

Ю. О. Колос, О. В. Манько, В. І. Шестаков, Ю. І. Міхєєв

**МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА
В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ
В ІНТЕРЕСАХ БЕЗПЕКИ ДЕРЖАВИ**

У роботі проводиться аналіз та систематизація інформаційних загроз для безпеки держави, які можуть діяти з використанням інформаційно-телекомунікаційних мереж. Узагальнено можливості ведення інформаційного протиборства в інформаційно-телекомунікаційних мережах. Запропоновано модель системи інформаційного протиборства в цій сфері.

Актуальність дослідження. Розвиток і широке застосування інформаційно-телекомунікаційних мереж (ІТМ) за останні роки є стійкою тенденцією світового прогресу. Рушійною силою глобальної комунікації став Інтернет – світова комп’ютерна мережа. Стрімке впровадження і використання ІТМ є одним із вирішальних чинників зростання ролі інформаційного протиборства. Досвід сучасних війн та конфліктів показує [1], що методами інформаційного протиборства з використанням ІТМ можна впливати на безпеку держави. Важливість ІТМ як об’єктів та засобів інформаційного протиборства полягає в їх широкому розповсюдженні, можливості впливу через них на автоматизовані системи управління, системи підтримки та прийняття рішень, користувачів інформації, громадську думку, свідомість і поведінку певних груп людей чи населення в цілому.

Огляд останніх досліджень і публікацій. У [2 – 4] розглядаються проблемні питання забезпечення безпеки держави в умовах широкого застосування ІТМ та використання технологій інформаційного протиборства, до яких належать:

відсутність цілісної системи органів державного та військового управління, що призначені для забезпечення безпеки держави у відповідній сфері;

комерціалізація телерадіомереж, які широко використовуються як основні чинники маніпулювання свідомістю суспільства;

наявність розбіжності в розумінні та застосуванні системоутворюючих понять інформаційного права;

використання створених за межами України програмно-апаратних засобів під час організації та розвитку ІТМ;

порушення встановленого регламенту збору, обробки та передачі інформації в ІТМ спеціального призначення, що супроводжуються помилками персоналу;

нерозуміння посадовими особами важливості інформаційного протиборства та його негативних наслідків.

У [5] відзначається, що існуюча законодавча база, яка регулює інформаційну безпеку держави, діяльність органів державного та військового управління у сфері інформаційної безпеки, на сьогоднішній день не здатні повною мірою протистояти викликам та загрозам в інформаційному середовищі країни.

Формулювання завдань дослідження. Виходячи із зазначеного, актуальною є розробка методологічних засад інформаційного протиборства в ІТМ в інтересах безпеки держави, яка передбачає вирішення таких завдань: систематизацію інформаційних загроз; обґрунтування можливостей та визначення принципів і видів інформаційного протиборства в ІТМ.

Виклад основного матеріалу. Інформаційне протиборство в ІТМ в інтересах безпеки держави – це реальний вид протиборства, який характеризується впливом на ІТМ, маніпулюванням інформаційними ресурсами, а через це – впливом на ефективність управління державою, свідомість і поведінку особового складу збройних сил (ЗС), відношення населення до військової політики та діяльності ЗС, а також захистом своїх мереж військового призначення, упередженням або нейтралізацією негативного інформаційного та психологічного впливу з використанням ІТМ. Системний аналіз можливостей інформаційного протиборства з використанням ІТМ та досвіду сучасних військових конфліктів дозволяє визначити такі види загроз безпеці держави [2]:

- виток закритої інформації;
- обмеження або викривлення службової інформації;
- зниження ефективності управління у військовій сфері;
- зниження морально-психологічної стійкості особового складу ЗС України та населення.

Канали реалізації загроз безпеці держави шляхом інформаційного протиборства в ІТМ зображені на рис. 1.



Рис. 1

Для організації та ведення інформаційного протиборства в ІТМ необхідно дотримуватись таких основних принципів: безперервності, достовірності отримання та цілеспрямованості подачі інформації, прихованості, комплексності, раптовості проведення наступальних дій, оперативності.

Безперервність передбачає постійне проведення дій та заходів інформаційного протиборства в ІТМ як у мирний, так і воєнний час, у будь-яких умовах обстановки.

Комплексність полягає у всебічному використанні ІТМ в інтересах безпеки держави як шляхом добування необхідної інформації так і активного впливу на елементи мережі та інформаційне середовище, а вже через нього на свідомість, поведінку осіб, груп людей, населення, боєздатність та боєготовність ЗС.

