

УДК 354.42

О.В. Левченко

Міністерство оборони України, Київ

## СИСТЕМА ЗАХОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ

На основі аналізу форм ведення інформаційної боротьби, запропоновано систему заходів протидії найбільш вагомій з них – інформаційні операції.

**Ключові слова:** інформаційні загрози, інформаційна кампанія, інформаційна операція, інформаційна акція, інформаційні заходи.

### Вступ

#### Постановка проблеми. Аналіз літератури.

На сьогодні формування світового геополітичного простору та зовнішньодержавних відносин відбувається в умовах жорсткого інформаційного протиборства.

Для України ця проблема особливо актуальна, зважаючи на відкрити інформаційну війну в ході російської агресії проти нашої держави. Крім цього, негативними чинниками для України є систематичний інформаційний тиск і з боку інших держав та їх союзів (коаліцій), а також до кінця невизначеність її геополітичного статусу, політична нестабільність, нестійкість вітчизняного інформаційного простору.

В цих умовах успішне ведення інформаційної боротьби залежить, серед іншого, від вчасного виявлення та попередження заходів деструктивного іноземного інформаційного впливу. Тому дослідження механізмів протидії негативному інформаційному впливу, що проявляється у різних формах ведення інформаційної боротьби, є **нагальною науковою проблемою**.

У наукових роботах багатьох дослідників [1 – 4] достатньо глибоко аналізуються механізми проведення інформаційних операцій. Однак аналізу проблем протидії таким операціям більшість робіт не містить, а ті, що є, переважно стосуються технічних питань.

Отже, **метою статті** є розроблення системи заходів протидії інформаційним операціям в ході інформаційної боротьби.

### Основний матеріал

Інформаційна боротьба (ІБ) має свої визначені форми реалізації [5]. Основними формами ведення інформаційної боротьби є такі:

- інформаційна кампанія,
- інформаційна операція,
- інформаційна акція,
- інформаційна атака.

Перелічені форми взаємопов'язані між собою і мають певну ієрархію.

Інформаційні атаки у більшості випадків мають технічний характер, проводяться за одним напрямом інформаційного впливу (ІВ) і тривають від декількох днів до тижня та спрямовуються на одиночний об'єкт (інформаційний ресурс, конкретні інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи). Інформаційні атаки психологічного характеру спрямовуються на конкретну посадову особу, що приймає важливі рішення в конкретній сфері життєдіяльності держави, або найважливіші органи, установи (організації).

Інформаційні акції за основними показниками схожі з інформаційними атаками (також проводяться за одним напрямом інформаційного впливу), але мають значно більший масштаб (спрямованість на груповий об'єкт ІВ) і тривалість (декілька тижнів – місяців).

Інформаційні операції проводяться за декількома напрямками ІВ в одній із сфер життєдіяльності держави. Їх об'єктами можуть бути населення протиборчої держави, певні соціальні групи, особи, що приймають державні рішення, керівництво і населення провідних країн світу та суміжних з Україною держав, а в ході воєнного конфлікту, крім того, особовий склад військ супротивника, населення країн-учасників воєнного конфлікту, системи державного і військового управління противника, елементи його інформаційної інфраструктури. Тривалість інформаційної операції може бути від одного до декількох місяців.

У мирний час метою інформаційних операцій може бути вплив на морально-психологічний стан вищого керівництва держави-супротивника і певних соціальних груп населення в інтересах схвалення їх до прийняття рішень та дій у потрібному для протиборчої держави напрямі.

У воєнний час цілі інформаційних операцій полягають у дезорганізації системи державного управління та систем управління військами і збро-

єю, знищенні інформаційної інфраструктури противника, завоюванні інформаційної переваги над ним та створенні сприятливих умов в інформаційному просторі для дій своїх військ, а також у забезпеченні захисту власної інформаційної інфраструктури та інших складових інформаційного простору від дій противника.

