УДК 327.88(470+571):004.56(477)

Михаїл Дем'яненко,
канд. політ. наук, наук. співроб.,
Національна бібліотека України імені В. І. Вернадського,
Україна, Київ

ПРОТИДІЯ ІНФОРМАЦІЙНІЙ АГРЕСІЇ: СВІТОВИЙ ДОСВІД ТА ВІТЧИЗНЯНІ РЕАЛІЇ

У статті досліджено специфіку інформаційної політики Російської Федерації відносно України, інших держав та НАТО, виокремлено потенційні та реальні інформаційні загрози для вітчизняної інформаційної безпеки, проаналізовано стан інформаційної безпеки України та захисту національного інформаційного простору від негативних інформаційно-маніпулятивних впливів. Розглянуто зарубіжний досвід протистояння інформаційній агресії та доведено необхідність консолідації міжнародних зусиль, а також охарактеризовано практичні рекомендації щодо вдосконалення системи інформаційної безпеки України.

Ключові слова: інформаційна агресія, інформаційна безпека України, інформаційний простір, державна інформаційна політика, інформаційні загрози, пропаганда, інформаційні війни.

Сучасні політичні, військові, економічні та інформаційні протистояння залишаються невід'ємним атрибутом суспільних відносин, при цьому саме інформаційні конфлікти вийшли на якісно новий рівень розвитку, а останні події у світі та Україні лише підтверджують цей факт. Словосполучення інформаційна безпека, інформаційна війна, інформаційна зброя та інформаційна агресія набули широкого застосування як у вітчизняному, так і зарубіжному комунікаційному середовищі.

Ефективність інформаційної зброї в сучасних умовах зумовлена тим фактом, що вона має визначальний вплив на свідомість людини, в якій програмуються потрібні суб'єкту впливу параметри: тип свідомості, штучні потреби, форми самовизначення тощо. Задоволення цих вимог для об'єкта інформаційного впливу стають пріоритетними, а тому змушують індивіда діяти відповідно. Тому забезпечення інформаційної безпеки та вироблення ефективних механізмів протидії інформаційній агресії залишаються серед ключових пріоритетів здійснення інформаційної політики багатьох країн.

Загалом проблемі забезпечення інформаційної безпеки та протидії інформаційної агресії в різних її проявах присвятили свої дослідження

багато науковців. Серед вітчизняних дослідників цієї тематики можемо відзначити Г. Почепцова, зокрема його працю «Інформаційні війни» [1], окремим аспектам цієї проблеми присвятили свої праці Г. Пєвцов, М. Хилько, С. Гнатюк, Д. Дубов, Т. Савчук та інші науковці.

Незважаючи на вагомі теоретичні та практичні результати наукового пошуку зарубіжних і вітчизняних вчених, на нашу думку, детальнішого вивчення заслуговує дослідження досвіду різних країн світу в питанні вироблення ефективних засобів протидії інформаційній агресії в контексті зміцнення інформаційної безпеки, захисту національного інформаційного простору та можливості застосування сучасних методів інформаційного захисту в Україні.

Визначальний вплив інформаційної зброї спонукає окремі країни реалізовувати агресивну інформаційну політику щодо інших, які вимушені вести політику захисту від чужого інформаційного впливу, і за таких обставин спостерігається конфронтація держав, що так само породжує кризові явища в міжнародних відносинах.

Яскравим сучасним прикладом інформаційної агресії є та інформаційна політика, яку Росія останнім часом реалізує стосовно НАТО, країн Європи та України. У цьому контексті можемо стверджувати, що інформаційна війна є елементом гібридної війни, яку Росія розв'язала проти України. Анексія Криму, який Україна фактично почала втрачати з набуттям незалежності, а також подальші події на Донбасі стали наслідком проведення масової соціально-комунікаційної роботи, з елементами інформаційної агресії з боку РФ, спричинили необхідність адекватного реагування у сфері інформаційної безпеки. Тому протистояння інформаційній агресії знаходиться серед безпекових пріоритетів більшості країн світу, в тому числі й України.

У кожному окремому випадку інформаційна агресія здійснюється зі своїми особливостями, враховуючи конкретні обставини, починаючи від рівня розвитку та поширення сучасних інформаційних технологій і закінчуючи підходами, якими послуговуються сторони інформаційних протистоянь.

