

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

**ГІБРИДНА ВІЙНА:
СУТНІСТЬ, ВИКЛИКИ ТА ЗАГРОЗИ**

Збірник матеріалів круглого столу

(Київ, 8 липня 2021 року)

Електронне видання

**Київ
2021**

Організаційний комітет:

Черняк А. М. – ректор Національної академії Служби безпеки України, доктор юридичних наук, доцент; **Чорний Р. Л.** – директор науково-організаційного центру Національної академії Служби безпеки України, доктор юридичних наук, старший науковий співробітник; **Гребенюк В. М.** – заступник директора науково-організаційного центру Національної академії Служби безпеки України, доктор юридичних наук, старший дослідник; **Давидова Т. О.** – начальник організаційно-наукового відділу науково-організаційного центру Національної академії Служби безпеки України, кандидат юридичних наук; **Зубенко В. С.** – старший науковий консультант організаційно-наукового відділу науково-організаційного центру Національної академії Служби безпеки України

*Рекомендовано до друку науково-організаційним центром
Національної академії Служби безпеки України
(протокол № 26 від 4 липня 2021 року)*

Гібридна війна: сутність, виклики та загрози: зб. матер. круглого столу (Київ, 8 липня 2021 р.). [Електронне видання]. – Київ : НА СБУ, 2021. – 189 с.

У збірнику тез наукових доповідей висвітлюються питання сутності та змісту гібридної війни як елемента цивілізаційного протистояння Російської Федерації з демократичними суспільствами за напрямками: політико-ідеологічне підґрунтя гібридної війни Російської Федерації проти міжнародного правопорядку; інформаційна складова гібридної війни Російської Федерації: викривлення реальності та деструктивна пропаганда в арсеналі політики Москви; економічна компонента гібридної війни й експансійні механізми у досягненні військово-політичних цілей РФ; силовий розвиток гібридної війни Російської Федерації – «гаряча» фаза сценаріїв «керованого хаосу».

УДК 355.488

ВСТУПНЕ СЛОВО

Доброго дня, шановні учасники!

Щиро вітаю вас з початком роботи круглого столу *«Гібридна війна: сутність, виклики та загрози»*. Висловлюю подяку за те, що знайшли час та можливість бути присутніми в Національній академії СБ України.

Сьогоднішній захід є логічним продовженням фахових дискусій щодо новітніх трендів визначення сутності поняття «гібридна війна», її нових форм та викликів, що постають перед державою, суспільством, і зрештою – кожним із нас. Це не перший форум, присвячений питанням гібридної війни, що проходить в стінах Національної академії.

На базі Національної академії СБ України було створено комунікаційний майданчик та проведено круглий стіл на тему «Удосконалення законодавства України з протидії гібридній агресії РФ в інформаційній сфері як умова забезпечення національної безпеки України». Проблематика протидії гібридним війнам регулярно підіймається під час щорічних наукових форумів, що проводить Академія – «Актуальні проблеми контррозвідувальної діяльності Служби безпеки України в сучасних умовах», «Актуальні проблеми оперативно-службової діяльності СБ України», «Актуальні проблеми управління інформаційною безпекою держави».

У Національній академії виконується науково-дослідна робота «Гібридна війна Російської Федерації проти міжнародного правопорядку». Під час її проведення науковці нашого навчального закладу накопичили фактаж, що засвідчив концентрацію зусиль Російської Федерації не лише за інформаційною операційною лінією, але й за іншими – воєнною, економічною, політичною, в межах яких російський політикум активно формує комплекс гібридних загроз Україні, країнам ЄС та НАТО.

Зауважимо, що Кремль постійно удосконалює тактику і стратегію сценаріїв керованого хаосу. Зважаючи на це, порядок денний, що стосується обговорення проблематики гібридної війни, не вичерпується. На прикладі військових доктрин РФ відбувається поєднання зазначених операційних ліній. Відповідно до Стратегії національної безпеки від 02.07.2021 року Москвою взято курс на «збереження загальноросійської культурної ідентичності» російського, українського та біло-

руського народів, зміцнення російської мови як «мови міжнародного спілкування».

З огляду на викладене, роботу круглого столу заплановано в межах таких напрямів:

- *політико-ідеологічне* підґрунтя гібридної війни Російської Федерації проти міжнародного правопорядку,
- *інформаційна* складова гібридної війни Російської Федерації: викривлення реальності та деструктивна пропаганда в арсеналі політики Москви,
- *економічна* компонента гібридної війни й експансійні механізми у досягненні військово-політичних цілей РФ,
- *силовий розвиток* гібридної війни Російської Федерації – «гаряча» фаза сценаріїв «керованого хаосу».

З метою вироблення узгодженої позиції щодо сутності та змісту гібридної війни як елемента цивілізаційного протистояння Російської Федерації з демократичними суспільствами, і проводиться сьогоднішній захід.

Переконаний, круглий стіл «Гібридна війна: сутність, виклики та загрози» стане гарною нагодою осмислити і проаналізувати операційні лінії гібридної війни РФ проти міжнародного правопорядку, і сприятиме формуванню єдності розуміння масштабів загроз, спричинених діями країни-агресора, підвищенню ефективності взаємодії між вітчизняними науковцями та практиками, експертами й законотворцями.

Бажаю всім конструктивних ідей та приємного спілкування, запрошую до дискусії! Дякую за увагу!

З повагою,
ректор Національної академії СБ України,
доктор юридичних наук, доцент
Андрій ЧЕРНЯК

Єхануров Ю. І.
кандидат економічних наук,
Київський національний університет
імені Тараса Шевченка,
український політик,
Прем'єр-міністр України (2005-2006 рр.),
Міністр оборони України (2007-2009 рр.)

ГІБРИДНА ВІЙНА – ТРЕБА АТАКУВАТИ!

Основним завданням вітчизняних науковців і практиків є вироблення ефективних заходів для протидії гібридній війні.

На мою думку, потрібен атакувальний підхід, що полягає в асиметричній відповіді на атаки суперника, тобто бити по основним «скрепам».

