

УДК 354.42.

А.О. Сірик<sup>1</sup>, С.В. Озеров<sup>2</sup>

<sup>1</sup>Військова частина А1906

<sup>2</sup>Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

## НАПРЯМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАХОДАМ ПІД ЧАС РОСІЙСЬКОЇ АГРЕСІЇ НА ТЕРИТОРІЇ УКРАЇНИ

*На основі аналізу інформаційних заходів, які проводяться Російською Федерацією відносно нашої держави розроблені пропозиції щодо напрямів інформаційної протидії на державному та відомчому рівнях.*

**Ключові слова:** інформаційні заходи, інформаційна операція, протидія, інформаційні загрози.

### Вступ

#### Постановка проблеми та аналіз літератури.

Хто володіє інформацією, той володіє світом – цим словам Натана Ротшильда більше двохсот років, однак сьогодні їх популярність виросла в рази. В епоху інформаційного суспільства історія розвитку будь-якої незалежної держави тісно переплетена з інформаційними заходами – маніпуляціями, інсинуаціями, дезінформаціями, обманами тощо. По суті, в сьогоденній боротьбі України за свою незалежність основний сегмент її займає інформаційна боротьба, проводиться в таких формах [1], як інформаційна кампанія, інформаційна операція, інформаційна акція, інформаційний удар та інформаційна атака.

Основним змістом зазначених форм є заходи, які в переважній більшості не застосовують летальну зброю але дають змогу добитися тих самих результатів, що й у випадку використання традиційної зброї, при цьому мінімізують втрати живої сили і руйнування інфраструктури противника.

Інформаційні заходи стали невід’ємною частиною політики всіх провідних країн світу. У цьому сенсі Росія не тільки випередила розвинені європейські країни, але й стала нарівні в питаннях інформаційного впливу зі США і Китаєм [2].

Сьогоднішні реалії в Україні – бойові дії на Донбасі, їх колосальна інформаційна і військова підтримка з боку Кремля наочно демонструють зацікавленість Москви в розпалюванні конфлікту. На передній план при цьому вийшли російські інформаційні кампанії, операції, акції, метою яких є руйнування України як незалежної держави, провокування внутрішньої нестабільності та конфліктів, завоювання інформаційної переваги.

У наукових працях багатьох дослідників [2, 3] переважно розкриваються теоретичні засади ведення інформаційних операцій. Однак практичні висновки з аналізу вітчизняного досвіду за результатами інформаційних заходів Росії під час анексії Криму та захоплення частини Луганської та Донецької областей України почали формуватися лише останнім часом.

**Метою статті** є аналіз основних особливостей інформаційних заходів під час застосування в збройному конфлікті на Донбасі сил інформаційних операцій Російської Федерації (РФ) та визначення напрямів протидії їхнім заходам з боку нашої держави.

## Основний матеріал

За результатами відкритих джерел до проведення інформаційних заходів на території Донецької та Луганської областей України російська сторона підійшла з дотриманням всіх канонів “пропагандистського букваря” доктора Геббельса. Для цього на “поле бою” залучаються спеціальні підрозділи (частини) збройних сил Росії та використовуються всі можливості її пропагандистської машини. До складу таких підрозділів, як правило, входять [4]:

*Групи спеціальних журналістів* (8-10 окремих груп) – працівники російських інформаційних каналів. Склад 3–4 особи – журналіст, оператор, водій, може бути охоронець. Основними завданнями такої групи є:

упереджене висвітлення подій на території України та безпосередньо в зоні проведення антитерористичної операції (АТО) з елементами повної брехні;

позиціонування ватажків незаконних збройних формувань непризнаних республік ДНР і ЛНР як борців із фашизмом та за незалежність Донбасу, а військовослужбовців Збройних Сил (ЗС) України як окупантів-загарбників.

*Оперативні групи психологічних операцій* (ПсО) (до 4 груп) – мобільні підрозділи від загону ПсО. До їхнього складу входять 2–4 особи.

На території окупованого Донбасу вони виконують завдання:

усна пропаганда, у тому числі і робота з місцевим населенням;

поширення пропагандистської літератури та іншої необхідної інформації;

створення пропагандистських груп у населених пунктах, що складаються з місцевих активістів, їх організація та координація дій;

сприяння роботі російських журналістів;

збір інформації і визначення найбільш гострих проблем у населення і використання їх надалі як інформаційного приводу;

моніторинг поточного морально-психологічного стану місцевого населення.