Як показує практика, подекуди такі підходи є досить «брудними» та не відповідають загальноприйнятим європейським принципам інформаційних відносин, доступу громадян до інформації, роботи ЗМІ тощо. Досить часто вони використовуються і проти нашої держави. Наприклад, в інформаційній агресії проти України російськими телеканалами були застосовані заборонені технології 25-го кадру для інформаційно-психологічного впливу на глядачів. Відповідні заяви зробили в СБУ та на підтвер-

дження продемонстрували відеофрагмент випуску новин на телеканалі «Росія-24», у якому протягом усього випуску про події в Одесі 2 травня 2014 р. у куті екрана з'являлися малопомітні написи: «підпал: «Правий сектор», «людей убивають бандерівці», «нацгвардія – вбивці». СБУ також вдалося встановити, що російські ЗМІ використовують інші методи впливу на глядачів: поширюють напівправду, показують деталізовані сцени вбивств, насильства й намагаються емоційно впливати на глядача [2].

В експертному середовищі протидія деструктивному впливу на національний інформаційний простір має різні підходи, які можуть навіть суперечити одне одному. Наприклад, підхід повного невтручання на рівні держави, нібито через безмежність й екстериторіальність інформаційного простору, є повною протилежністю тотальній цензурі та політиці загальних заборон. Компромісний варіант варто шукати посередині, одним з таких рішень може бути ведення поняття «спеціальний режим використання національного інформаційного простору в умовах загрози або настання серйозної кризової ситуації». Реалізація подібного режиму цілком виправдовує себе в умовах інформаційної агресії Росії проти України. До речі, таке формулювання є в тексті «Воєнної доктрини України». Це демонструє необхідність наявності законодавчо врегульованого і завчасно відпрацьованого механізму ефективного захисту свого інформаційного простору.

Подібну агресивну інформаційну політику Кремль реалізує не лише в Україні. На думку польського експерта, президента Інституту нових медіа Е. Містевича, росіяни користуються слабкістю демократичних механізмів та відкривають у Західній Європі впливові центри пропаганди, такі як телебачення RT (раніше Russia Today) або радіостанція Sputnik. «Триває війна розповідей, війна інтерпретацій, відбувається спроба переконати громадськість як у своїй країні, так і в решті країн, що саме наше бачення є правильним. Росія вже багато років дуже сильна у сфері інформаційного маркетингу. По відношенню до Західної Європи вона діє з більш продуманою стратегією, більшою увагою, ефективністю, ніж Західна Європа щодо Росії», – додає Е. Містевич [3].

Разом з цим в інформаційній політиці РФ простежується формування образу ворога – країн Заходу, особливо США, а також низки держав колишнього соцтабору: України, Грузії, Польщі, країн Балтії. Сучасне покоління російських журналістів, медійників і піарників, яке було виховане на таких підвалинах, використовують соціально-комунікаційні технології як зброю, часто не обтяжуючи себе моральними принципами щодо їх застосування та вважають нормальним маніпулювати свідо-

містю, вести інформаційні війни, перекручувати факти й навіть творити паралельну, вигадану інформаційну реальність [4].

Центр з досліджень безпеки при Федеральній вищій технічній школі Цюриха нещодавно опублікував нове дослідження «Кібернетична та інформаційна війна в українському конфлікті», у якому автори М. Безнер та П. Робін вивчають природу інформаційної війни, яку Росія веде проти України, та розмірковують над наслідками цієї війни для України [5].

Автори зазначають, що хоча й російська кібердіяльність стала широко помітною лише під час виборчої кампанії в США у 2016 р., насправді Росія постійно нарощувала та вдосконалювала свій потенціал у цій сфері протягом останніх 10 років. Після детального огляду основних методів та хронології розвитку російської кіберагресії в Україні дослідники звертають увагу, зокрема, на те, що внаслідок кібернетичної та інформаційної війни, яку веде Росія проти України, жителі окупованої частини Донбасу та анексованого Криму стали «повністю ізольованими від інформації, що надходить із зовнішнього світу», адже у них є доступ лише до російського радіо та телебачення. Також зазначається, що російська пропаганда є дуже ефективною та діє через багато різних каналів від традиційного телебачення до соціальних мереж та чатів. Це дає змогу донести пропаганду до більшої кількості людей, при цьому на відміну від ЗМІ в соціальних мережах не витрачається час на перевірку правдивості інформації. Для підвищення довіри до російської пропаганди для її поширення запрошують відомих людей.

Ефективність такої інформаційної політики Росії в Україні було досягнуто завдяки тому, що агресор вжив максимум заходів, щоб ізолювати Крим та частину Донбасу для недопущення альтернативних ЗМІ для отримання об'єктивної інформації про події в цих регіонах.

Тож дослідники зазначають, що необхідно зробити все можливе для більшої обізнаності населення України про те, чим є насправді інформаційна війна та як вона працює. У цьому контексті небезпека проявляється в тому, що українське населення ще донедавна використовувало електронну пошту російських провайдерів, послуговувалося російськими соціальними мережами або ж іншими її інтернет-ресурсами, що давало змогу російській стороні відстежувати інформацію, яка була розміщена на цих платформах.