Зокрема, науковці повинні знайти спільне «руського мира» з ідеологіями націонал-соціалізму та комунізму, і згодом на законодавчому рівні має відбутися прирівняння цих ідеологій.

Крім того, потребує ґрунтового опису ситуація з колаборантами у Другій світовій війні, зважаючи на наявність достатнього матеріалу на цю тему. Однак, до цих пір відсутні наступальні роз'яснення про значну чисельність і роль російських підрозділів, у тому числі в складі СС. Цей матеріал має знати не тільки кожен українець, починаючи зі школи, але й кожен росіянин.

Ще одна тема, яка потребує детального наукового дослідження – роль програми ленд-лізу під час війни. Ленд-ліз припинився у 1947 році, і одразу наступив голод у Радянському Союзі.

Наше завдання – не давати приватизувати власну історію нашому хамовитому сусіду. Відтак існує потреба у виробленні чеканих формулювань про Київську Русь, Велике Князівство Литовське, Річ Посполиту, Російську імперію, Радянський Союз тощо. І це робота для вчених-гуманітаріїв, насамперед, з НАН України.

Україна є форпостом Західної цивілізації. Ми орієнтовані на Європу. З об'єктивних причин українське суспільство не пройшло деякі, як виявилось, обов'язкові етапи свого структурування та розвитку, і це треба надолужувати. Стадію становлення української політичної нації ми проходимо лише зараз. У сучасному світі немає часу на повільний розвиток. Те, що інші держави проходили століттями, ми маємо пройти за 1-2 десятиліття. Суттєво цьому «допомогла» російська агресія.

Існує необхідність у якнайшвидшому закріпленні тих положень, про які йшлося вище, і рухатися далі. Важливу роль відіграють мова, віросповідання, відношення до діаспор. Потрібна інтенсивна дискусія в суспільстві і закріплення у свідомості більшості населення чеканих формул.

Томенко М. В.
кандидат історичних наук,
доктор політичних наук, професор,
політичний діяч України,
Київський національний університеті
імені Тараса Шевченка

ІСТОРИКО-ПОЛІТОЛОГІЧНІ МІФИ ТА ЗАГРОЗИ «РОСІЙСЬКОГО СВІТУ» В УКРАЇНІ

Нині в сучасному інформаційному просторі, включно із соціальними мережами, платні й світоглядні друзі Путіна в Україні системно і послідовно поширюють історичні та політологічні міфи й вимоги, які сформульовані в так званій доктрині «Російського світу Путіна».

Якщо на початку 90-років 20 століття ідеологами та пропагандистами «Російського світу», а відповідно й проекту боротьби з НЕЗАЛЕЖНОЮ УКРАЇНОЮ були радикально-націоналістичні та українофобські організації та особи, то тепер маємо справу з офіційною, державною доктриною Росії.

Недаремно в Указі Президента Російської Федерації «О Стратегии национальной безопасности Российской Федерации» від 2 липня 2021 року для досягнення цілей зовнішньої політики Російської Федерації вказані такі завдання:

«...18) ...укрепление позиций русского языка как языка международного общения;

19) оказание поддержки соотечественникам, проживающим за рубежом, в осуществлении их прав, в том числе права на сохранение ОБЩЕРОССИЙСКОЙ культурной идентичности, обеспечение защиты их интересов;

20) укрепление братских связей между русским, белорусским и украинским народами...»

Див. Static.kremlin.ru

А в сумновідомій статті Володимира Путіна «Про історичну єдність росіян та українців», розміщеної на сайті Президента Росії російською та українською мовами, сформульовані головні історичні міфи «Російського світу», які формувалися та пропагувалися останні століття через переписування історії та фальсифікацію та знищення історичних джерел.

Див.kremlin.ru

Отож, маємо щонайменше 5 історико-політологічних міфів для утвердження так званого «Російського світу» в Україні.

1. Росіяни, українці та білоруси – «єдиний православний народ».

Московщина з моменту крадіжки давньої назви України - Русь й до нині активно просуває власну фальшиву історію етногенезу власного народу як єдиного «государствообразующего» для росіян, українців та білорусів. Для цього створювалися спеціальні комісії, переписувалися і знищувалися джерела, заборонялися і цензурувалися науково-сумлінні історичні праці тощо.

2. Україна – «багатонаціональна держава і повинна бути федерацією з двома державними або офіційними мовами».

За всіма ознаками сучасна Україна - НАЦІОНАЛЬНА держава з поліетнічним складом населення, де лише українці споконвічно живуть на своїй історичній території та не мають іншої держави де-інде і кримські татари - відповідно на території Криму. Всі решта - росіяни, євреї, поляки, румуни, угорці...пошановані в Україні національні меншини, які мають власні держави поза межами України. Тут не обговорюємо тему малих корінних народів та етносів, таких як кримчаки, караїми чи гагаузи.

Відповідно й мовна політика, яку визначив Основний Закон: єдина державна – українська і захист та підтримка мов національних меншин.

3. Подвійне громадянство – «це найкращий варіант для громадян сучасної України та діаспори».

Введення подвійного громадянства по-перше, неможливе без всеукраїнського референдуму (див відповідно статті 4 та 156) і по-друге - з міркувань геополітичних та олігархічних загроз та з огляду на відкриття земельного ринку.

4. «Нейтральний статус передбачений Конституцією й захистить та збереже Україну».

Про нейтральний статус у майбутньому йдеться в Декларації про державний суверенітет від 16 липня 1990 року. Цей документ - важливий у справі підготовки проголошення Незалежності, проте

мав перехідний характер від УРСР до самостійної України. Про нього не згадує чинна Конституція і якщо виконувати пункт Декларації про нейтральний статус, то чому не виконувати інші пункти: про Союзний договір на базі СРСР і збереження громадянства СРСР?!

5. НАТО – «це військові бази на території України, а отже і неминуча ВІЙНА з “братською” Росією».

