УДК 65.012.8(477)

В. М. Абакумов

Загальна характеристика форм та засобів ведення інформаційних війн в Україні

Дано характеристику основних форм та засобів ведення інформаційних війн як однієї із форм реалізації загроз інформаційній безпеці держави з метою вироблення технологій захисту від таких війн.

***

Дана характеристика основных форм и средств ведения информационных войн как одной из форм реализации угроз информационной безопасности государства с целью выработки технологий защиты от таких войн.

***

Characteristic to the main forms and means of conducting informational wars as one of the forms of realizing threatens to informational safety of the state in order to elaborate technologies of protection from such wars is made.

Розширення інформаційного простору та прискорення обігу інформації завдяки новітнім інформаційно-телекомунікаційним технологіям, крім таких позитивних наслідків, як широке розповсюдження та впровадження новітніх інформаційно-телекомунікаційних технологій серед широких верств населення, також сприяє акумуляції протиріч (реальних та тих, що штучно створюються у сфері інформації), посиленню конфліктних процесів інформаційного характеру, внесенню суттєвих корективів до існуючих методів військових, торговельних, економічних конфліктів, оскільки прямі силові методи поступаються перед інформаційними. Така значна кількість протиріч, що виникають у суспільстві з приводу правильного використання інформації, зумовлена, у першу чергу, здатністю інформації впливати на суб'єктів, що її отримують, так сильно, що це може повністю змінити поведінку людини, суспільства або держави в необхідному напрямку. Тобто можна зробити висновок, що існують випадки, коли позитивні властивості інформації та інформаційних технологій, які створювалися на користь людині, суспільству та державі, можуть бути використані в корисних та злочинних цілях, що створюватиме суттєву загрозу інформаційній безпеці.

Таким чином, враховуючи надзвичайну важливість та значущість належного забезпечення інформаційної безпеки людини, суспільства та держави, зокрема шляхом ефективної протидії інформаційним війнам, метою роботи було визначено дослідження основних форм та засобів ведення інформаційних війн як однієї із форм реалізації загроз інформаційній безпеці

держави. Хотілося б підкреслити, що якісний аналіз основних форм, методів та засобів ведення інформаційних війн сприятиме підвищенню ефективності діяльності відповідних органів державної влади України щодо протидії інформаційним війнам та виведенню зазначеної діяльності на якісно новий рівень у відповідності до загальновизнаних європейських стандартів.

У результаті аналізу положень чинного законодавства України (зокрема, Конституції України, законів України «Про основи національної безпеки України» та «Про Концепцію Національної інформатизації» [1–3]), а також праць науковців, присвячених дослідженню інформаційної безпеки та вивченню проблем, що заважають ефективному функціонуванню інформаційної сфери (зокрема, Н. Р. Нижник, Г. П. Ситника, В. Т. Білоуса, Б. А. Кормича, О. В. Литвиненка, В. А. Ліпкана, Ю. Є. Максименка, В. М. Желіховського [4–7]), можна дійти висновку, що, незважаючи на численні наукові дослідження, формування понятійного апарату в інформаційній сфері ще остаточно не завершено, відсутня узгодженість поглядів науковців щодо тлумачення окремих визначень, зокрема інформаційна війна, інформаційне протиборство, інформаційний ресурс, інформаційний продукт, інформаційна зброя, форми інформаційної війни, відсутнє чітке закріплення на законодавчому рівні цих понять.

Перш ніж перейти безпосередньо до вивчення форм та засобів ведення інформаційних війн хотілося б зазначити, що автор розуміє під інформаційною війною. Так, інформаційна війна – це сукупність методів та способів цілеспрямованого впливу суб'єктів-агресорів в умовах інформаційної відкритості на соціальні відносини (відносини людей між собою, відносини в суспільстві та державі), інформаційні ресурси, інформаційно-аналітичні та інформаційно-технічні системи, системи формування масової свідомості та психіки окремої людини з використанням усіх властивостей інформації, інформаційних ресурсів та новітніх інформаційно-телекомунікаційних технологій з метою штучного створення факторів гальмування розвитку людини, суспільства та держави, встановлення контролю над інформаційними ресурсами потенційного супротивника задля отримання переваг у пріоритетних сферах суспільного життя.