В умовах «гібридної війни», однією зі складових якої є інформаційна агресія, яка проявляється в пропаганді, зростанні кількості інформаційних потоків та зокрема сфальшованих повідомлень тощо, постає

необхідність забезпечення громадян знаннями про технології інформаційного впливу, засоби його розпізнавання та нейтралізації, а також ефективного механізму протидії інформаційній агресії, особливо з урахуванням міжнародного досвіду.

Серед основних кроків щодо забезпечення інформаційної безпеки в Україні можна виокремити врегулювання доступу в наш національний інформаційний простір. Однак необхідно розуміти, що лише заборонно-обмежувальні заходи в сучасних умовах не можуть повністю розв'язати проблему інформаційного впливу.

У цьому аспекті можна виокремити низку досліджень та аналітичних матеріалів, які були проведені як державними, так і недержавними організаціями. Зокрема досить ґрунтовними є матеріали дослідження «Міжнародний досвід здійснення спеціальних режимів мовлення: висновки для України», яке було проведено у 2016 р. колективом Національного інституту стратегічних досліджень. У ньому проаналізовано відповідний досвід США під час подій в Іраку, починаючи з 2003 р., де інформаційна складова операції та її медіа-супровід мали велике значення. Передбачалося медіа-охоплення іракської (та частково близько-східної), американської, а також світової цільової аудиторії. У самому Іраку інформаційна кампанія повинна була проходити в кілька етапів – підготовчий, висвітлення самої військової операції та післявоєнний, – перебудова медіа-системи країни в інтересах США і держав коаліції. Важливим моментом є той факт, що стан тодішнього іракського медіа-простору в окремих моментах є дещо подібним, до того, що сьогодні існує на непідконтрольних територіях в Україні (переважну частину в структурі ЗМІ займають радіо та телебачення).

У дослідженні також розглянуто досвід Грузії в інформаційному протистоянні з Росією у 2008 р. та прибалтійських держав. Характерним є той факт, що коли США та Грузія вирішували ці питання в умовах кризової ситуації, то країни Балтії щодо Росії намагалися попередити можливі ризики. Як приклад, можна згадати завчасне рішення Литви з заборони окремих російських каналів, жорсткий контроль за національними ЗМІ проросійської орієнтації тощо. Подібної тактики в протистоянні російській інформаційній агресії дотримується і Латвія, яка врахувала досвід подій в Україні за період, починаючи з 2014 р. [6].

Якщо не брати до уваги можливі політичні утиски, то в контексті протидії російській інформаційній агресії з боку української влади можна згадати нещодавнє рішення вітчизняного парламенту, який закликав Раду національної безпеки та оборони України запровадити санкції

проти телеканалів NewsOne і «112 Україна». Заступник голови Комітету Верховної Ради з питань свободи слова та інформаційної політики, нардеп від «Народного фронту» С. Висоцький підкреслив під час обговорення, що Україна повинна «захистити від проросійської брехні та маніпуляцій свій суверенний інформаційний простір» [7].

Окремі аспекти ведення інформаційної війни та протидія інформаційній агресії стали предметом обговорення учасниками конференції «Інформаційна війна в інтернеті. Викриття і протидія прокремлівській дезінформації в країнах Центральної та Східної Європи», яка відбулася в Українському кризовому медіа-центрі наприкінці лютого 2017 р. у м. Київ. Доповідачі відзначали що в усіх країнах Східної Європи та в Україні російська пропаганда використовує практично однакові інструменти і меседжі. Змінюються лише деякі акценти, з огляду на специфіку ситуації у кожній конкретній країні. Такими виявилися результати досліджень фахівців з Польщі, Чехії, Словаччини, Угорщини, Молдови та України. Усі партнери-учасники проекту робили це у своїй країні, де проаналізували діяльність кількасот порталів і виявили кількасот прикладів фейкової або зманіпульованої інформації, лише за липень – жовтень 2016 р. У таких матеріалах широко використовується маніпуляція фактами і емоціями, гра на страхах і болючих темах, роздування проблем.

При цьому поширенню дезінформації сприяють умови сучасного інформаційного середовища – доступний Інтернет і соцмережі, високий рівень анонімності, особливо за умов недостатньої медіа-грамотності частини населення та не завжди професійної роботи журналістів.

Мережа пропагандистських ЗМІ містить різні інформаційні сайти та соцмережі. Дуже активні «тролі», особливо в коментарях до новин, які стосуються НАТО, України, відносин між США, Росією та ЄС. Для маніпулятивних матеріалів характерне змішування реальних фактів і особистої точки зору автора. Такі пропагандистські та маніпулятивні матеріали зазвичай написані анонімними авторами, що не дає змоги публічно викрити цих «журналістів». Тому, для ефективнішої протидії кремлівській пропаганді дуже важливо розповідати широкому загалові про таких авторів дезінформації.

