УДК 34:316.774

Г. В. Форос, канд. юрид. наук, доцент

Одеського національного університету імені І. І. Мечникова
Французький бульвар, 24/26, Одеса, 65058, Україна

СУЧАСНИЙ СТАН РОЗВИТКУ ІНФОРМАЦІЙНОЇ ПРОТИДІЇ

В статті надано визначення поняття «інформаційна протидія», встановлені принципові розбіжності з такими поняттями як «інформаційна війна», «інформаційна боротьба», наведено класифікацію видів інформаційної зброї, а також встановлено взаємозв'язок цих понять із поняттям «інформаційна безпека».

Ключові слова: інформаційна протидія, інформаційна війна, інформаційна зброя, інформаційна боротьба, інформаційна безпека.

Початок нового тисячоліття характеризується глобалізацією світових економічних і політичних процесів, невід'ємною складовою яких є розробка та впровадження сучасних інформаційних технологій. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем інформаційної інфраструктури. Інформація стала чинником, який визначає стратегічні напрямки державної політики, може призвести до значних технологічних аварій, військових конфліктів, дезорганізувати державне управління, роботу наукових установ та фінансову систему, сприяє появі нових напрямків злочинної діяльності. Під впливом інформаційних атак може змінюватися світогляд та мораль окремих осіб та їх спільнот, нав'язуватися чужі ідеї, мотиви, інтереси. В сучасній науковій та спеціальній літературі, засобах масової інформації останнім часом все частіше зустрічаються такі поняття як «інформаційна протидія», «інформаційна війна», «інформаційна боротьба», «інформаційне протиборство», що свідчить про те, що ці категорії вийшли на рівень суспільної свідомості. На наш погляд, це пов'язано з тенденціями розвитку інформаційного впливу на громадян, суспільство та державу. Якщо XX сторіччя називали сторіччям кібернетики, то XXI сторіччя — це, безумовно, інформаційне сторіччя.

Досліджуючи інформаційну протидію, учені та фахівці в основному використовують такі поняття як «інформаційна боротьба», «інформаційна війна» та «інформаційна зброя». Багато хто ототожнює ці поняття, що є грубою помилкою, також інтерес викликають взаємозв'язки цих понять із поняттям «інформаційна безпека».

На сьогодні саме інформаційні війни становлять найбільшу небезпеку нормальному функціонуванню системи органів державної влади. Це і зумовлює детальний розгляд нами питань щодо визначення поняття та встановлення суттєвих ознак інформаційної війни.

Поняття «інформаційна війна» виникає з нових підходів до застосування інформації, визначення її ролі та місця. Можна виділити два визначення поняття інформаційної війни: гуманітарна і технічна. Наприклад, Павлютенкова М. зазначає, що у гуманітарному сенсі інформаційна війна являє собою активні методи трансформації інформаційного простору, що знаходять відображення у системі нав'язування моделей світу, які покликані забезпечити бажані типи поведінки, атаках на структури породження інформації — процеси міркувань [1, 21].

Що стосується іншого розуміння поняття інформаційної війни, тобто технічного, то тут обов'язковою умовою є те, що ведення інформаційної війни є результатом

узгодженої діяльності по використанню інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності. При цьому інформаційна війна включає такі дії: здійснення впливу на інфраструктуру систем життєзабезпечення — телекомунікації, транспортні мережі, електростанції тощо; хакінг — злам і використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Взагалі існує багато визначень «інформаційної війни», в яких вона тлумачиться як комплекс заходів і операцій, здійснюваних у конфліктних ситуаціях, коли інформація є водночас зброєю, ресурсом і ціллю. Цікавою є думка, що це інформаційне протиборство з метою нанесення збитку критично важливим структурам супротивника, підриву його політичної і соціальної систем, а також стабілізації товариства і держави супротивника. Сутність інформаційного протиборства полягає в тому, що це форма міждержавного суперництва, реалізована за допомогою інформаційного впливу на систему керування інших держав і їхніх збройних сил, а також на політичне і військове керівництво і товариство загалом, інформаційну інфраструктуру і засоби масової інформації цих держав для досягнення вигідних для себе цілей при одночасному захисті від аналогічних дій у своєму інформаційному просторі.