Важливо нагадати, що стаття 17 Конституції прямо забороняє розташування іноземних військових баз на території України. Тож створення та розміщення баз НАТО чи інших військових союзів і організацій можливе лише за згоди українського народу через Всеукраїнський референдум. (знову нагадую про особливість внесення змін до Розділу 1 Конституції України, див. статтю 156).

Отож, коли ми чуємо від формально українських політиків, експертів чи журналістів ці тези - ми повинні розуміти, що йдеться про відпрацювання своєрідного ТЕМНИКА ПУТІНА для будівників «російського світу» в Україні.

Для протидії цій доктрині «Російського світу» в Україні потрібна максимальна координація дій як відповідних органів державної та місцевої влади так і наукового та експертного середовища. Необхідно невідкладно актуалізувати перелік пріоритетних тем та проектів, що їх виконують гуманітарні Інститути НАН та виші України. Не менш важливим завданням є також підтримка відповідних медіапроектів.

Лише спільна діяльність може створити систему протидії доктрині «Російського світу» в Україні та забезпечить просування і утвердження власної світоглядної доктрини «Українського світу».

Зеленько Г. І.

член-кореспондент Національної академії наук України,
доктор політичних наук, професор,
Інститут політичних і етнонаціональних
досліджень ім. І. Кураса НАН України

ЕКОНОМІЧНІ ЗАГРОЗИ ТА ЇХ ПОТЕНЦІАЛ В РОСІЙСЬКО-УКРАЇНСЬКОМУ ПРОТИСТОЯННІ

В останні кілька десятиліть таке поняття як «війна» істотно трансформувалося і поняття «гібридна війна», «безконтактна війна» або військовий збройний конфлікт.

Звісно, що це є дуже позитивним явищем. Водночас поява нових різновидів і форм війн ускладнює стратегію їх ведення. Якщо у звичайній війні, незважаючи на ті фізичні, матеріальні та моральні втрати, які вона несе – все зрозуміло – де ворог, де лінія фронту, які озброєння застосовуються і т.д. То у війнах нового покоління вищезгадані поняття, характерні для звичних воєн, розмиваються або й взагалі не існують. Таким чином це спричиняє дезорієнтацію і не дає можливість обрати вірно форми та засоби ведення війни, прорахувати наслідки і т. ін.

Водночас у нас зараз чи не вживанішим поняттям є поняття «гібридна війна». Причому якщо ми її вживаємо по відношенню до Російської Федерації, то у РФ це поняття вживають по відношенню до Заходу і усіх країн, які не підтримали Росію у її агресії проти України, анексію Криму тощо. На наш погляд, така постановка питання дещо дезорієнтує громадян, які беруть участь у цій війні, намагаючись у ній протистояти супернику. Адже будь яка війна «гібридна» чи «безконтактна» має свої складові, направленість і т. ін. Тому тут важливо структурувати цей різновид війн з тим, щоб їм успішно протидіяти.

Якщо вести мову конкретніше про російсько-український конфлікт, то тут очевидно, слід зануритися в історію і згадати таке: Україна фактично до 2014 року перебувала у сфері впливу РФ і збройний конфлікт трапився як наслідок того, що Україна підписанням Угоди про Євроасоціацію спробувала вирватися зі сфери впливу Росії. Проте за період перебування у тому ж такій впливі РФ в Україні сформувалися не просто стійкі ідентичності (ставлення громадян окремих регіонів до РФ), які війна, яка триває з 2014 р. слабо змінила. Сформувалася, а точніше дісталася у спадок від СРСР доволі стійка соціально-економічна кооперація, яка наразі і є найвразливішою точкою у тій такій безконтактній війні. Якщо подивитися статистику, то Росія й надалі входить до п'ятірки найбільших торговельних партнерів. За останніми оцінками вона є третім торговельним партнером України, що досить парадоксально, зважаючи на те, що Україна і Росія фактично вже сьомий рік перебувають у статусі оголошеної війни. Натомість як Україна для Росії не входить навіть у десятку основних торговельних партнерів. Іншими словами – український експорт не є критично важливим для Росії. Тоді як для України експорт товарів на російський ринок є критично важливим з огляду на те, що Росія не просто входить у трійку найбільших торговельних партнерів України, а й структура українського експорту до Росії істотно відрізняється від структури українського експорту на європейські ринки. З Росією ми

торгуємо переважно продукцією з високою додатковою вартістю – високотехнологічна продукція. Велика кількість українських підприємств причому у сфері переробної промисловості або з високою додатковою вартістю (турбіни, комплектуючі) орієнтовані виключно на російський ринок. За роки російсько-української війни Україна так і не спромоглася знайти їм заміну, диверсифікувавши ринки збуту.

Тому наразі основним викликом у так званій «безконтактній війні» є саме економічна сфера. І якщо ми вже навчилися більш-менш адекватно реагувати на інформаційні випадки РФ, на різноманітні провокації, у позиційну війну переросла війна на Донбасі, то перед економічними викликами з боку РФ Україна фактично безсила. І у разі, якщо Росія все ж захоче остаточно розправитися з Україною, а це можливо у разі послаблення підтримки Заходу, точкові удари будуть завдані саме по статтях торгівлі з Росією і по цих підприємствах. Тому нам наразі слід думати про нові структурні компоненти безконтактної війни і заздалегідь шукати адекватну відповідь (реакцію) на подібні дії. І якщо за роки Російсько-українського протистояння ми вже навчилися реагувати на російську пропаганду, інформаційні впливи, війну на Донбасі перевели фактично у стан позиційної війни низької інтенсивності, то економічні позиції залишаються надзвичайно вразливими, що створює передумови для нанесення «ударів» по цих больових точках у найближчому майбутньому.

Бебик В. М.