Серед основних джерел поширення дезінформації автори дослідження виділили дві основні групи – «сайти про теорії змов» та «альтернативні медіа». Перші – надзвичайно непрофесійні та маніпулятивні, їхня читацька аудиторія невелика. Другі працюють професійніше і позиціонують себе як альтернативу «упередженим мейнстрімним ЗМІ». Там читацька аудиторія значно більша.

Спільні риси для обох груп – фокус на подіях за кордоном і зациклене повторення новин тієї самої тематики (міграційна криза, тероризм тощо). У матеріалах широко вдаються до викривленої інтерпретації фактів, маніпулятивних використань фото, посилання на «внутрішні джерела», гри на емоціях. Меседжі також типові – позиціонування В. Путіна як сильного лідера, засудження НАТО як агресора, тези на підтримку російського втручання в Україні і Сирії, «загниваючий захід», розпад ЄС, «хунта в Україні», «американський імперіалізм» тощо [8].

Загалом експерти відзначають, що здатність суспільства не піддаватися впливу пропаганди потребує, насамперед, усвідомлення того, що ця проблема існує. Разом з тим вони пропонують підвищувати рівень освіти, запроваджувати наприклад, курс медіа-грамотності вже зі шкільних років, а фахівцям інших країн, рекомендують об'єднувати зусилля і виносити цю тему на публічне обговорення. З точки зору оцінки потенційних ризиків та розробки засобів захисту від них для інших країн вбачається доцільною міжнародна діяльність, спрямована на дослідження агресивної інформаційної політики Росії в Україні.

Інформаційний аспект світової безпеки в контексті російсько-української «гібридної війни» став також предметом обговорення на 9-му Київському безпековому форумі «Відкрий Україну», який проходив у квітні 2016 р. На форумі понад 400 міжнародних і українських лідерів, представників політичних, ділових та громадських кіл з понад 20 країн світу обговорили глобальні безпекові тенденції та виклики в сучасних міжнародних відносинах [9].

Основна тема форуму присвячена останнім подіям в Україні та біля її кордонів, їх передумовам і можливим наслідкам для держави, регіону, Європи і навіть для світу в цілому. Переважна більшість присутніх висловили думку про те, що Росія є загрозою для безпеки і не лише в регіоні. Зокрема, президент Центру вивчення та дослідження політичних рішень Н. Тензер (Франція) зауважив, що демократичний світ повинен формувати власний порядок денний інформаційних війн. «Путінська Росія просто бреше, презентуючи деякі факти, які не мають нічого спільного з дійсністю. А нам потім треба відбивати всю цю брехливу інформацію. Одним з таких прикладів є повідомлення про те, що Росія воювала проти ІДІЛ. Але Росія насправді не воювала проти ІДІЛ, а підтримувала режим Асада. І нам треба спростовувати, пояснювати це… Дуже важливо не дозволити Росії встановлювати інформаційний порядок денний. Тому, що фактично ми намагаємося відповідати Росії, часто не пропонуючи наше власне бачення світу чи реальності».

Якщо аналізувати глобальний масштаб інформаційних протистоянь, то тут простежується досить чітка опозиція Росії та НАТО. На думку доктора військових наук та директора Центру досліджень над тероризмом Collegium Civitas К. Ліделя, успіх російської сторони – очевидний, тоді як НАТО, хоча і має значний потенціал, у питаннях інформаційної війни тільки відповідає, а росіяни диктують умови. «Вони перші б'ють, перші діють, перші готуються. Маю враження, що НАТО занедбало цю роботу. Росія як рупор пропаганди від самого початку створювалася та фінансувалася спецслужбами, а такий механізм у більшості країн Західної Європи не можливий. Вже на старті Захід займає дещо програшну позицію. НАТО та Захід повинні розробити інформаційну стратегію – конкретну державну політику, політику мас-медіа, суспільну політику», – переконаний експерт. Зокрема, він звертає увагу на те, що росіяни займаються у себе в країні пропагандою, що скерована на потреби внутрішньої політики і свого суспільства, наголошуючи при цьому на агресивності НАТО.

Звернув увагу К. Ліделль і на окремий аспект російсько-українського інформаційного протистояння. «Нещодавно я мав нагоду відвідати спеціально створене Міністерство інформації в Україні, яке займається цими питаннями. Там я ознайомився із аналізами підручників для початкових, середніх шкіл в Україні, видані кілька або кільканадцять років тому, де видно елементи інформаційної війни, ніби росіяни готувалися до того, що сталося в Україні, впродовж кільканадцяти років», – зазначив він [10].