Під достовірністю отримання та цілеспрямованістю подачі інформації розуміють, з одного боку, її збирання, добування, уточнення, перевірку з використанням ІТМ для відтворення обстановки максимально наближеної до реальної, з іншого – видачу інформації в ІТМ в інтересах вирішуваних завдань.

Прихованість полягає у непомітному для протиборчої сторони добуванні інформації, підготовці до активних дій, надійному захисті даних, що впливає на безпеку держави.

Раптовість наступальних дій вимагає проведення таких заходів і в такі терміни, які не очікуються противником.

Оперативність передбачає негайне реагування на зміни структури ІТМ та їх інформаційних ресурсів, які стосуються безпеки держави, випередження протиборчої сторони у часі проведення розвідки, захисту та наступу.

Ведення інформаційного протиборства в ІТМ в інтересах безпеки держави здійснюється певною системою – комплексом людських, матеріальних й інформаційних ресурсів, технічних засобів, технологій, процедур, організаційних заходів та методів. Модель системи інформаційного протиборства в ІТМ можна зобразити схематично (рис. 2).

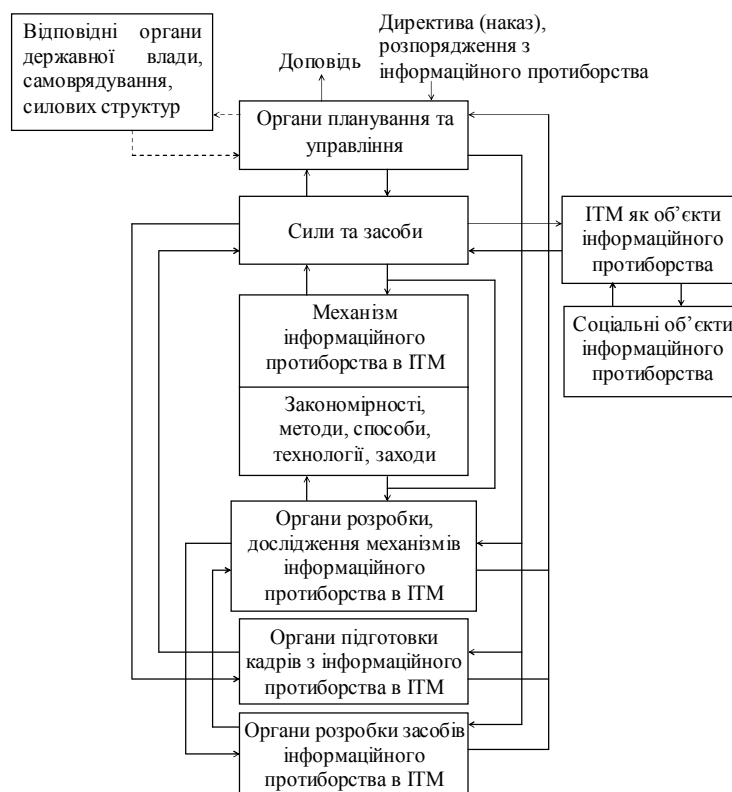


Рис. 2

До основних видів інформаційного протиборства в ІТМ належать [1, 6]:

інформаційна розвідка – це організовані дії щодо доступу до інформаційних ресурсів ІТМ, їх обробки для отримання інформації про військовий потенціал противника, наміри, методи, способи, прийоми його дій; дані про осіб, що приймають рішення, конфлікти, негативні явища у протидіючої сторони, які можна використати;

інформаційний наступ – це організовані впливи на ІТМ противника з метою зниження ефективності та дезорганізації військового управління, блокування інформаційного забезпечення або введення в оману керівних державних органів, інформаційно-психологічного впливу (ІПсВ) через мережі для зниження морально-психологічної стійкості військ противника, позбавлення їх підтримки населенням;

інформаційний захист – це організовані дії, які спрямовані на запобігання несанкціонованому заволодінню інформацією у своїх мережах, виявлення та нейтралізацію деструктивних впливів на ІТМ та через них.

Інформаційна розвідка може проводитись шляхом спостереження та аналізу структури, режимів роботи та інформаційних ресурсів ІТМ. Проблемними питаннями на сьогодні є створення системи збору інформаційних повідомлень, які передаються ІТМ, підготовка фахівців та створення методик, технологій і програмних засобів для обробки різномовних, різнотипних інформаційних повідомлень з метою виявлення загроз безпеці держави, запобігання підготовці та здійсненню деструктивного інформаційно-психологічного впливу.