Слід звернути увагу і на той факт, що інформаційна війна, як і будь-яка інша дія, може вестися виключно заради досягнення чітко визначених цілей (усвідомлюваних або неусвідомлюваних). Так, на основі вивчення існуючих точок зору щодо переліку цілей, котрі ставляться перед особами, які ведуть або тільки починають вести інформаційну війну (наприклад, В. Е. Разуваєва [8]), можна виділити такі найбільш поширені цілі ведення інформаційних війн в Україні:

– політична дезінформація з боку окремих політичних сил, створення хибних уявлень про геополітичну ситуацію в суспільстві;

– послаблення політичної ролі влади;

– розповсюдження поглядів, що відповідають інтересам конкретної людини, групи людей або різних об'єднань;

– критика духовних ідеалів народів, що мешкають на території певної держави;

– розпалення суперечок між різними соціальними групами (наприклад, національностями або професійними об'єднаннями);

– внесення в суспільну та індивідуальну свідомість ідеологічно ворожих поглядів, думок, уявлень та моралей;

– порушення працездатності або повне виведення з ладу інформаційних систем, систем зв'язку, комунікацій, електростанцій, транспортних мереж, комп'ютерів, вилучення або перекручення даних, цілеспрямоване введення спеціальної інформації (дезінформація), злам та незаконне використання персональних даних, інформації з обмеженим доступом;

– промисловий шпіонаж тощо.

Таким чином, можна дійти такого висновку, що в переважній більшості випадків інформаційна війна може бути спрямована проти людини, ефективної роботи органів державної влади та належного функціонування програмного забезпечення. Звісно, що наведеними вище цілями ведення інформаційних війн не обмежується весь спектр можливих намірів супротивника, але в роботі вважалося за доцільне визначити найбільш поширені та найбільш небезпечні цілі в разі їх досягнення.

Загальновідомим є той факт, що будь-яка мета може досягатися різноманітними засобами; так само і мета інформаційної війни може досягатися за допомогою використання різноманітних засобів – інформаційної зброї. Треба акцентувати увагу на тому, що поняття «інформаційна зброя» слід застосовувати вже після того, як була розпочата діяльність щодо незаконного (спрямованого на нанесення максимальної шкоди) використання інформації та інформаційно-телекомунікаційних технологій. До того часу мова може вестися виключно про інформаційний продукт або інформаційний ресурс. Отже, застосування інформаційного продукту або інформаційного ресурсу (які водночас постають об'єктами цього шкідливого впливу), спрямоване на нанесення максимальної шкоди роботі систем управління та інформаційних систем, перекручення даних або цілеспрямоване введення спеціальної інформації, надає інформаційному продукту або інформаційному ресурсу характеру інформаційної зброї.

Перш ніж перейти безпосередньо до аналізу інформаційної зброї як основного засобу ведення інформаційної війни, хотілося б акцентувати увагу на тому, що не можна ототожнювати такі два поняття, як інформаційний ресурс та інформаційний продукт, оскільки це дві різнопланові категорії. На нашу думку, головною відмінністю інформаційного ресурсу від інформаційного продукту є цілі власника інформації та стан відповідності або невідповідності інформації для потреб конкретного споживача. Таким чином, можна дійти висновку, що інформаційна війна є процесом, під час якого відбувається перероблення інформації (тобто інформаційних ресурсів), цілеспрямоване створення та розповсюдження до конкретного суб'єкта певного інформаційного продукту. Тобто можна стверджувати, що весь сенс інформаційної війни полягає в тому, що під час її ведення не використовується фізичне знищення супротивника в якості засобу досягнення поставленої цілі; інформаційна війна використовує в якості засобів нефізичну зброю та інформаційні засоби переваги над супротивником.