Така, дещо пасивна позиція Альянсу сприяла тому, що, крім структур НАТО, більшість провідних країн світу самостійно формує координуючі органи з контролю за створенням і застосуванням інформаційної зброї, об'єднання зусиль у наукових дослідженнях проблем інформаційної боротьби, забезпечення інформаційної безпеки тощо.

У Великобританії проблемами інформаційної боротьби займається департамент урядових комунікацій (The Government Communications Head-quarters). Питаннями проведення інформаційних операцій у військовому відомстві займається група координації військових інформаційних операцій, яка підпорядкована міністру оборони.

У Німеччині створений та активно функціонує центр безпеки інформаційної техніки. Передбачається ведення наступальних і оборонних операцій інформаційної війни для досягнення національних цілей. При визначенні загроз і можливих наслідків країни та недержавні об'єднання розглядаються окремо, кримінальні угруповання виділено в окрему

категорію. Німецькі аналітики розглядають керування засобами масової інформації як дієвий елемент інформаційної війни.

Французькі експерти дотримуються концепції інформаційної війни, що складається з двох головних компонентів – військового та економічного (цивільного). Військова складова передбачає обмежену роль інформаційних операцій, оскільки інформаційна війна розглядається, головним чином, у контексті конфліктів малої інтенсивності або у миротворчих операціях. Економічна (цивільна) концепція передбачає ширший діапазон застосування інформаційних операцій.

Останнім часом у збройних силах НАТО, особливо США, значна увага приділяється ролі і технологіям, інформаційної зброї та психо-пропагандистським операціям у війнах XXI ст., які суттєво змінюють характер застосування різного роду військ у військових операціях, а також геополітичного та цивілізаційного протистояння ключових гравців. Інформаційно-психологічні технології – це широкомасштабне застосування способів і засобів інформаційної дії на психіку особового складу військ і населення протилежної сторони для досягнення політичних, дипломатичних, воєнних, економічних та інших цілей. Застосування цих технологій призводить до порушення систем державного та військового управління противника, інформаційного впливу на його державне та військове керівництво, особовий склад військ, формування сприятливої громадської думки у власній державі та інших країнах світу щодо подій, які відбуваються в зоні воєнного конфлікту, і сприяють досягненню воєнно-політичних і воєнно-стратегічних цілей у війні [11].

У цьому контексті хотілося б зауважити, що досвід проведення спочатку антитерористичної операції (АТО), а нині вже Операції об'єднаних сил, в Україні свідчить про необхідність розробки сучасної нормативно-правової бази та дієвої структури органів для ведення інформаційної боротьби Україною, у тому числі її Збройними силами. Хоча окремі позитивні моменти спостерігаються. Це, наприклад, поява влітку 2014 р. у ЗС України нового виду фахівців із цивільно-військового співробітництва, які здійснюють координацію та співробітництво з місцевим населенням, владою, міжнародними, урядовими та неурядовими організаціями. Свій досвід вони отримували при здійсненні миротворчих операцій, зокрема в Іраку.

Разом з тим окремі кроки української влади в питанні протидії інформаційній агресії все ж мають позитивні наслідки. Один з наочних прикладів – державне міжнародне телебачення UA|TV, яке за задумом повинно розповісти всьому світові про реальний стан справ в Україні.

Проте, зауважимо, що кількість передплатників каналу UA|TV у мережі Youtube станом на жовтень 2018 р. близько 38 тис., тоді як російський конкурент RT має понад 3 млн передплатників.

Поліпшити ситуацію з протидією російському впливу покликана підписана Президентом України Доктрина інформаційної безпеки. У ній, зокрема, визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [12].

У Доктрині також прописано сфери відповідальності більшості українських державних органів, цивільних і військових. Однак головна проблема інформаційного протиборства – це дотримання балансу між свободою слова та цензурою і чисельними заборонами, оскільки, недостатньо просто зробити обмеження російським інформаційним продуктам (ЗМІ, кінофільмам чи пісням). Такі заходи повинні поєднуватися створенням якісної української альтернативи, щоб користувач міг самостійно, без примусу, обрати для себе національний продукт. А отже, і змінити свій світогляд на український.

Ухвалене РНБО рішення «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 р. також викликане необхідністю вдосконалення нормативно-правового забезпечення та запобігання й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері. Рішенням було передбачено: розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема забороною ретрансляції телевізійних каналів; посилити контроль за додержанням законодавства з питань інформаційно-психологічної та кібернетичної безпеки; ужити заходів щодо забезпечення поширення у світі об'єктивних відомостей про суспільно-політичну ситуацію в Україні, зокрема, через створення відповідного медіа-холдингу для підготовки якісного конкурентоспроможного інформаційного продукту; розробити порядок аналізу інформа-

ційних матеріалів іноземних ЗМІ, що мають представництва в Україні, з метою впровадження дієвого механізму акредитації журналістів; ужити заходів до активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності [13].