доктор політичних наук, професор,
голова Всеукраїнської асоціації політичних наук

ТЕОРЕТИЧНІ ТА ПРАКСЕОЛОГІЧНІ ЗАСАДИ ГІБРИДНИХ ВІЙН

Системно-аналітичний підхід до проблем дослідження особливостей протистояння російській гібридній агресії проти української демократії потрібно здійснювати не тільки через призму традиційних та латентних військових дій російської армії, фінансованих Росією терористів і найманців, спеціальних операцій російських спецслужб проти України. Всі ці процеси, на наш погляд, потрібно розглядати в контексті:

- цивілізаційного, ідейно-політичного протистояння тоталітарних форм організації суспільства (в даному випадку у формі «російської

квазі-імперії») і демократичних форм організації суспільства (у формі так званої «української олігархічної республіки»);

- особливостей формування глобального інформаційного суспільства та української національної моделі інформаційного суспільства, особливостей становлення і функціонування глобального інформаційного простору та українського національного інформаційного простору.

На жаль, формування глобального інформаційного суспільства не змогло заблокувати війни як спосіб розв'язання політичних, економічних, територіальних, етнічних, релігійних та інших конфліктів. Більше того, процеси запровадження сучасних інформаційно-комунікаційних, соціально-політичних та соціально-психологічних технологій зробили ці війни більш витонченими і підступними.

В умовах інформаційних війн руйнуються суспільні організми (державні, політичні, соціальні інститути і організації), деформується цивілізаційно-культурний код нації і суспільна мораль, руйнується почуття патріотизму, розхитується людська психіка, паралізується здатність народу до спротиву агресії ворога.

Домінування інформаційних чинників при веденні інформаційних та гібридних війн визначається сутністю інформаційного суспільства, яке, на думку його ідеологів, визначається якісним переходом людської цивілізації від аграрної та індустріальної до інформаційної стадії розвитку, коли інформаційно-комунікаційні ресурси стають набагато важливішими, ніж матеріально-технічні ресурси суспільства.

Відповідно до цієї базової філософської конструкції, в умовах інформаційної та гібридної війни противник активно використовує соціальні структури, які мають достатньо вагомий вплив на глобальну суспільну свідомість та національну суспільну свідомість країни, що стала об'єктом інформаційного нападу відразу чи протягом тривалого часу:

- засоби масової комунікації: ефірне, кабельне, супутникове телебачення і радіо, мобільний відео, аудіо та інтернет-зв'язок, соціальні мультимедіа мережі, сайти, паперові та електронні газети, журнали і книги;

- релігійні, культурологічні, профспілкові, екологічні, правозахисні, журналістські та інші соціальні організації;

- дипломатичні структури (МЗС, посольства та представництва при міжнародних організаціях);

- зовнішню розвідку (через своїх таємних та легалізованих агентів в мас-медіа, міжнародних та суспільних організаціях).

Досліджуючи проблеми інформаційних і гібридних війн варто, зрештою, розібратися з термінологією і визначитися, який же зв'язок існує між цими поняттями, що активно використовуються у виступах політиків та повідомленнях мас-медіа.

Пропонуємо розглядати гібридну війну як логічне продовження інформаційної війни, коли тривалі інформаційно-психологічні атаки на національний інформаційний простір та суспільну свідомість нації, які є об'єктом нападу агресора, на останньому етапі закінчуються введенням на територію країни (жертви нападу) обмежених військових контингентів.

Варто особливо відзначити, що процеси глобалізації в економіці, політиці, соціальній та духовній сферах відбувалися на основі революційного запровадження нових інформаційно-комунікаційних технологій. Перехід на сучасні інформаційно-комунікаційні технології та мультимедіа платформ кардинально змінив не тільки особливості продукування, обробки та трансляції інформаційних масивів та повідомлень, але й змінив особливості та технології сприйняття інформації суспільною свідомістю, що має врахувати у своїй практичній діяльності зовнішня розвідка України.

Зрозуміло, що інформаційні війська противника завжди спрямовані на руйнування національного інформаційного простору та суспільної свідомості суспільства, яке є об'єктом нападу.

На українському прикладі можемо відзначити, що національний інформаційний простір України формується в складних геополітичних та цивілізаційно-культурних умовах: недостатньо сильної держави, олігархізованих і де-українізованих мас-медіа, потужного впливу засобів масової інформації нашого ворога - Росії.

Стратегічно важливими є й головні ідеологічні пріоритети та базові цінності, які мають бути покладені в основу функціонування національної моделі інформаційного суспільства в умовах ведення проти нього гібридної війни.

На думку французького дослідника Бертрана Коста, найбільшою проблемою України сьогодні є те, що її розглядають у світі як країну з двома націями (українці і росіяни). І пріоритетом тут має бути створення політично інтегрованої нації на одних спільних демократичних цінностях.

Саме цю тезу, на нашу думку, і мають просувати в глобальному інформаційному просторі інформаційні війська України, у тому числі, силами та засобами зовнішньої розвідки.

Розпочавши гібридну війну проти України і зруйнувавши правовий світовий порядок, який було встановлено після 1945 року, Росія фактично розв'язала Третю світову війну проти всього цивілізованого світу, який поступово починає розуміти всі небезпеки гібридних воєн російського агресора. Тому гібридна російська квазіімперія, на думку експертного середовища, не має довгострокових шансів на виграш, оскільки ресурсно не здатна конкурувати з провідними глобальними гравцями (США, КНР, ЄС, Японією та Індією).

У найближчій історичній перспективі Росія, напевно, припинить своє існування (втратить частину своїх територій або «конфедерується»):

- не зважаючи на велику територію, чималі енергетичні ресурси і потужний ядерний потенціал;
- зважаючи на невеликі людські ресурси і виродження російської нації;
- науково-технологічну відсталість та неспроможність корумпованої російської еліти здійснювати модернізацію економічної та політичної системи РФ.

Падіння гібридного політичного режиму в Росії, на нашу думку, буде значно прискорене:

- енерго-технологічною революцією (переходом на нові, відновлювані джерела видобування електроенергії);
- фінансово-економічними і науково-технологічними санкціями проти Росії (за окупацію Криму і Донбасу, підтримку ІДІЛ та втручання у внутрішні справи країн НАТО);
- консолідацією глобальних держав в протистоянні інформаційній експансії Росії в глобальному інформаційному просторі;
- «гібридними технологіями» повернення Маньчжурії до складу КНР, яка прагне повернути свої землі відповідними методами економічної та етнічної політики на Далекому Сході;
- політико-дипломатичними та економічними діями Японії, яка прагне повернути о. Сахалін та Куріли;
- «технологіями руйнування Берлінської стіни» з боку ФРН, яка складними дипломатично-економічними іграми (рано чи пізно) захоче повернути окупований росіянами Кенігсберг.