Інформаційна кампанія носить переважно довготерміновий перманентний характер. Вона проводиться, як правило, за декількома напрямками ІВ у декількох сферах життєдіяльності держави-супротивника (зовнішньополітична, внутрішньополітична, економічна, військово-технічна тощо) і може тривати роками, до досягнення своєї кінцевої мети, а також може посилюватися або затухати залежно від початку чи закінчення інформаційних операцій або окремих інформаційних акцій, які є її складовими.

У рамках однієї інформаційної кампанії можуть одночасно або послідовно проводитися декілька інформаційних операцій, кожна з яких має власну сферу спрямованості та мету, яка, разом з тим, є частковою метою всієї кампанії.

Основною системоутворюючою формою ІВ слід вважати інформаційну операцію. Вона, як правило, проводиться в декілька етапів [4].

Підготовчий етап. Сутність цього етапу полягає у плануванні операції, визначенні сил і засобів, що залучаються, та їх підготовці до проведення заходів інформаційного впливу.

Основними завданнями підготовчого етапу є:

- визначення мети операції;

- визначення "цільової аудиторії" впливу, а саме: об'єкта (об'єктів), на який спрямовуватиметься інформаційний вплив;

- визначення необхідних сил (відповідальних виконавців) і засобів (ресурсів) для проведення операції;

- визначення методів (способів) і прийомів проведення операції;

- розробка орієнтовного сценарію (плану) проведення операції, підготовка заяв, інформаційних повідомлень (в т. ч. чуток) та їх розподіл між виконавцями згідно зі сценарієм;

- підготовка залучених сил до проведення заходів інформаційного впливу та організація взаємодії між ними;

- визначення критеріїв оцінки успіху операції.

Підготовчий етап інформаційної операції не може бути виявлений шляхом аналізу публікацій засобів масової інформації (ЗМІ), оскільки жодним чином через них не проявляється.

Основною можливістю визначення підготовки протилежної держави до проведення такої операції є використання агентурних джерел розвідувальної інформації.

Початковий етап. На цьому етапі інформаційної операції обирається або штучно створюється так званий інформаційний привід подія, якою можна скористатися як приводом для розгортання скоординованих інформаційно-психологічних акцій. Як інформаційний привід може бути використана будь-яка подія, яка якимось чином співвідноситься з наявними проблемами, актуальними стереотипами і викликає живий інтерес у визначеній аудиторії (об'єкта впливу).

Найкращим варіантом вважається такий, коли інформаційний привід є важливою подією у житті країни в цілому або в житті певної соціальної групи. У переважній більшості випадків у якості інформаційного приводу використовуються негативні події, оскільки вони набагато чіткіше фіксуються у свідомості аудиторії та викликають у неї відповідну реакцію.

У ряді випадків інформаційним приводом слугує будь-яка подія, оскільки її наявність є лише формальним підґрунтям для початку вже спланованої інформаційної операції.

На цьому етапі спеціально підготовлені повідомлення носять, як правило, обмежений характер та майже не виходять за рамки самого інформаційного приводу. Між ними існують певні часові інтервали для вивчення результатів їх впливу, тобто для підтримання постійного зворотного зв'язку. При цьому беззаперечно дотримується основна умова маніпуляції свідомістю – початок інформаційної операції обов'язково повинен залишатися незрозумілим і прихованим (непомітним) для об'єкта впливу.

Основний етап. Це є найбільш складний і достатньо тривалий етап операції. Його сутність полягає у масованому і повному використанні залучених інформаційних ресурсів для формування або руйнування визначених психологічних стереотипів і установок у об'єктів, на які спрямовується вплив. Фактично цей етап є сукупністю інформаційних заходів, пропагандистських і психологічних акцій та інших дій, які проводяться за єдиним замислом для досягнення поставленої мети операції.

Саме на цьому етапі можна вже виявити ознаки ведення інформаційної операції, так як він характеризується найбільшою кількістю однотипних публікацій, повідомлень, заяв тощо.