Серед останніх кроків з боку української влади в питанні протидії інформаційній агресії можемо відзначити рішення Ради національної безпеки і оборони України від 26 січня 2018 р. «Про додаткові заходи з протидії інформаційній агресії Російської Федерації». Рішення РНБО, введене в дію цим указом, не публічне та призначене для службового користування.

У цілому низку позитивних кроків у питанні протидії інформаційній агресії можемо виокремити: створення Міністерства інформаційної політики; прийняття Доктрини інформаційної безпеки України; рішення про заборону окремих інформаційних ресурсів країни-агресора та інше, що дало змогу певною мірою відреагувати на інформаційні загрози. Хоча це не знімає з порядку денного питання інформаційної безпеки. При цьому, реалізуючи політику інформаційної безпеки, влада намагається не порушувати право громадян на інформацію. Головною метою такої інформаційної політики на непідконтрольних та звільнених територіях є не маніпулятивні та деструктивні інформаційно-психологічні впливи на мешканців регіону, а повноцінна соціально-психологічна реабілітація та реінтеграція громадян, а також поступове включення в усі сфери й процеси загальноукраїнського життя.

Агресивна інформаційна політика Росії, зокрема в Україні, все ж не залишилася поза увагою провідних зарубіжних країн, які зробили певні висновки та почали протидіяти їй на міжнародному рівні. Канадський уряд на початку вересня 2014 р. виділив цільову фінансову допомогу на користь трьох європейських центрів НАТО – кібербезпеки, енергетичної безпеки та стратегічних комунікацій – «з метою допомоги у стримані російських операцій у Східній Європі». 13 березня 2015 р. тодішній прем'єр-міністр Великобританії Д. Кемерон і Генеральний секретар НАТО Й. Столтенберг під час зустрічі обговорили необхідність боротьби з тактикою «гібридної війни», яку застосовує Росія в Україні, Молдові і Грузії, особливо щодо поширюваної неправдивої інформації та відповідних інформаційних кампаній, і дійшли висновку, що «ефективні стратегічні комунікації відіграють головну роль у протидії російській пропаганді».

Реакція Росії на ці процеси відобразилася у прийнятті в грудні 2014 р. нової Воєнної доктрини Російської Федерації. Доктрина, зокрема, перед-

бачає, що інформаційна війна є однією з домінуючих складових сучасного військового протистояння. Тобто Росія фактично визнала, що інформація – це зброя, якою можливо досягти перемоги, а інформаційна зброя разом із традиційними методами ведення збройної боротьби отримала визнання в російського військово-політичного керівництва. При цьому Російська Федерація включила інформаційну складову в перелік основних загроз національній безпеці, як у внутрішній, так і в зовнішній політиці.

Так, у лютому 2017 р. міністр оборони РФ С. Шойгу заявив про створення в країні військ інформаційних операцій. Нібито для ведення контрпропаганди й захисту національних інтересів національної оборони та протиборства в інформаційній сфері, хоча ймовірніше, з метою консолідації існуючих підрозділів та централізації керування інформаційними військами.

Висновок. Можна констатувати, що в сучасному світі інформаційна війна стала одним з найпоширеніших конфліктів, а її значення у військових протистояннях XXI ст. буде лише зростати. Відтак, залишається важливим завданням для державних, громадських, експертних інституцій розробити ефективні заходи (правові, організаційні, технічні), спрямовані на використання потенціалу держструктур з врегулювання доступу до інформаційного простору, механізмів швидкого його обмеження у разі виявлення фактів антиукраїнської діяльності; створення ефективної інформаційної інфраструктури держави, удосконалення нормативно-правової бази щодо виявлення та запобігання загрозам інформаційної та кібербезпеки, які постійно розвиваються й удосконалюються; модернізації всієї системи інформаційної безпеки держави, у тому числі, з урахуванням міжнародного досвіду. А консолідація міжнародних зусиль у сфері протидії цим викликам повинна стати тим фактором, який якщо не нівелює, то хоча б мінімізує негативний вплив російської інформаційної кампанії не лише в регіоні, а й у всьому світі. Водночас перспективними напрямами для подальших наукових досліджень залишаються: аналіз зарубіжного досвіду протидії негативним пропагандистсько-маніпулятивним інформаційним впливам, а також глибше дослідження технологій здійснення інформаційних операцій та війн.

Список використаних джерел

1. *Почепцов Г. Г.* Информационные войны / Г. Г. Почепцов. – Київ : Ваклер. – 2000. – 576 с.