На рис. 3 наведено способи здійснення інформаційного наступу в ІТМ.

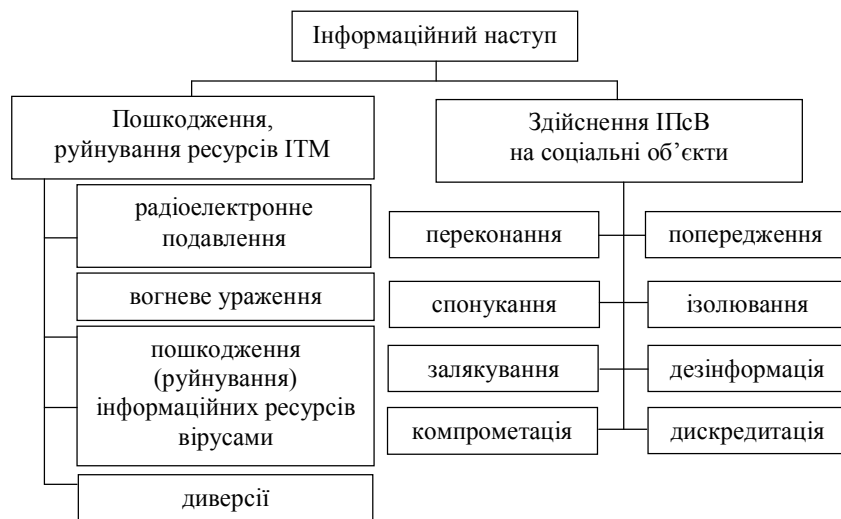


Рис. 3

Відповідно до зазначених способів наступу необхідно виділити проблемні питання:
створення технічних та програмних засобів для реалізації каналів витоку інформації;
створення засобів дії на ІТМ шляхом опромінювання або через мережі живлення;
створення програмно-алгоритмічного забезпечення для здійснення доступу до ІТМ, модифікації їх інформаційних ресурсів;

моніторинг існуючих та розробка нових програмних продуктів для обмеження функціональності ІТМ;

розробка й удосконалення методик та технологій реалізації різних способів проведення ІПсВ;

створення системи моніторингу об'єктів наступу;
розробка методик, інструкцій, настанов щодо проведення атак на ІТМ.
Основні завдання інформаційного захисту власних ІТМ наведено на рис. 4.

