Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

Сучасний стан інформаційної протидії

Форос Г.В.
кандидат юридичних наук., доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
Корсун М.М.
слухач магістратури ННІЗДН

В сучасній науковій та спеціальній літературі, засобах масової інформації все частіше зустрічаються такі поняття як «інформаційна протидія», «інформаційна війна», «інформаційна боротьба», «інформаційне протиборіння», що свідчить про те, що ці категорії вийшли на рівень суспільної свідомості. Досліджуючи інформаційну протидію учені та фахівці в основному використовують такі поняття як «інформаційна боротьба», «інформаційна війна» та «інформаційна зброя».

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.

На нашу думку, 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.

До інформаційної зброї частіше відносять, засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи 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.

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.

Інформаційні 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 ї 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 протиборствуючої сторони.

Інформаційні 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.

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. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Монографія / За заг. ред. д-ра юрид. наук Калюжного Р. А. – Запоріжжя: Просвіта, 2001.

2. Хорошко В.О., Чередниченко В.С., Шелест М.Є. Х 80 Основиінформаційноїбезпеки / За ред. проф. В.О. Хорошка. - К.: ДУІКТ, 2008.- 186 с.

3. Цимбалюк В.С. Основи інформаційного права України [Текст]: Навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін. [за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника]. – К.: Знання, 2004. – 274 с.

Правове регулювання обігу інформації з обмеженим доступом

Форос Г.В.
кандидат юридичних наук., доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
Васильєв С.
слухач магістратури ННІЗДН

Науково-технічний прогрес зумовив розвиток у галузі інформаційних технологій, зокрема, в сфері розробки та впровадження програмного забезпечення в діяльність державних органів, розповсюдженість використання інформаційних обліків, а також активність у формування баз персональних даних, що в свою чергу загострило проблему правового регулювання обігу інформації з обмеженим доступом. Доступність інформації обумовлена не лише її юридичним статусом, а й фактичними умовами її використання для різних суб'єктів. Для визначення юридичних аспектів вживається поняття "порядок доступу". За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Для визначення останньої вживається ще закрита, або секретна, тобто така, що з тих чи інших міркувань являє собою таємницю і розповсюдження якої можливе лише за згодою органів, уповноважених контролювати питання пов'язані з цією інформацією.

Обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений. Інформація з обмеженим доступом у свою чергу поділяється на конфіденційну, таємну і службову.

Зростання загроз для інформації, спричинене кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів неправомірного доступу до інформації та впливу на неї, визначає необхідність розвитку захисту інформації, і насамперед, інформації з обмеженим доступом.