2. Заборонені технології психологічного впливу виявили у новинах

щодо подій в Україні [Електронний ресурс]. – Режим доступу: https://tsn.ua/politika/u-sbu-zayavili-scho-rosiyski-kanali-zastosovuyut-proti-teleglyadachiv-25-y-kadr-350517.html https://tsn.ua/politika/u-sbu-zayavili-scho-rosiyski-kanali-zastosovuyut-proti-teleglyadachiv-25-y-kadr-35051-7.html. – Назва з екрана.

3. В інформаційній війні НАТО має не лише захищатися, але і наступати [Електронний ресурс]. – Режим доступу: http://www.polradio.pl/5/39/Artykul/261875. – Назва з екрана.

4. *Хилько М.* Масово- та соціально-комунікаційні технології в реалізації цілей зовнішньої політики Російської Федерації у XXI ст. [Електронний ресурс] / М. Хилько // Наук. пр. Нац. б-ки України ім. В. І. Вернадського. – 2014. – Вип. 39. – С. 84–93. – Режим доступу: http://nbuv.gov.ua/UJRN/npnbuimviv_2014_39_9. – Назва з екрана.

5. *Савчук Т.* Інформаційна війна Росії в Україні та кібербезпека (огляд дослідження) [Електронний ресурс] / Т. Савчук. – Режим доступу: https://www.radiosvoboda.org/a/28580039.html. – Назва з екрана.

6. *Гнатюк С.* Міжнародний досвід здійснення спеціальних режимів мовлення: висновки для України [Електронний ресурс] / С. Гнатюк. – Режим доступу: http://www.niss.gov.ua/content/articles/files/specrezim-1161 e.pdf. – Назва з екрана.

7. Рада предложила СНБО ввести санкции против каналов «112 Украина» и NewsOne [Электронный ресурс]. – Режим доступа: https://gordonua.com/news/politics/rada-predlozhila-snbo-vvesti-sankcii-protiv-kanalov-112-ukraina-i-newsone-399608.html. – Загл. с экрана.

8. Інструменти російської пропаганди у країнах Східної Європи – однакові – дослідження [Електронний ресурс]. – Режим доступу: http://uacrisis.org/ua/53099-information-warfare. – Назва з екрана.

9. Інформаційна війна, плани Варшавського саміту НАТО та масштабні військові навчання «Анаконда» – важливі тези 9-го Київського Безпекового Форуму [Електронний ресурс]. – Режим доступу: https://informnapalm.org/ua/ksf2016-forum/. – Назва з екрана.

10. В інформаційній війні НАТО має не лише захищатися, але і наступати [Електронний ресурс]. – Режим доступу: http://www.polradio.pl/5/39/Artykul/261875. – Назва з екрана.

11. Досвід і концепції ведення інформаційної боротьби у провідних країнах світу / Г. В. Пєвцов, А. М. Гордієнко, С. В. Залкін [та ін.] // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 1. – С. 12–16.

12. Доктрина інформаційної безпеки України [Електронний ресурс]. –

Режим доступу: http://www.zakon3.rada.gov.ua/laws/show/514/2009.– Назва з екрана.

13. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/n0004525–14. – Назва з екрана.

References

1. Pochepcov, G. G. (2000). Informacionnye vojny [Infowars]. Kyiv: Vakler [in Russian].

2. Zaboroneni tekhnolohii psykholohichnoho vplyvu vyiavyly u novynakh shchodo podii v Ukraini [The forbidden technologies of psychological influence educed in news in relation to events in Ukraine]. Retrieved from https://tsn.ua/politika/u-sbu-zayavili-scho-rosiyski-kanali-zastosovuyut-proti-teleglyadachiv-25-y-kadr-350517.html https://tsn.ua/politika/u-sbu-zayavili-scho-rosiyski-kanali-zastosovuyut-proti-teleglyadachiv-25-y-kadr-350517.html [in Ukrainian].

3. V informatsiinii viini NATO maie ne lyshe zakhyshchatysia, ale i nastupaty [In an infowar NATO must not only be on the defensive but also come]. Retrieved from http://www.polradio.pl/5/39/Artykul/261875 [in Ukrainian].

4. Khylko, M. (2014). Masovo- ta sotsialno-komunikatsiini tekhnolohii v realizatsii tsilei zovnishnoi polityky Rosiiskoi Federatsii u dvadtsiat pershomu st. [Mass- and of socialcommunication technologies in realization of aims of foreign policy of Russian Federation in XXI of century]. *Naukovi pratsi Natsionalnoi biblioteky Ukrainy imeni V. I. Vernadskoho – Transactions of V. I. Vernadsky Nation*al Library of Ukraine, issue 39, pp. 84–93. Retrieved from http://nbuv.gov.ua/UJRN/npnbuimviv_2014_39_9 [in Ukrainian].