Зокрема, характерними ознаками ведення інформаційної операції є:

- одночасне і масове оприлюднення подібних між собою публікацій у ЗМІ (в першу чергу, державних);

- чітка координованість як тематики інформаційних повідомлень, так і часу їх подання у ЗМІ на кожному наступному етапі (інформаційній акції, атаці) операції;

активне залучення до оприлюднення державної позиції з даного питання не тільки національних, а й іноземних засобів масової інформації. Перелічені вище ознаки можуть свідчити про високу ймовірність координації інформаційних заходів з одного керівного центру;

виступи із посланнями, заявами на пресконференціях і т. ін. вищих посадових осіб держави, в яких вони висловлюють претензії або звинувачення щодо проблемного, на їх погляд, питання. Опосередковано це може говорити про санкціонування проведення інформаційної операції на вищому державному рівні.

Якщо одночасні масові інформаційні заходи здійснюються хвилеподібно (при цьому проявляється зв'язок кожної наступної хвилі заходів з попередніми) та проводяться на одному з напрямів певної сфери національної безпеки (сфери життєдіяльності) держави, то можна говорити про наявність взаємопов'язаних за метою, завданнями і часом інформаційних акцій і атак та наявність, у підсумку, інформаційної операції, яка складається із зазначених акцій і атак.

Слід також наголосити, що інформаційні акції і атаки, взаємопов'язані в рамках однієї інформаційної операції, можуть проводитися як послідовно, так і одночасно для досягнення власних часткових цілей.

*Заключний етап.* Зміст цього етапу полягає у плавному завершенні інформаційної операції та закріпленні її результатів після досягнення поставлених цілей операції чи в результаті якихось форс-мажорних обставин. Головне завдання етапу – вийти з операції таким чином, щоб супротивник навіть не здогадався про її проведення, або хоча б не дати можливості йому зрозуміти мети проведеного на нього впливу. Інформаційна операція інформаційно-психологічної спрямованості має в своїй основі маніпулювання суспільною або індивідуальною свідомістю.

Тому викрита маніпуляція, за визначенням, є невдалою. Адже, якщо об'єкт впливу розуміє, що на нього здійснюється або здійснювався спеціально підготовлений інформаційний вплив, він завжди може знайти можливість йому протидіяти.

Наприклад, ігнорувати певні повідомлення та повернутися до попередніх позицій з посиленням впевненості у їх істинності.

Виходячи з цього, на заключному етапі інформаційної операції, як правило, оприлюднюються повідомлення про значні успіхи у вирішенні проблеми або виконанні актуального для суспільства завдання тощо.

Для виявлення на ранніх стадіях і протидії інформаційним операціям пропонується система заходів, яка складається з таких підсистем [6]:

1. Попередження умов проведення інформаційних операцій.
2. Виявлення інформаційних операцій.
3. Припинення інформаційних операцій.

**Підсистема попередження** умов проведення інформаційних операцій містить такі заходи:

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

безперервний пошук і усунення вразливостей у системі інформаційної безпеки нашої держави;

виявлення та ліквідацію умов, сприятливих для реалізації іноземними державами своїх агресивних намірів у формі розв'язання інформаційної кампанії, ведення інформаційних операцій, акцій і атак;

безперервний пошук нових джерел інформаційно-психологічної напруженості, відстеження переміщення й розростання (зменшення) уже виявлених зон інформаційно-психологічних конфліктів (моніторинг розподілу конфліктогенного потенціалу в інформаційній сфері), а також їхніх зон впливу й оцінку загроз безпеки держави, пов'язаних з можливим залученням до одного з таких конфліктів;

моніторинг просторового розподілу та зосередження зусиль сил і засобів потенційних супротивників із числа іноземних держав і інших суб'єктів геополітичної конкуренції навколо життєво важливих об'єктів інформаційної інфраструктури держави;

виявлення та припинення умов для виникнення усередині держави деструктивних суб'єктів геополітичної конкуренції, здатних самостійно виходити із власними антидержавними ініціативами на міжнародний рівень;

виявлення та блокування процесів ініціювання та підтримки ззовні проявів сепаратизму всередині української держави;