Повертаючись до дослідження засобів ведення інформаційної війни, треба підкреслити, що під інформаційною зброєю розуміється сукупність засобів та технологій, призначених для ведення інформаційної боротьби, впливу на психіку людини, суспільства та держави в цілому, розповсюдження дезінформації в системі формування суспільної свідомості й прийняття рішень; система пристроїв та засобів, призначених для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів) [4, с. 96, 110]. До числа інформаційної зброї відносяться:

– засоби знищення, перекручення або викрадення інформації, незважаючи на існуючі системи захисту, засоби обмеження допуску законних користувачів, засоби дезорганізації роботи технічних засобів та комп'ютерних систем (тобто засоби інформаційно-технічного характеру, до яких можна віднести комп'ютерні віруси, спам, засоби нейтралізації тестових програм);

– засоби, що дезорганізовують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, впливаючи на суспільну думку, життя суспільства або держави, морально-психологічний стан людини (тобто інформаційно-психологічні засоби, під якими можна розуміти засоби зменшення інформаційного обміну в телекомунікаційних мережах, фальсифікація інформації) [4, с. 95–96; 8, с. 14–15].

До числа найбільш поширених видів інформаційної зброї, що застосовуються під час ведення інформаційних війн в Україні,

слід віднести: чутки, шкідливу інформацію, неправдиву інформацію (дезінформацію), недобросовісну рекламну діяльність, засоби інформаційної зброї, що застосовуються в мережі Інтернет (наприклад, масова розсилка попередньо неузгоджених електронних повідомлень з обов'язковою наявністю умислу спричинення шкоди – спам), засоби несанкціонованого збирання інформації, засоби порушення функціонування комп'ютерно-телекомунікаційних мереж і т. ін. У той же час слід акцентувати увагу на тому, що у зв'язку зі стрімким зростанням технічного потенціалу суспільства, прогресуючим розвитком інформаційно-телекомунікаційних технологій, постійно з'являтимуться нові види інформаційної зброї, що, у свою чергу, вимагатиме розроблення нових засобів боротьби із незаконним використанням інформаційної зброї, розроблення та впровадження засобів захисту від агресивних інформаційних дій. Таким чином, уважаємо за необхідне зазначити, що застосування інформаційної зброї (одного або кількох її видів одночасно) обов'язково має враховувати варіанти протидії їй, отже, чим більше буде варіантів протидії інформаційній зброї, тим більше буде шансів на успіх в інформаційній війні. Зважаючи на той факт, що інформаційна війна в Україні знаходиться на стадії становлення, сутність інформаційної війни ще продовжує коригуватися та поступово розвиватися, а різноманітність та розповсюдженість інформаційної зброї ще не досягла такого стану, як у найбільш розвинених країнах світу, цілком логічною постає доцільність вивчення передового досвіду цих країн щодо існуючих видів інформаційної зброї, засобів, що можуть протидіяти цій зброї, та особливостей правового регулювання відносин в інформаційній сфері.

Інформаційну зброю залежно від об'єкта впливу можна розподілити на чотири класи:

– інформаційно-психологічна зброя (зброя, що впливає на психологічний та моральний стан конкретної людини, окремих соціальних груп, суспільства в цілому);

– інформаційно-політична зброя (зброя, що впливає на політичну ситуацію в регіоні);

– інформаційно-технічна, або комп'ютерна, зброя (зброя, що впливає на належну роботу інформаційних масивів, баз даних, систем захисту, телекомунікаційних мереж, комп'ютерних систем, тобто усіх ключових засобів забезпечення життя людини та суспільства і належного функціонування держави);

– інформаційно-шпигунська зброя, або засоби несанкціонованого збирання інформації (зброя, що сприяє незаконному отриманню необхідної інформації, яка міститься в інформаційних базах даних органів державної влади, місцевого самовря-

дування, підприємств, установ чи організацій, а також окремих фізичних осіб).