5. Savchuk, T. Informatsiina viina Rosii v Ukraini ta kiberbezpeka (ohliad doslidzhennia) [Infowar of Russia in Ukraine and кібербезпека (research review)]. Retrieved from https://www.radiosvoboda.org/a/28580039.html [in Ukrainian].

6. Hnatiuk, S. Mizhnarodnyi dosvid zdiisnennia spetsialnykh rezhymiv movlennia: vysnovky dlia Ukrainy [International experience of realization of the dedicaded modes of broadcasting: conclusions for Ukraine]. Retrieved from http://www.niss.gov.ua/content/articles/files/specrezim-1161 e.pdf [in Ukrainian].

7. Rada predlozhila SNBO vvesti sankcii protiv kanalov «112 Ukraina» i NewsOne [Rada offered to СНБО to enter approvals against channels «112 Ukraine» and NewsOne]. Retrieved from https://gordonua.com/news/politics/rada-predlozhila-snbo-vvesti-sankcii-protiv-kanalov-112-ukraina-i-newsone-399608.html [in Russian].

8. Instrumenty rosiiskoi propahandy u krainakh Skhidnoi Yevropy – odnakovi – doslidzhennia [Instruments of Russian propaganda in the countries of East Europe – identical is research] Retrieved from http://uacrisis.org/ua/53099-information-warfare [in Ukrainian].

9. Informatsiina viina, plany Varshavskoho samitu NATO ta masshtabni viiskovi navchannia «Anakonda» – vazhlyvi tezy 9-ho Kyivskoho Bezpekovoho Forumu [Infowar, plans of the Warsaw summit of NATO and scale soldiery manoeuvres «Anaconda» is important theses of 9 th Kyiv Safety Forum]. Retrieved from https://informnapalm.org/ua/ksf2016-forum [in Ukrainian].

10. V informatsiinii viini NATO maie ne lyshe zakhyshchatysia, ale i nastupaty [In an infowar NATO must not only be on the defensive but also come]. Retrieved from http://www.polradio.pl/5/39/Artykul/261875 [in Ukrainian].

11. Pievtsov, H. V., Hordiienko, A. M., Zalkin, S. V., Sidchenko, S. O., Khudarkovskyi, K. I. (2015). Dosvid i kontseptsii vedennia informatsiinoi borotby u providnykh krainakh svitu [Experience and conceptions of conduct of informative fight are in the leading countries of the world]. *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy*. – *Science and Technology of the Air Force of Ukraine*, no 1. – pp. 12–16 [in Ukrainian].

12. Doktryna informatsiinoi bezpeky Ukrainy [Doctrine of informative safety of Ukraine]. Retrieved from http://www.zakon3.rada.gov.ua/laws/show/514/2009 [in Ukrainian].

13. «Pro zakhody shchodo vdoskonalennia formuvannia ta realizatsii derzhavnoi polityky u sferi informatsiinoi bezpeky Ukrainy» Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2014 r. [«About events in relation to perfection of forming and realization of public policy in the field of informative safety of Ukraine». Decision of national security and defensive of Ukraine Council from April, 28 in 2014]. Retrieved from http://zakon.rada.gov.ua/laws/show/n0004525–14 [in Ukrainian].

Стаття надійшла до редакції 28.11.2018.

Mykhail Demianenko,
Cand. Sci. (Political), Research Associate,
V. I. Vernadsky National Library of Ukraine,
Ukraine, Kyiv

Countering Information Aggression: World Experience and Domestic Realities

The article examines the specifics of the current foreign information policy of the Russian Federation, namely the information aggression which it has recently implemented against NATO, European countries and Ukraine. In this regard, the current state of Ukraine's information security is analyzed, as well as potential and real information threats are identified. At the same time, the retrospective and modern state of foreign experience of confronting information aggression is considered. The necessity to use means of effective protection the national information space from negative informational and manipulative influences is proved. In particular, such a means are: individual steps to regulate access to the domestic information space; mechanisms of implementation rapid restrictions in case of revealing facts of anti-Ukrainian activities; creation of an effective information state infrastructure, which envisages improving the regulatory framework for the detection and prevention of threats to information and cyber security, which are constantly evolving and perfected; creation of necessary structures in the system of law enforcement bodies and defense departments; modernization of the whole system of information security of the state, which meets the modern requirements, including, taking into account international experience. The practical recommendations for improving the information security system of Ukraine are highlighted and the need for consolidation of international efforts is proved.

Keywords: information aggression, information security of Ukraine, information space, state information policy, information threats, propaganda, information wars.