оцінка та аналіз рівня присутності і впливу (фінансового, технологічного, інформаційного, ідеологічного) іноземних структур над національними засобами масової інформації та прийняття заходів з метою недопущення встановлення зовнішнього контролю над національними інформаційними ресурсами і психологічною сферою суспільства;

пошук і припинення спроб створення негативного психологічного фону відносно діяльності (або окремих її напрямків) системи органів державної влади й місцевого самоврядування;

виявлення спроб встановлення інформаційної блокади України;

демонстрація (пропаганда) власної сили (могутності) держави в інформаційному просторі (у

вигляді, наприклад, оперативно-тактичних навчань сил інформаційно-психологічних операцій з використанням інформаційної зброї з метою стримування потенційних агресорів;

забезпечення національної інформаційної безпеки.

Заходи попередження умов проведення інформаційних операцій здійснюються на етапі підготовки такої операції і розпочинаються з моменту виявлення ознак проведення останньої.

**Підсистема виявлення** інформаційних операцій містить:

безперервний пошук (моніторинг) зовнішніх загроз інформаційній безпеці держави, можливих ознак, слідів і зовнішніх проявів здійснення антиукраїнських інформаційних заходів;

виявлення напрямків експансії іноземних держав в інформаційній (інформаційно-психологічній) сфері;

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

аналітична реконструкція.

Заходи з виявлення інформаційних операцій проводяться на початковому етапі проведення такої операції.

**Підсистема припинення** інформаційних операцій складається із заходів щодо:

знищення джерел ведення інформаційних операцій;

нейтралізації джерел ведення інформаційних операцій.

Заходи з припинення інформаційних операцій проводяться на основному етапі проведення такої операції.

Зазначені заходи мають переважно активний (силовий) характер.

## Висновки

Таким чином, сьогодні надзвичайно актуальним і важливим є пошук дієвих механізмів протидії

інформаційним впливам в умовах російської агресії проти України та ведення Росією потужних антиукраїнських інформаційних операцій.

**Подальші дослідження** можуть бути спрямовані на розвиток теорії протидії деструктивному іноземному інформаційному впливу та розроблення методик виявлення інформаційних операцій і проведення упереджувальних заходів з протидії їм.

## Список літератури

1. Ланде Д.В. Как организовать оборону: 12 шагов противодействия / Д.В. Ланде // Телеком – 2009. – № 6. – С. 46–51.

2. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій. Навч. посібник / В.М. Петрик, В.В. Остроухов та ін. – К.: Росава, 2006. – 208 с.

3. Горбулін В.П. Проблеми захисту інформаційного простору України: монографія / В.П. Горбулін, М.М. Биченок; ін-т пробл. нац. безпеки. – К.: Інтертехнологія, 2009. – 136 с.

4. Жук С.Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С.Я. Жук, В.О. Чмельов, Т.М. Дзюба // Наука і оборона. – 2006. – № 2. – С. 35–41.

5. Левченко О.В. Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату. / О.В. Левченко // Наука і оборона. – 2013. – № 3. – С. 36–40.

6. Левченко О.В. Попередження акцій інформаційного впливу на ранніх стадіях їх підготовки / О.В. Левченко, О.М. Косогов // Перспективи розвитку сучасної науки. Матеріали II Міжнародної конференції (м. Київ, 7 – 8 травня 2015 року). – У 2-х частинах. – Херсон : Видавничий дім «Гельветика», 2015. – Ч. II. – С. 64–66

Надійшла до редколегії 15.04.2016

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

## СИСТЕМА МЕР ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ ОПЕРАЦИЯМ

А.В. Левченко

*На основе анализа форм ведения информационной борьбы, предложена система мер противодействия наиболее весомой из них – информационные операции.*

**Ключевые слова:** информационные угрозы, информационная кампания, информационная операция, информационная акция, информационные меры.

## SYSTEM COUNTER MEASURES INFORMATION OPERATIONS

O.V. Levchenko

*Based on the analysis of forms of information warfare, proposed system countermeasures the most important of them is information operations.*

**Keywords:** information threat, information campaign, information operation, information action, information action.