Зважаючи на безпосередню спрямованість інформаційно-психологічної зброї на людину та різноманітні соціальні групи в роботі вважалося за можливе коротко зупинитися на аналізі цього засобу ведення інформаційної війни. Так, як зазначають В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський, під інформаційно-психологічною зброєю слід розуміти засоби і технології, що реалізовують інформаційні впливи на психіку, свідомість особи, соціальних груп, з метою впровадження необхідних ідеологічних і соціальних установок, формування помилкових стереотипів поводження та прийняття рішень, трансформації в потрібному напрямку їх настроїв, почуттів і волі [4, с. 114]. На сьогодні існує декілька видів психофізичних впливів на психіку особи та окремих соціальних груп, до основних із яких можна віднести: пропагандистський, нейролінгвістичний, психоаналітичний, психотронний, психотропний, психогенний [4, с. 114]. Найбільш поширеними засобами (видами інформаційно-психологічної зброї), з використанням яких може відбуватися інформаційна війна, є безпосереднє спілкування, підготовка, видання та розповсюдження друкованої продукції, виступи в засобах масової інформації, застосування спеціальних технічних засобів тощо.

Необхідно відмітити, що всі види інформаційної зброї можуть застосовуватися як самостійно, так і в сукупності з іншими видами, тобто під час інформаційної війни, що ведеться в одному напрямку, може застосовуватися як один вид інформаційної зброї, так і кілька, або навіть усі види. Звісно, застосування декількох видів інформаційної зброї вимагає розроблення цілої низки заходів, спрямованих на протидію зазначеним засобам, залучення значної кількості фахівців, здатних своєчасно приймати зважені та обґрунтовані, а головне, ефективні рішення, спрямовані на нейтралізацію загроз належному функціонуванню інформаційної сфери, своєчасне врахування всіх варіантів протидії видам інформаційної зброї, що застосовується в конкретному випадку, та передбачення застосування нових видів інформаційної зброї із обов'язковим врахуванням заходів протидії.

Хотілося б підкреслити, що суттєвою відмінністю інформаційної війни від усіх інших суперечок, що виникають в інформаційній сфері, є її безперервний характер, наявність найвищого ступеня інформаційного протиборства та здатність проявляти себе в найрізноманітніших формах, до числа яких, у першу чергу, слід віднести інформаційні війни в політиці, у системі державного управління, економічні, ідеологічні, психоло-

гічні (психотропні та психотронні) інформаційні війни, атаки на комп'ютерні мережі, штабні війни, сприяння опозиційним або дисидентським рухам тощо. Зважаючи на тематичну спрямованість нашого дослідження коротко зупинимося на аналізі окремих форм.

Ефективність політичних інформаційних війн уже тривалий час знаходиться поза конкуренцією, випадки ведення інформаційних війн усе частіше входять до системи сучасних відносин між учасниками політичного життя суспільства та держави. Таку значущість інформаційна війна в політиці набула завдяки поширенню демократичних інститутів і, як наслідок, залежності політичних рішень від думки громадськості. Це означає, що зараз для прийняття конкретного рішення для учасника політичного життя суспільства не є достатнім аналіз питання вузьким колом професіоналів, необхідно також здобути схвалення з боку цільової аудиторії, у якості якої може виступати як населення в цілому (мешканці певної територіальної частини), так і окремі групи населення (за різними ознаками: соціальними, культурними, професійними тощо). Звісно, частіше за все інформаційні війни в політиці розпочинаються під час передвиборчої кампанії, коли з подвійною силою активізуються основні учасники інформаційної війни, що представляють різноманітні фінансово-промислові групи (олігархи, крупні банки, нафтові та газові компанії), що намагаються отримати контроль над фінансовими потоками шляхом висунення до владних структур своїх представників.