Ми дотримуємося позиції, відповідно до якої інформаційне протиборство — це форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів впливу на інформаційне поле супротивника, а також захисту власного інформаційного поля в інтересах досягнення поставлених цілей. Враховуючи таке визначення, можна зазначити, що інформаційне протиборство включає в себе три незмінні складові: вплив, аналіз, протиборство. Причому основним елементом, від якого залежить ефективність кампанії, є аналіз, мета якого полягає в оцінці, стратегічному прогнозуванні та плануванні в аспектах внутріполітичного та зовнішньополітичного положення.

На Заході інформаційну війну визначають як «нефізичну атаку на інформацію, інформаційні процеси та інформаційну інфраструктуру», причому «ціллю інформаційної війни є вплив на систему знань та уявлень зовнішнього супротивника». Під знанням тут розуміється об'єктивна інформація, загальна для всіх, а під уявленнями — інформація, що носить суб'єктивний характер.

Основним інструментом ведення інформаційної війни є інформаційна зброя, тобто це комплекс технічних та інших засобів, методів і технологій, спрямованих на встановлення контролю над інформаційними ресурсами, втручання в роботу систем керування, інформаційних мереж, систем зв'язку, поширення вигідної інформації та дезінформації.

До інформаційної зброї частіше відносять засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, незважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів, а також інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи таким чином на думку суспільства та на функціонування органів влади.

Виходячи зі змісту нашого дослідження, об'єктами впливу інформаційної зброї можуть бути: інформаційно-аналітичні системи, інформаційно-технічні системи, які включають канали та засоби зв'язку, інформаційні ресурси, державні засоби масової інформації, а також психіка конкретного співробітника органу. Необхідно підкреслити, що інформаційна зброя є інструментом встановлення контролю над інформаційними ресурсами потенційного супротивника, тому інформаційна зброя втручається в роботу систем управління, зв'язку, інформаційних систем та ін. з метою порушення їх працездатності аж до повного виведення їх з ладу, вилучення, перекручення даних, які в них містяться, або цілеспрямованого введення

спеціальної інформації. Часто інформаційна зброя виступає в ролі поширювача дезінформації в системі формування суспільної свідомості й прийняття рішень. Особливу небезпеку в цьому випадку становлять дані, що надходять для органів влади, тому що від їх достовірності залежать поінформованість і здатність певних органів приймати вірні рішення та вживати своєчасні заходи по управлінню державою. Також до інформаційної зброї відносять і сукупність спеціальних засобів та способів впливу на психіку суспільства та держави в цілому.

Таким чином, ми можемо згрупувати види інформаційної зброї, яка використовується в інформаційній війні:

– засоби пропагандистсько-психологічного впливу (через засоби масової інформації, Інтернет та інші канали);

– засоби програмно-математичного впливу (комп'ютерні віруси, різноманітні логічні пристрої по типу логічних «бомб» та троянських коней, засоби впливу на комп'ютерні мережі);

– засоби психологічного впливу (голографічні зображення в атмосфері, синтезатори голосів відомих політичних діячів та інше);

– психотропна зброя (методи програмування поведінки, методи парапсихології та біоенергоінформатики);

– засоби, засновані на впливі полів різної природи (акустична зброя, електромагнітні ураження, радіоелектронне придушення).

Для проведення будь-якої інформаційної кампанії як в міжнародних відносинах, так і на внутрішньому інформаційному полі, необхідно враховувати особливості конкретного інформаційного простору. Спочатку необхідно розшукати вразливі місця в інформаційному просторі і тільки потім переходити до рішучих дій. Інформаційна зброя повинна враховувати варіанти протидії — і чим більше варіантів протидії враховано, тим більша вірогідність успіху в тій чи іншій інформаційній агресії. Також варто підкреслити, що специфікою інформаційної війни (інформаційного протиборства) є те, що вона ведеться, на відміну від збройної боротьби, як у мирний, так і у воєнний час. Вона націлена на всі можливості та фактори ураження, які неминуче виникають при зростанні залежності від інформації, а також на використання інформації у найрізноманітніших конфліктах. Об'єктом уваги стають інформаційні системи (включаючи відповідні лінії передач, центри обробки та людський фактор цих систем).