*Загін ПсО* – дислокується, як правило, на території РФ, недалеко від кордону з Україною. Він є основним органом управління при здійсненні інформаційно-психологічного впливу (ІПсВ) на цільову аудиторію (об’єкти інформаційних заходів). Його завданнями є:

управління підрозділами ПсО, які виконують спеціальні завдання щодо ІПсВ;

збір, обробка і аналіз інформації про поточний морально-психологічний стан населення України і підрозділів російсько-терористичних військ (зона

інтересів загону ПсО поширюється на всю територію України);

організація і проведення заходів інформаційних операцій (акцій, ударів, атак) на території України.

*Агенти диверсійно-психологічної роботи* (фахівці ГРУ ГШ або ФСБ РФ) – ведення диверсійно-психологічної роботи в інших областях України, основними їх завданнями є:

створення диверсійно-пропагандистських груп в інших областях України серед місцевого авторитетного населення; навчання місцевих груп проведенню підривних пропагандистських акцій;

забезпечення груп необхідним матеріально-технічним майном;

безпосереднє проведення мітингів, акцій протесту та поширення пропагандистських матеріалів.

Слід зазначити, що в 2014 році в російській армії були створені так звані кібер-війська, основним завданням яких є захист національних комп’ютерних мереж, що забезпечують оборонні потреби, а також проведення кібернетичних атак на об’єкти потенційного противника. Ця нова категорія оборонного відомства стосується інформаційних заходів технічного характеру в інтернет-просторі стратегічного рівня ЗС РФ. За наявною інформацією, військові кібер-фахівці залучаються до виконання завдань інформаційних операцій не тільки в окупованому Донбасі, але й на об’єктах всієї України.

Крім цього, фахівці інших загонів ПсО ЗС Росії, які перебувають за тисячі кілометрів від Донбасу, віддалено працюють у мережі Інтернет з контентного наповнення сайтів терористичних угруповань (“Новоросія”, “Сварог”, “Штаб російської армії” тощо), а також з тролінгу в соціальних мережах на форумах і блогах населення України та інших громадян, які висловлюють проукраїнську позицію.

Аналіз інформаційних заходів Росії під час воєнного конфлікту на Донбасі, у всіх формах їх прояву, дає змогу визначити основні їх особливості:

ефективне планування інформаційних заходів, високий ступінь їх координації та інтегрованості на найвищих щаблях влади, безпосередня узгодженість з політичними, дипломатичними та військовими заходами;

розвиток і посилення можливостей ЗС РФ щодо проведення інформаційних операцій, вдосконалення взаємодії військових із ЗМІ РФ в процесі інформаційного супроводження бойових дій;

широке використання заходів із дезінформації (незаконна присутність і участь у бойових діях російських військ в окупованому регіоні Донбасу маскується під навчання на території РФ, для цього застосовується демонстраційне переміщення техніки, перевдягання військовослужбовців ЗС Росії у форму незаконних-збройних формувань або використання позначень українських сил АТО на своїй техніці);

лобіювання російських інтересів у конфлікті на Донбасі в інформаційному просторі західних та інших країн світу шляхом підкупу власників і журналістів авторитетних ЗМІ, експертів, політиків, неурядових організацій, а також залучення неінформаційних інструментів (представництв та посольств Росії, різних державних та недержавних організацій);

постійне застосування чуток – від політичних застережень Жириновського, Захарченка, Плотницького, Стрелкова до розмов на зупинках жителів окупованих міст. Чутки – це джерело паніки, а якщо в умовах війни можна управляти панікою – то мета інформаційно-психологічного впливу досягнута;

потужний інформаційно-психологічний вплив на частину українського та російського населення за допомогою федеральних ЗМІ спрямований на спонукування і заохочення його до участі в бойових діях на боці сепаратистів під приводом боротьби з фашизмом та захистом “русского мира”;

чітке визначення об’єктів ІІСВ їх морально-психологічних особливостей, ціннісних орієнтирів, мотивації та ретельне планування і коригування інформаційних заходів, які максимально адаптовані до кожної із груп впливу.