До універсальних технологій ведення інформаційних війн у політиці відносяться публічні дискусії та групові обговорення, виступи на мітингах і демонстраціях, у засобах масової інформації, у групових та міжособистісних конфліктах, що характеризуються достатньо високим ефектом та впливом на психіку людини. Інструментом, що частіше за все використовується під час ведення інформаційних війн у політиці, є правильне кодування інформації, яка викликає очікувані емоції та мотивує раніше заплановані ініціатором інформаційної війни дії. Як зазначає Д. О. Кучумов [9, с. 17], правильне кодування інформації під час ведення інформаційної війни в політиці залежить, у першу чергу, від: вибору та конструювання слів та висловлювань, створення нових слів та висловлювань, ретельного вибору граматичної форми, вибору черговості, логічних операцій, обов'язкового врахування звукової форми, зваженого вибору макроструктур, когнітивних операцій тощо.

Але хотілося б нагадати, що до органів державної влади внаслідок проведення перевиборчих кампаній мають приходити, перш за все, кваліфіковані фахівці, люди, які будуть ефективно

виконувати свою справу, незважаючи на «вказівки зверху», від чого, власне, і залежить майбутнє України. Саме тому, уважаємо за доцільне акцентувати увагу на тому, що інформаційні війни в політиці несуть значну загрозу належному функціонуванню суспільства та держави, отже, слід на законодавчому рівні передбачити низку ефективних організаційно-правових заходів, спрямованих на ліквідацію загроз, що несуть у собі політичні інформаційні війни, недопущення їх виникнення або введення відповідальності за заважання належному функціонуванню органів державної влади та місцевого самоврядування.

За умов сучасного інформаційного суспільства в Україні процес управління соціальними системами реалізується за допомогою комплексних технологій інформаційно-психологічного впливу. Психологічний вплив слід розуміти як один із способів здійснення впливу на людину або групи людей, що застосовується з метою зміни ідеологічних та психологічних структур їх свідомості та підсвідомості, трансформації емоційних станів, стимулювання певних типів поведінки з використанням різноманітних способів психологічного примусу [10, с. 97]. Комплексне використання різних способів психологічного примусу людей у вигляді системи психологічних операцій, пропагандистських акцій та рекламних кампаній, скоординованих у часі й просторі, постає одним із найпоширеніших засобів політичної боротьби та притаманне внутрішньополітичній діяльності. Інформаційно-психологічний вплив, що застосовується з метою заважання ефективному функціонуванню інформаційної сфери в ході інформаційних війн, може реалізовуватися шляхом впливу вербальними засобами, друкованими засобами, за допомогою радіо, телебачення й комп'ютерної техніки на конкретні сфери психіки окремої людини, групи людей та суспільної свідомості в цілому. До основних способів та форм інформаційно-психологічного впливу можна віднести наступні: афери, махінації, шахрайство, блеф, політичні ігри, містифікації, маніпулятивний вплив, провокації, психологічні й потаємні операції, пропаганда, рекламні кампанії, політична й комерційна реклама, дезінформація тощо.

Погоджуючись з точкою зору О. В. Манойла [10, с. 103–104], треба акцентувати увагу на існуванні таких двох основних видів інформаційно-психологічного впливу, як мотивація та примус. Мотивація об'єкта інформаційно-психологічного впливу – це відкритий для свідомості об'єкта вплив (шляхом переконання, роз'яснення, інформування, обговорення, узгодження, порівняння, виховання, сприяння, підтримки), у результаті чого у свідомості відбувається формування мотивації до вчинення певних дій. Під примусом як видом інформаційно-психологічного

впливу слід розуміти вплив (шляхом державного або громадського примусу, психологічних маніпуляцій, дезінформації, агресивної пропаганди, шантажу), у результаті чого у свідомості об'єкта відбувається формування мотивації до обов'язкового виконання певних вчинків всупереч власній волі або бажання.