Сучасний досвід українського державотворення показав, що Україна вибрала ліберальну модель формування інформаційного суспільства. В результаті держава фактично віддала національний інформаційний простір вітчизняним та зарубіжним олігархам, які в критичні часи працювали (і частково продовжують працювати) проти України, та зарубіжним інформаційним та спеціальним військам.

У цьому контексті експерти з національної безпеки вважають, що потрібно в Конституції України, як в суспільному договорі, визначити взаємовідносини нації, як замовника на послуги держави, і держави, яка має надавати українському суспільству ці послуги; особливо в інформаційно-комунікаційній сфері, яка стає провідним театром військових дій в умовах гібридної війни проти Росії.

Тітко Е. В.

доктор юридичних наук, доцент,
Голова ГО «Український осередок з прав людини
та розвитку освітніх новацій»,
Університет державної фіскальної служби України,
Навчально-науковий інститут права

РОЛЬ ТА ЗНАЧЕННЯ ЦИВІЛЬНО-ВІЙСЬКОВОГО СПІВРОБІТНИЦТВА (СІМІС) У ВИБРАНИХ СУЧАСНИХ ОБОРОННИХ СТРАТЕГІЯХ КРАЇН СВІТ

Сьогодні необхідність вивчення такого феномена, як цивільно-військове співробітництво (СІМІС, ЦВС), вже не викликає сумнівів. Так як при виконанні операцій завдання військових сил полягають не в досягненні результатів будь-якими способами і витратами, а проведення місії, в першу чергу, повинно проходити з мінімізацією втрат і наданням захисту місцевого населення, на благо «життя», де очікуваний результат – це світ і безпека для людини.

Особливість ЦВС полягає в тому, що військові сили повинні бути в тісній співпраці з цивільною складовою, до якої відноситься все цивільне середовище: місцеве населення, місцевість, організації (урядові, неурядові), цивільні установи, місцеві авторитети та багато іншого. Багаторічна практика показала, що без тісної співпраці виконання місій є важким [1, с. 22].

Так, на прикладі Франції, яка є однією з країн-засновниць НАТО і має свою історичну специфіку участі. Згідно військовій доктрині Франції – ЦВС відводиться особлива роль і, французька політика в сфері СІМІС є дуже показовою як на доктринальному, так і на координаційній рівні. Відповідно до «Білої книги оборони та національної безпеки» від 2013 року, визначено наступні: (1) в сферу зовнішньої і внутрішньої безпеки включаються як військові засоби, так і цивільні інструменти; (2) здійснюється координація між цивільними та війсь-

ковими департаментами та установами; (3) відбувається відповідне наповнення і забезпечення Європи військовим і цивільним потенціалом; (4) надається максимальна можливість здійснення політики в професійній підготовці як цивільних, так і військових; (5) наголошено на важливості цивільно-військової операції у врегулюванні кризових ситуацій; (6) формується система необхідних людських ресурсів для задоволення зростаючих потреб, наприклад, поліції, адвокатів та ін. [4].

У положеннях даної Білої книги виділяються три типи операцій в контексті ЦВС: (1) «цивільні операції», до яких відносяться гуманітарна допомога або відновлення громадянського суспільства; (2) «цивільно-військові операції», які проходять приблизно на іноземній території, в контексті стабілізації або реконструкції; (3) «військові операції», як правило, сприяють створенню нової політичної обстановки на місцях і досягненню цивільних цілей. Цікавими особливостями військової політики Франції є те, що ЦВС направлено ще й на боротьбу зі злочинною торгівлею за межами національної і європейської території, де використовується як цивільний, так і військовий потенціал [4].

Безпосередньо положення СІМІСа прописані у «французькій доктрині СІМІС» (*Doctrine interarmées DIA-3.10.3 (A) СІМІС*, 2012), яка вказує на його мету – співпраця між цивільними і військовими силами. Основними положеннями даної Доктрини, на яких слід акцентувати увагу, є наступні: участь СІМІСа в короткостроковій і довгостроковій перспективі операцій; зміцнення своїх позицій серед місцевого населення в зоні проведення операції, що безпосередньо впливає на мінімізацію наслідків військових операцій для населення; планування СІМІСа на політичних і військових (стратегічний, оперативний і тактичний) рівнях; оцінка рамок зобов'язань на початковому етапі операції, де співпраця між цивільними та військовими сприяє підготовці прогнозів сил, в тому, що стосується залучення їхніх фахівців до громадянської обстановки в зоні дій. У Доктрині виписані основні принципи в області співпраці між цивільними і військовими силами двох типів [3].

Разом з тим, в німецькому варіанті термін ЦВС виглядає як *Zivil-Militärische Zusammenarbeit*, ZMZ і описує взаємодію урядових і неурядових організацій, в умовах / рамках яких функціонує військовий захист в області національної оборони військових операцій. Це включає в себе всі плани, угоди, заходи, сили і ресурси, які підтримують, полегшують відносини між військовими установами і громадськими організаціями, а також цивільними особами. До них відносяться такі критерії: допомога цивільному населенню; участь ЗС у сфері цивіль-

ного захисту, зокрема, шляхом підтримки громадських організацій в великомасштабних надзвичайних і кризових ситуаціях; співробітництво між збройними силами та цивільними органами в охороні здоров'я, охорони навколишнього середовища тощо. Тобто визначення СІМІС, в першу чергу, йде через поняття «допомоги», що і є прямим прообразом суті ЦВС. Також необхідно додати, що відповідно до німецької доктрини оборони «Керівні принципи оборонної політики» від 2011, ЦВС розглядається як інструмент для запобігання конфліктам, регулювання криз і надання підтримки у постконфліктному відновленні через сили НАТО і ЄС [6].