У більшості випадків силами інформаційних операцій РФ вдається досягти успіху під час проведення заходів інформаційної боротьби проти України. Це демонструє неготовність відповідних державних структур адекватно реагувати на такі прояви [4]. Українська інформаційна політика працює в основному на локалізацію інформаційних загроз, а не на їхнє попередження. Причин цьому є багато, але головною з них є – фактична відсутність в державі національної системи забезпечення інформаційної безпеки, яка б гарантувала не тільки виявлення, аналіз та оцінювання інформаційних загроз, а й відповідну протидію таким загрозам. Таким чином, протидію інформаційним заходам в умовах інформаційної боротьби з РФ, на нашу думку, необхідно організовувати та здійснювати за наступними напрямками.

На державному рівні:

1. Розроблення нормативно-правової бази стосовно засад державної політики у сфері інформаційної боротьби та які б визначали взаємодію спеціалістів сил ІІСО ЗС України з місцевими органами самоврядування, державними (недержавними) установами, громадсько-політичними організаціями, правоохоронними органами, засобами масової інформації (ЗМІ) тощо.

2. Створення єдиного міжвідомчого органу, який здійснюватиме керівництво та координацію заходів інформаційної боротьби (наприклад, міжвідомча комісія при Раді національної безпеки і оборони України).

3. Закінчення формування національної системи забезпечення інформаційної безпеки та її складо-

вих в МО України, МВС України, СБУ та інших відомствах.

4. Визначення об’єктів критичної інформаційної інфраструктури держави, виведення з ладу, знищення яких призведе до вагомих наслідків та матеріальних втрат у будь-якій сфері національної безпеки України.

5. Використання за єдиним замислом патріотичного ресурсу (працівників недержавних установ, звичайних громадян України – хакерів-любителів) для виконання завдань протидії інформаційним заходам в інтернет-просторі з метою формування суспільної думки через соціальні мережі, форуми, блоги.

6. Об’єднання ЗМІ різних форм власності навколо національної ідеї з метою розвитку інформаційної політики держави. Вони повинні бути носієм ідеології, оскільки майже вся інформація про події в країні та за її межами поширюється через їхні комунікативні канали.

7. Створення повноцінного інформаційного потоку з метою формування у населення окупованих територій Донбасу позитивної суспільної думки, при цьому необхідно більше уваги звертати на морально-психологічну підтримку людей (люди зневірені діями як української влади, так і ватажків самопроголошених республік ДНР та ЛНР). З метою створення умов для адекватного сприйняття цільовою аудиторією подій на цих територіях та інших областях України необхідно відновити (створити) канали поточного інформування (телебачення і радіо), організувати наповнення відповідним контентом мережі Інтернет.

7. Нарощування суб’єктів, що генерують інформацію, а також присутність технічних можливостей для її поширення не тільки в інформаційному просторі України, а й за її межами. Закордонні споживачі інформації про події в Україні, як правило, довідуються із запізненням на декілька днів, а перекручені новини з Росії про Україну отримуються вчасно. А це вже є приводом, щоб сумніватися в правдоподібності українських джерел інформації. Тому питання із закордонним інформуванням в Україні необхідно вирішувати якомога скоріше.

На відомчому рівні:

1. Термінове розроблення регламентуючих документів у сфері ведення інформаційних операцій (керівництво, настанова, положення).

2. Підвищення ефективності роботи штабів стратегічного та оперативного рівнів Збройних Сил України щодо підготовки та проведення інформаційних операцій (акцій, ударів, атак).

3. Кадрове забезпечення та удосконалення (відновлення) належної підготовки зазначених фахівців інформаційно-психологічних операцій тактичної та оперативно-тактичної ланки Збройних Сил України.

4. Забезпечення відповідних військових частин (підрозділів) специфічними засобами, які б сприяли

на сучасному рівні розвитку інформаційних технологій, вирішенню таких завдань:

створення і тиражування друкованих матеріалів;

створення і транслявання теле- і радіопередач у визначених районах бойових дій;

передавання необхідних повідомлень за допомогою звукомовних засобів; використання всіх можливостей глобальної мережі Інтернет (соціальні мережі, чати, блоги).