Останнім часом інформаційні війни почали активно застосовуватися і в економічній сфері. В Україні інформаційні війни у сфері економіки частіше за все пов'язані не з конкурентною боротьбою за споживача, а з перерозподілом власності, конфліктами власників та директорів, протиборством акціонерів (наприклад, конфлікти на Нікопольському заводі феросплавів, ВАТ «Турбоатом» у Харкові). Особливістю інформаційних війн в економічній сфері навколо крупних промислових підприємств є те, що в якості цільової аудиторії тут виступає дуже вузьке коло партнерів або акціонерів підприємства. Але треба зазначити, що ефективність інформаційних війн у бізнесі дуже рідко постає дійсно результативною, оскільки ці війни незавжди відображаються на економічному стані бізнесу, але завжди на репутації керівника компанії, що, у свою чергу, може проявитися у вигляді суттєвих збитків у довгостроковій перспективі (оскільки в умовах сьогодення іміджева історія набуває не меншого значення, ніж кредитна). До того ж, слід звернути увагу на той факт, що останнім часом дуже часто економічні інформаційні війни пов'язані із веденням політичних інформаційних війн, що дозволяє нам зробити висновок про можливість ведення кількох форм інформаційних війн в одному напрямі.

Таким чином, у результаті проведеного дослідження можна зробити висновок, що вироблення технологій захисту від інформаційних війн є значно важчим заняттям, ніж вироблення технології нападу. Частіше за все як варіант захисту від інформаційної війни застосовуються ігнорування інформаційної війни, виявлення технології нападу, початок активних дій, спрямованих на ліквідацію негативних наслідків, усунення приводу інформаційної війни, подання позову до суду тощо. Але такими діями можна лише підірвати репутацію супротивника, але ж не повною мірою компенсувати збитки, заподіяні інформаційною війною. На нашу думку, з метою максимального компенсування збитків, заподіяних інформаційною війною, слід розробити низку організаційно-правових заходів, спрямованих на недопущення початку інформаційної війни або дієвої боротьби в разі її ведення, а роботу цю необхідно доручити дійсним професіоналам у своїй справі, які будуть працювати над репутацією свого «клієнта» у «мирний» час, створювати максимально широкий кредит довіри у своїх контрагентів (превентивна спрямованість).

Список літератури: **1.** Конституція України : від 28 черв. 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141. **2.** Про основи національної безпеки України : закон України від 19 черв. 2003 р. // Офіційний вісник України. – 2003. – № 29. – Ст. 1433. **3.** Про Концепцію Національної інформатизації : закон України від 4 лют. 1998 р. // Офіційний вісник України. – 1998. – № 10. – Ст. 15. **4.** Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – К. : КНТ, 2006. – 280 с. **5.** Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : навч. посіб. / Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус ; за заг. ред. П. В. Мельника, Н. Р. Нижник. – Ірпінь, 2000. – 304 с. **6.** Кормич Б. А. Правові засади політики інформаційної безпеки України : монографія / Б. А. Кормич. – О. : Юрид. літ., 2003. – 472 с. **7.** Литвиненко О. В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії) : автореф. дис. на здобуття наук. ступеня канд. політолог. наук : спец. 23.00.04 / Литвиненко О. В. – К., 1997. – 18 с. **8.** Разуваев В. Э. Правовые средства противостояния информационным войнам : автореф. дис. на соискание науч. степени канд. юрид. наук : спец. 12.00.14 / Разуваев В. Э. – М., 2007. – 24 с. **9.** Кучумов Д. О. Семантический анализ информационной войны (на примере осетино-ингушского конфликта) : автореф. дис. на соискание науч. степени канд. политолог. наук : спец. 23.00.02 / Кучумов Д. О. – Ростов н/Д, 2007. – 27 с. **10.** Манойло А. В. Государственная информационная политика в особых условиях : монография / А. В. Манойло. – М. : МИФИ, 2003. – 388 с.

Надійшла до редколегії 09.09.2010