Однак «німецька концепція ZMZ» спрямована як на внутрішнє розгортання сил в разі надзвичайних ситуацій, так і на іноземне розгортання в рамках військових і гуманітарних місій.

Разом з тим, відповідно до Доктрини спільних операцій Сполученого Королівства від 2014 року (UK Joint Operations Doctrine) зазначено, що операції, які проводяться, наприклад, під керівництвом ЄС, можуть включати цілий ряд важелів влади, в тому числі дипломатичних, економічних, гуманітарних і цивільних, а також військових, і тому їх необхідно координувати [5]. Британський СІМІС ґрунтується на національній Доктрині цивільно-військового співробітництва 3-90 від 2003 р. [2]. Хоча Сполучене Королівство погоджується з визначенням НАТО, підхід країни полягає в «розгляді СІМІСа в контексті того, щоб дозволити військовим операціям внести більш узгоджений внесок в досягнення Сполученого Королівства і міжнародних політичних цілей. Сполучене Королівство робить це за рахунок повної інтеграції персоналу і процесу СІМІС в ланцюжок командування. Це принципово відрізняється від підходу, застосовуваного деякими іншими країнами, особливо США.

Таким чином практичний та доктринальний досвід вибраних стратегій різних країн світу має велике значення у напрямку застосування сил СІМІС, що і впливає на формування, як міжнародних так і національних доктрин, які (вибрані) лягали в основу тієї ж, наприклад, Доктрини СІМІС НАТО.

Література

1. Титко Э.В. Международно-правовые аспекты (СІМІС). Винница. ТОВ «Нилан-ЛТД». 2021. 544 с.
2. Civil-Military Cooperation (СІМІС), Interim Joint Warfare Publication 3-90, 2003. URL: [http://ids.nic.in/UK%20Doctrine/UK%20\(3\).pdf](http://ids.nic.in/UK%20Doctrine/UK%20(3).pdf).
3. Doctrine interarmées DIA-3.10.3(A)_СІМІС, Centre interarmées de concepts, de doctrines et d'expérimentations, 2012. URL: http://www.cicde.defense.gouv.fr/IMG/pdf/20120717_np_cicde_dia-3-10-3a-cimic.pdf.

4. The French White Paper on defence and national security, 2013. URL: [https://www.defense.gouv.fr/content/download/215253/2394121/White paper on defense2013.pdf](https://www.defense.gouv.fr/content/download/215253/2394121/White%20paper%20on%20defence2013.pdf).

5. *UK Joint Operations Doctrine, Joint Doctrine Publication 01 (JDP 01)*, 2014. URL: <https://goo.gl/pwkwjL>.

6. Verteidigungspolitische Richtlinien, 2011. URL: <https://goo.gl/th4uca>.

Горовий В. М.

доктор історичних наук, професор,
заслужений діяч науки техніки,

Національна бібліотека України імені В.І. Вернадського

НАУКОВО-ІНФОРМАЦІЙНИЙ АСПЕКТ ПРОТИСТОЯННЯ НЕГАТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ

Важливим завданням сучасних гуманітарних наук є дослідження трансформації системи соціальних структур держави, нації в умовах розвитку глобальної інформатизації. Характерною особливістю цих структур стало зростаюче значення в їх прояві етнонаціонального чинника, що знаходить нові можливості для розвитку завдяки розширеному доступу до зростаючих обсягів інформації. Дана обставина має враховуватись при розробці стратегії оборони в інформаційній війні і активної протидії інформаційній агресії РФ.

Насамперед, слід зазначити, що на перше місце в боротьбі з негативними зарубіжними впливами в інформаційній сфері мають входити інформаційні ресурси, **вироблені на основі сучасної етнонаціональної єдності українського народу**. Вони мають акумулювати в собі ментальні особливості всіх регіонів України, включаючи недостатньо вивчений розвиток сучасної ментальності Слобожанщини півдня України національних меншин на території нашої держави. Йдеться, таким чином, про наукове освоєння і використання етнонаціонального матеріалу, знаходження в ньому спільних особливостей на рівні реалізації державницьких інтересів, формування сучасних орієнтирів розвитку України.

При цьому, саме держава має стати замовником і координатором у виробленні об'єднуючої українське суспільство системи орієнтирів розвитку. Для цього має бути організоване співробітництво гуманітар-

ної сфери вітчизняної науки, органів державної влади, культури, освіти, громадських організацій культурологічного спрямування. Уже визначений вектор розвитку, напрацювання практичного досвіду суспільної трансформації на основі етнонаціонального синтезу на даному етапі мають бути відображені в кінцевому результаті – в концептуальному документі – офіційному дороговказу для розвитку України.

Такий документ потрібен, насамперед, для внутрішньої консолідації України. В тому числі, для ефективного розвитку децентралізації та налагодження співдружності з нацменшинами.

Крім забезпечення політичної стійкості українського суспільства, прогнозованості і зрозумілості його розвитку на міжнародній арені, дані орієнтири стають ефективною основою організації оперативного протистояння зовнішній інформаційній агресії.

Суттєве значення ці орієнтири можуть мати також для налагодження зав'язків України з усіма категоріями наших земляків за кордоном:

- для більш ніж тримільйонної чисельності українських заробітчан в Росії національні українські орієнтири розвитку мають стати уявленням про свою життєву перспективу на майбутнє при поверненні в Україну;

- для організацій, в яких об'єднуються етнічні українці в місцях суспільного проживання в Росії (регіони Тюмені, Новосибірська, Далекого Сходу та ін.) такі орієнтири можуть бути основою для обґрунтування національної єдності українців в еміграції, культурологічного розвитку української діаспори в контексті загальноукраїнського еволюційного процесу;

- для так званої російської еміграції в Росії та світі загальноукраїнські орієнтири розвитку з допомогою сучасних інформаційних технологій дають можливість зберігати етнонаціональний зв'язок з Україною, з її духовністю, можливість солідаризуватися з її національним розвитком.