5. Налаштування тісної взаємодії з проукраїнськими неурядовими організаціями за кордоном, загальнодержавними, регіональними ЗМІ, лояльними представниками інтернет-співтовариства з метою:

створення і трансляції рекламних роликів на телевізійних і радіоканалах в інтересах проведення інформаційних заходів;

залучення операторів мобільного зв'язку для забезпечення передачі текстових, фотографічних, звукових і аудіовізуальних повідомлень пропагандистського характеру за допомогою мобільних телефонів;

залучення інтернет-провайдерів для забезпечення надання послуги доступу до мережі Інтернет для роботи фахівців військових частин (підрозділів) ПСсО в мережі.

6. Впровадження нових методів і засобів інформаційної боротьби, що характеризуються безперервністю та цілеспрямованістю інформаційних заходів, які проводяться з метою недопущення утворення у цільовій аудиторії "інформаційного вакууму", який безперечно використовує противник.

7. Забезпечення перебування і неупередженого висвітлення подій в зоні АТО журналістами західних країн світу, які можуть перебувати під впливом російських пропагандистських ЗМІ ("RT", "Голос Росії" тощо).

8. Оперативне реагування на неправдиву, упереджену інформацію стосовно стану справ на лінії зіткнення з противником та в інших випадках компрометації діяльності МО України і ЗС України, вищого воєнно-політичного керівництва держави.

9. Чітке регламентування порядку використання військовослужбовцями особистих засобів мобільного зв'язку (телефонів, смартфонів) з метою

недопущення протидією стороною визначення їх місцеперебування, перехоплення переговорів (повідомлень) тощо.

10. Удосконалення наукових досліджень у сфері інформаційної боротьби.

## Висновки

1. Противник використовує широке коло комунікаційних та інформаційних методів, засобів і технологій, сповідуючи принцип "мета виправдовує засоби". Демократичні чи журналістські стандарти, об'єктивність, правові норми – це обмеження для слабких, а не для воїнів інформаційного фронту Росії.

2. Сьогоднішня дійсність України наочно підтвердила її готовність до активного протистояння РФ в інформаційному просторі шляхом скоординованого, тісного інформаційного супроводу всіх дипломатичних, політичних, економічних, військових, кроків для забезпечення її національної безпеки.

3. Для того, щоб ефективно протидіяти інформаційним кампаніям, операціям, акціям в умовах агресії РФ, заходи протидії необхідно організовувати та проводити комплексно, планово, за єдиним замислом та за напрямками, які окреслені в статті.

## Список літератури

1. Левченко О.В. *Форми ведення інформаційної боротьби: практичний підхід до понятійного апарату* / О.В. Левченко // *Наука і оборона*. – 2013. – № 3. – С. 21-26.
2. Почепцов Г.Г. *Информационные войны* / Г.Г. Почепцов. – М.: Релф-бук, 2011. – 576 с.
3. *Інформаційна безпека держави у контексті протидії інформаційним війнам: навч. посібник* / А.О. Рось та ін.; за ред. В.Б. Толубка. – К.: НАОУ, 2004. – 176 с.
4. Гусаров В. *Силы информационных операций России: каким должен быть ответ Украины?* [Електронний ресурс] / В. Гусаров. – Режим доступу до ресурсу: [www.sprotuv.info/ru/news/5931/...](http://www.sprotuv.info/ru/news/5931/...)
5. Левченко О.В. *Проблеми і шляхи формування системи інформаційної безпеки держави* / О.В. Левченко // *Збірник наукових праць Харківського університету Повітряних Сил*. – X.: ХУПС, 2014. – Вип. 2 (39). – С. 166-168.

Надійшла до редколегії 17.08.2015

Рецензент: д-р техн. наук, проф. К.С. Васюта, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

## НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННЫМ МЕРОПРИЯТИЯМ ВО ВРЕМЯ РОССИЙСКОЙ АГРЕССИИ НА ТЕРРИТОРИИ УКРАИНЫ

А.О. Сирьк, С.В. Озеров

*На основании анализа информационных мероприятий, проводимых Российской Федерацией относительно нашей страны разработаны предложения направлений информационного противодействия на государственном та ведомственном уровнях.*

**Ключевые слова:** *информационные мероприятия, информационная операция, противодействия, информационные угрозы.*

## AREAS OF ANTI INFORMATION ACTIVITIES DURING THE RUSSIAN AGGRESSION IN UKRAINE

A.O. Siryk, S.V. Ozerov

*On the basis of information events held by the Russian Federation regarding our country's proposals on countering trends of information at the national and departmental levels.*

**Keywords:** *information measures, information operations, countering, information threats.*