах реальної небезпеки розв'язання учасниками інформаційного протиборства інформаційної війни. Вона може складатися з підсистем протидії інформаційним акціям, операціям, кампаніям на ранніх стадіях їх планування та ведення, оперативного реагування на раптово виявлені акції (заходи) інформаційної кампанії та підсистеми сил та засобів інформаційних операцій.

Така система дозволить своєчасно виявляти загрози інформаційній безпеці, мобілізовувати визначені сили та засоби для захисту державних інтересів, протидії агресії в кожній з її форм, а також організовувати протидію акціям інформаційної агресії на ранніх стадіях виникнення конфлікту, оперативно реагувати на раптово виявлені загрози.

Список літератури

1. Основи стратегії національної безпеки та оборони держави: підруч. / О.П. Дузь-Крятченко, Т.М. Дзюба, А.О. Рось та ін. – К.: НУОУ, 2010. – 591 с.

2. Левченко О.В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки / О.В Левченко // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 3 (20). – С. 47 – 50.

3. Морально-психологічне забезпечення у Збройних Силах України: підр. у 2-х ч. Ч.1. / [В.М. Вілко, В.М. Грицюк, В.Г. Дикун та ін.]. – К.: НУОУ, 2012. – 464 с.

4. Горбулін В.П Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: моногр. / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

5. Радковець Ю.І. Погляди на створення системи інформаційної безпеки України та її Збройних Сил / Ю.І. Радковець, О.В. Левченко, О.М. Косогов // Наука і оборона. – 2014. – № 1. – С. 38–41.

Надійшла до редколегії 30.09.2015

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

ПОДХОД К ПОСТРОЕНИЮ ГОСУДОРСТВЕННОЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ УГРОЗАМ В ОСОБЫЙ ПЕРИОД

А.Н. Косогов

На основе анализа сущности противодействия информационным угрозам государства в особый период предлагается подход к построению государственной системы противодействия информационным угрозам как согласованной, целенаправленной, управляемой с единого центра деятельности центральных органов исполнительной власти и местного самоуправления, которая направлена на обеспечение информационной безопасности личности, общества и государства в условиях начала информационной агрессии. Выделены основные составные части данной системы и основные задачи центральных органов исполнительной власти в области противодействия информационным акциям (операциям, кампаниям).

Ключевые слова: *информационная безопасность, угрозы информационной безопасности, государственная система противодействия, особый период.*

APPROACH TO THE CONSTRUCTION OF THE STATE SYSTEM OF RESISTING INFORMATIONAL THREATS IN THE SPECIAL PERIOD

O.M. Kosogov

Based on analysis of the essence of counter information threat to the state in a special period, an approach to the construction of the state system of counteraction to information threats as a coherent, focused, controlled from a single center of activity of central executive bodies and local self-government, which aims to ensure the information security of individuals, society and the state conditions of the early information aggression. The basic components of the system and basic tasks of the central executive authorities in combating shares information (operations, campaigns).

Keywords*: information security, information security threats, the state system of counteraction, a special period.*