Зміцнення зав'язків з українцями, що проживають в Росії, включаючи тих, що в силу історичних обставин одержали російське громадянство, матиме стабілізуюче значення для збереження дружніх відносин з населенням сусідньої країни, не зважаючи на наявну міждержавну інформаційну війну.

Слід зауважити, що етнонаціональний фактор може ефективно використовуватись не лише при захисті національного інформаційного простору від ворожої пропаганди, але й у активних інформаційних операціях на території противника в гібридній війні.

В активних операціях варто мати на увазі ту обставину, що при серйозному рівні російської суспільнознавчої науки, активізації політичних процесів, пов'язаних із відбудовою важливих елементів російської державності, особисто В. Путін і його найближче оточення демонструє відверту несхильність до формування ідеології розвитку в умовах сучасного глобалізму. При дотриманні даної позиції російським президентом, можна з достатньою вірогідністю прогнозувати після вичерпання ресурсу так званої «ідеології відбудови протягом одного-двох десятирічь значне послаблення стійкості російської державності.

При розробці стратегії інформаційного протистояння в інформаційній війні вітчизняні політтехнологи мають враховувати проблематичні перспективи російської державності.

Фактично сьогодні «безідейна» Росія знаходиться в оточенні ідейноорієнтованих сусідів США (з месіанською ідеєю принесення демократії американського зразка всьому світу), ЄС (з ліберально-демократичними варіаціями суспільної трансформації), Туреччини (з розвитком оновленого пантюркізму), Китаю (з китайським варіантом соціалізму). Під впливом глобальних процесів і інформатизації ідеології цих російських сусідів розвиваються, поширюють свій вплив і знаходять все більше прихильників, насамперед, в середовищі нацменшин, що не мають загальнодержавного вектора розвитку на безідейних просторах Росії.

Російська «безідейність» на сьогодні вже обернулася фактичним провалом багаторічної кампанії по поверненню росіян в РФ з бувших союзних республік.

Ще одна проблема нинішнього російського суспільства пов'язана з релігійним питанням, з фактичною офіційною орієнтацією нинішнього російського керівництва на РПЦ. Керівництво інших релігійних об'єднань офіційно співпрацює з путінським режимом, однак, в етнонаціональних неправославних масах населення такий стан справ викликає незадоволення і протиправні дії. Особливо це спостерігається в мусульманському середовищі. Чимало таки прикладів можна згадати і на Кавказі, і в Поволжі, і в інших регіонах. Так, скажімо, останнім часом ЗМІ не раз повідомляли про вивішені турецькі прапори на територіях мало не до полярного кола, де проживає мусульманське населення.

Безідейне суспільство поступово створює серйозні проблеми в молодіжному середовищі. Активізація етнонаціонального чинника в такому нестійкому світоглядному середовищі призводить до антису-

спільних проявів навіть в культурних центрах країни, що вже викликало стурбованість релігійних організацій в Москві. Красномовним фактом такого розвитку подій може бути рішення Казанських властей про введення загальнонаціонального анτισлов'янського свята.

Дослідження розвитку постіндустріального етапу розвитку суспільства підводять до висновку про зростаючі можливості енергетики етнонаціонального розвитку. В умовах трансформації сучасної загальнодержавної ідеології ця активність може знаходити шляхи своєї реалізації в розвитку державності. Однак, при відсутності державницьких орієнтирів, при відсутності в суспільстві сучасної ідеології етноси формують власні канали самореалізації. Прояв енергії цих каналів часто не співпадає з державними інтересами, призводить до національного радикалізму, до внутрішніх конфліктів.

Дані особливості сучасного національного розвитку мають враховуватись при вдосконаленні стратегії інформаційного протистояння в гібридній війні. Енергія етнонаціонального розвитку в умовах глобальної інформатизації може стати важливим чинником протистояння в інформаційній агресії.

Новакова О. В.

доктор політичних наук, професор,
Національний педагогічний університет
імені М. П. Драгоманова

ПРОПАГАНДИСТСЬКІ НАРАТИВИ ЯК ЗБРОЯ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В ГІБРИДНІЙ ВІЙНІ ПРОТИ УКРАЇНИ

Інформаційне суспільство не тільки наступило, але і почало розвиватися та набувати все нових, більш складних форм. Поставленої мети тих чи інших суб'єктів соціально-політичної діяльності вже складно досягти лише за рахунок створення простих інформаційних меседжів, вибагливий споживач інформації потребує все більш витончених та креативних форм. Однією з таких форм стало створення наративів – історій та оповідань, які у формі живої розгорнутої та багатопланової розповіді просувають потрібні цінності, цілі та ідеали.

В своїй фундаментальній праці «Джерела соціальної влади» Майкл Манн як одну з тенденцій розвитку сучасного суспільства визначив те, що у військовій сфері Марс виходить з тіні Меркурія, тоб-

то активізуються агресивні конфліктні дії у вирішенні як внутрішніх, так і міжнародних проблем. Те саме можна сказати і про розвиток інформаційної сфери, де створений продукт все частіше використовується саме як зброя, метод агресивного вторгнення, брутального спотворення цінностей аж до повного руйнування межі між добром і злом, або між правдою та брехнею в інформаційному контексті.

Яскравим прикладом використання інформаційного продукту як зброї є діяльність Російської Федерації, що веде війну проти нашої країни. Чи не головним методом цієї війни є інформаційна агресія, розв'язана Російською Федерацією з метою створення викривленої реальності та системи цінностей на користь агресора, послаблення та руйнування національної ідентичності і громадянської свідомості українців.

Пропагандистські операції Росії характеризуються дестабілізацією інформаційно-комунікативного простору, застосуванням великої кількості джерел інформування з метою дискредитації та фейкового спростування правдивих повідомлень. Яскравим прикладом агресивних інформаційних кампаній є створення та розповсюдження пропагандистських наративів. Таких, як так звана доктрина «ДНР» «Русский Донбасс», просування змісту якої ґрунтується на тезах: «Донбас – історична частина Росії», «право розмовляти рідною мовою», «братовбивча війна на Донбасі» та ін. За допомогою таких інформаційних диверсій російські агресори намагаються змінити свідомість громадян, спотворити розуміння реальності та використати їх як безвольний ресурс у гібридній війні.