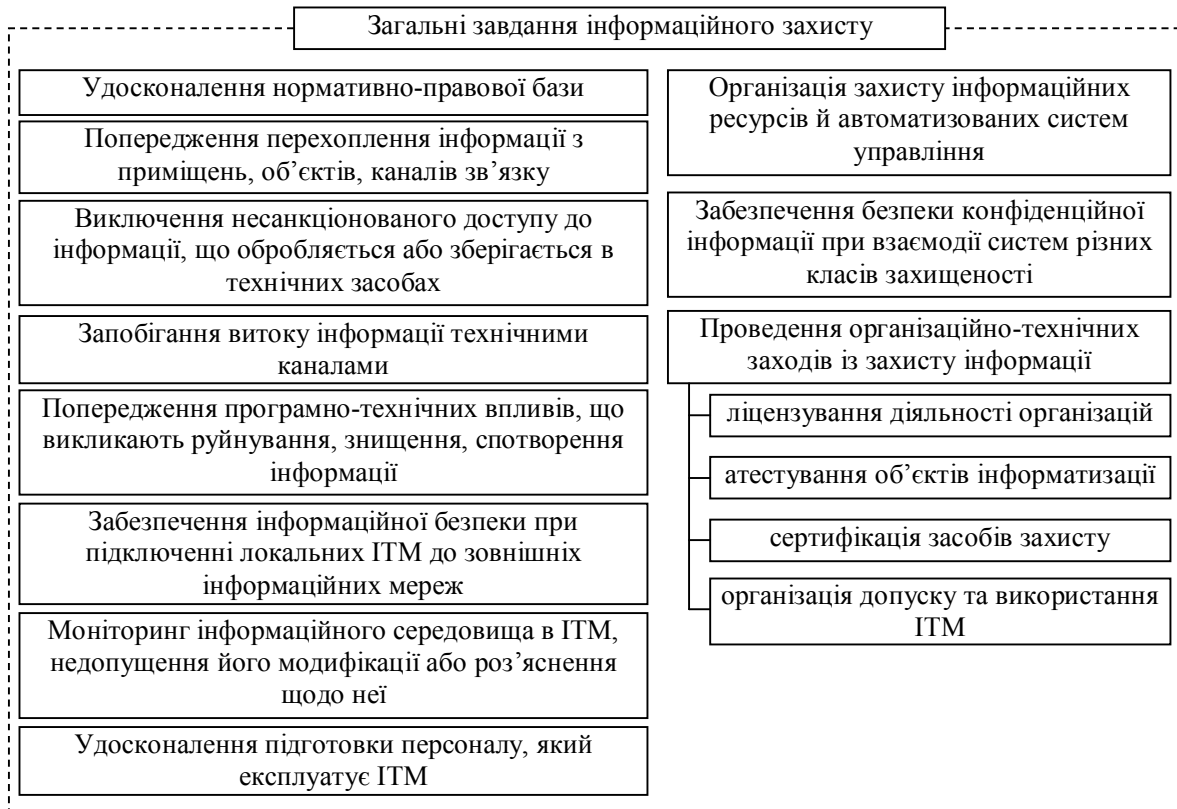


Рис. 4

Також важливим завданням щодо захисту є своєчасне виявлення та нейтралізація загроз ІПсВ через ІТМ, серед яких вирізняють:

здійснення деструктивного ідеологічного впливу на органи управління безпекою держави, на особовий склад ЗС та населення;

маніпулювання громадською думкою, дестабілізація ставлення громадськості до ЗС, розпалення недовіри особового складу до керівництва, стимулювання підозри, ворожнечі між різними прошарками ЗС;

зниження рівня інформаційного забезпечення органів влади та військового управління, інспірація помилкових рішень;

підрив міжнародного авторитету діяльності держави, її ЗС, заходів, дій у військовій сфері;

формування умов до поразки, втрати волі до протистояння та перемоги;

підрив морального духу населення і, як наслідок, зниження бойового потенціалу;

дискредитація дій керівництва щодо безпеки держави та військового управління, ініціювання актів протесту проти діяльності ЗС.

Висновки та перспективи подальших досліджень. Таким чином, інформаційне протистояння в ІТМ – це об'єктивна реальність сьогодення. Вона несе загрози безпеці держави, зокрема у військовій сфері. Для протистояння цим загрозам необхідно створити систему інформаційного протистояння в ІТМ, модель якої розглянута. Досліджено також проблемні питання та завдання, які необхідно вирішити для організації та ефективного ведення інформаційного протистояння в ІТМ.

У подальшому планується розробити конкретні методики та технології інформаційного протидіювання в ІТМ.

СПИСОК ЛІТЕРАТУРИ

1. Прибутко П. С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П. С. Прибутко, І. Б. Лук'янець. – К. : видавець ПАЛІВОДА А. В., 2007. – 252 с.
2. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : МК-Прес, 2005. – 432 с.
3. Ведущие страны разрабатывают информационное оружие [Электронный ресурс]. – Режим доступа : <http://www.crime-research.ru/articles/cyberwar/>.
4. Даник Ю. Г. Національна безпека і запобігання критичним ситуаціям : монографія / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін. – Житомир: Рута, 2006. – 388 с.
5. Форми та методи забезпечення інформаційної безпеки держави : зб. матеріалів Міжнар. наук.-практ. конф., 13 берез. 2008 р. – К. : видавець Захаренко В. О., 2008. – 216 с.
6. Манойло А. В. Информационно-психологические операции как организационная форма реализации концепции информационно-психологической войны / А. В. Манойло, Д. Б. Фролов // Проблемы информационной безопасности. Компьютерные системы. – 2003. – № 2. – С. 7 – 14.

Подано 04.11.09

Ю. А. Колос, О. В. Манько, Ю. И. Михеев, В. И. Шестаков

В статье представлены результаты анализа и систематизации информационных угроз для безопасности государства, которые могут действовать с использованием информационно-телекоммуникационных сетей. Обобщены возможности ведения информационного противоборства в информационно-телекоммуникационных сетях. Предложена модель системы информационного противоборства в этой сфере.

Y. O. Kolos, O. V. Manko, Y. I. Mikheev, V. I. Shestakov

In the article are presented results of analysis and systematizations of informative threats for state safeties the which can conducted with the use of informational-telekonication networks. Possibilities of conduct of informative war are generalized in informational-telecommunication networks. The model of the system of informative war is offered in informational-telecommunication networks.