Інформаційна війна може бути спрямована проти трьох елементів: комп'ютер; програмне забезпечення; людина. Крім того, неможливо заперечувати й того факту, що одним з головних завдань інформаційної війни є подавлення в людині морального творчого початку. Технології інформаційних війн певним чином зрівняли індустріальні, постіндустріальні і доіндустріальні країни: всі вони мають доступ до інструментарію, необхідного для ведення інформаційної війни, отже виступають як суб'єктами, так і об'єктами інформаційної війни, а відповідно і забезпечення внутрішньої інформаційної безпеки.

Інформаційна війна, інформаційне протиборство й інформаційна боротьба є проявами одного більш широкого поняття — загрози інформаційній безпеці. Як свідчить аналіз джерел, ядром методології інформаційної безпеки є поняття інформаційної боротьби, триєдина сутність якого відбита у наступних взаємопов'язаних визначеннях:

– інформаційна боротьба — це об'єктивно існуюча форма прояву відносин між суб'єктами при вирішенні ними завдань, що містять елементи конфліктності різної природи на інформаційному рівні;

– інформаційна боротьба — це наука про механізми, прийоми, методи та засоби інформаційного протиборства;

– інформаційна боротьба — це комплекс заходів, спрямованих на вирішення завдань, що стоять перед суб'єктом, методами і засобами боротьби.

Існування інформаційної боротьби обумовлене як існуванням інформації, так і природністю процесу її використання, її властивостей для вирішення різних завдань. Із визначення інформаційної боротьби випливає, що вона по суті своїй неагресивна, на відміну від інформаційної війни. Метою інформаційної боротьби і забезпечення переваги у вирішенні певних завдань однієї сторони над іншою за рахунок досягнення вищості на інформаційному рівні. В основному вона виявляється в двох основних напрямках: боротьба за вірогідну інформацію і боротьба за вплив на інформаційне уявлення протидіючої сторони.

Інформаційна війна, інформаційне протиборство й інформаційна боротьба є проявами одного більш широкого поняття — загрози інформаційній безпеці. Слід зазначити, що аналізу змісту поняття «інформаційна безпека» зазвичай дослідники приділяють значну увагу, у той час як поняття «небезпека» і «загроза» розглядаються дещо спрощено і здебільшого у звуженому плані, відірваному від контексту поняття «інформаційна безпека». Найбільш широко загрози інформаційним ресурсам системи органів державної влади можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній. Виникнення загрози, тобто знаходження джерела актуалізації певних подій у загрози, характеризується таким елементом, як вразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз.

Інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання [2, 56; 3, 67], вважаємо, що можна виділити такі види загроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення цілісності інформаційних ресурсів, збій у роботі обладнання.

Виходячи із зазначеного, можна зробити висновок, що проблематика захисту інформаційного простору, протидії інформаційній зброї, розробки стратегії інформаційної боротьби у науці й практиці України ще перебуває на стадії становлення і потребує ґрунтовного наукового забезпечення, зокрема систематизації, в тому числі на рівні організаційно-правового аспекту.

Література

1. Павлютенкова М. Информационная война — реальная угроза или современный миф? // Власть. — 2001. — № 12. — С. 19–23.

2. Зіма І. І., Ніколаєв І. М. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів) // Наука і оборона. — 1998. — № 1. — С. 56–58.

3. Рибак М. І., Атрохов А. В. До питання про інформаційні війни // Наука і оборона. — 1998. — № 2. — С. 65–68.

А. В. Форос, канд. юрид. наук, доцент

Одесского национального университета имени И. И. Мечникова
Французский бульвар, 24/26, Одесса, 65058, Украина

СОВРЕМЕННОЕ СОСТОЯНИЕ РАЗВИТИЯ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ

РЕЗЮМЕ

В статье проанализировано понятие «информационное противодействие», установлены принципиальные различия с такими понятиями как «информационная война», «информационная борьба», приведена классификация видов информационного оружия, а также установлена взаимосвязь этих понятий с понятием «информационная безопасность».

Ключевые слова: информационное противодействие, информационная война, информационное оружие, информационная борьба, информационная безопасность.