Модель, що застосовується російськими пропагандистами, достатньо потужна. Сила її полягає в високій ресурсній забезпеченості, діяльності широкої мережі каналів передачі інформації. До того ж, російські ЗМІ не опікуються правдивістю інформації, тому не витрачають часу на перевірку даних, вони самі створюють потрібні «новини», їх відповідність реальності абсолютно для них не важлива, головне, щоб досягалася поставлена мета.

Створення пропагандистських наративів підготовляє ґрунт та супроводжує будь-які політичні акції Росії. Так, справжня атака з її боку на навчання Sea Breeze, мала відповідну інформаційну складову. Майже одночасно із мирним проходом британського есмінця в 12 милях від Криму, російські ЗМІ вибухнули заявами про «агресивний характер навчань» і закликами до США й НАТО їх зупинити.

Дана інформаційно-пропагандистська кампанія, спрямована на дискредитацію НАТО та виправдання російської мілітаризації регіо-

ну отримала своє так би мовити «укорінення» в реальній державній політиці РФ. Так, було прийнято закон, який надає право Національній гвардії РФ здійснювати блокування територій та акваторій, прилеглих до низки об'єктів, грубо нехтуючи правами України як прибережної держави щодо Чорного та Азовського морів і Керченської протоки.

Важливість пропагандистських наративів для Росії підтверджується хоча б тим, що часто вони озвучуються першою особою держави – В. Путіним та його глашатаєм – Д. Песковим. Д. Песков 5 липня виступив з заявою, що В. Путін особисто працює над статтею про справжні відносини між росіянами та українцями, де буцім то відкриє єдину та святую правду про «братню єдність та історичний зв'язок». Останнім часом російські спікери буквально вибухнули власними історіями про «єдиний народ», який, мовляв, споконвіку існував в триєдності «великоросів, білорусів і *малоросів (!???)*», який «намагалися розтягнути і роздрібнити», зокрема зусиллями Речі Посполитої і Австро-Угорщини. Активізація цього наративу пов'язана з незадоволенням російської влади законопроектом, що ініційований Володимиром Зеленським про корінні народи на території України. Причому ступінь цього незадоволення сягнула того, що Путін порівняв цей законопроект зі зброєю масового ураження. Таким чином, мова йде про пряме агресивне втручання у внутрішню політику України шляхом просування пропагандистських наративів.

Таких прикладів можна назвати ще безліч, всім вони добре відомі, але хочу ще раз підкреслити особливу загрозу таких пропагандистських впливів з огляду на їх стратегічний, цілеспрямований характер та повномасштабну підтримку на рівні державної політики. Так уже 3 липня Володимир Путін затвердив стратегію національної безпеки країни, в якій, крім іншого, прописані плани стосовно українців. У документі зазначено, що досягнення цілей зовнішньої політики Кремля буде реалізовано зокрема за допомогою зміцнення «братніх зв'язків між російським, білоруським та українським народами». Окреслені і методи досягнення поставленої мети - зміцнення позиції російської мови як «мови міжнародного спілкування» і підтримка громадян РФ, які проживають в інших країнах, в збереженні їх «загальноросійської культурної ідентичності».

З такої ситуації постає головне питання – як здійснити ефективний захист нашого інформаційного простору, свідомості та ідентичності українців, досягти достатнього рівня безпеки розвитку держави. Ці особливості ускладнюють розробку механізмів боротьби та проти-

дії масованій дезінформації. В даній ситуації недостатньо діяти «у відповідь», руйнуючи та спростовуючи брехливі повідомлення, необхідно звертатися до превентивних дій, створювати власний якісний контент та досягати найширшого його розповсюдження.

Так, наприклад, зрозуміло, що реальна деокупація Криму на сьогодні неможлива. Але всі також добре знають, що задовго до фактичної окупації Російська Федерація активно створювала, розповсюджувала, укоріняла в свідомості громадян та міжнародному інформаційному полі деструктивні наративи про історичну єдність Росії та Криму, відірваність Криму від України, існування своєрідного «кримського народу» та інше.

Відповідно до цього, вже сьогодні, не очікуючи настання моменту для реального повернення Криму, необхідно активно просувати змістовні, креативні та масштабні наративи, спрямовані на гуманітарну деокупацію Кримського півострова. Мовою культури та історії розповідати про формування ідентичностей, роль українців у розвитку Криму, культурних зв'язках, порушеннях прав людини, штучну мілітаризацію Кримського півострова та Чорного моря з боку РФ, долю політв'язнів та ін.

Ще приклад. Прес-служба Генштабу Збройних Сил України повідомила, що «17-30 липня 2021 в Міжнародному центрі миротворчості та безпеки Національної академії сухопутних військ імені гетьмана Петра Сагайдачного відбудуться Багатонаціональні військові навчання Литовсько-польсько-української бригади імені Великого гетьмана Костянтина Острозького «Три мечі 2021»». В контексті нашої теми необхідно зазначити, що було б дуже корисно підготувати ґрунт для цієї події, створивши наративи, які, з одного боку, доводили б до широкої громадськості, як в Україні, так і за кордоном (зокрема і на окупованих територіях) справжні цілі та завдання таких навчань, а з іншого – демонстрували послідовність України у досягненні мети захисту власного суверенітету та територіальної цілісності шляхом розширення взаємодії з демократичними партнерами, попри усі закиди російської пропаганди.

Шемаєва Л. Г.
доктор економічних наук, професор,
Національний інститут стратегічних досліджень

ВИМУШЕНЕ ЗБІЛЬШЕННЯ ОБОРОННИХ ВИТРАТ ЄВРОПЕЙСЬКИМИ КРАЇНАМИ ЯК ІНСТРУМЕНТ ГІБРИДНОЇ ВІЙНИ З БОКУ РФ

Гібридна агресія проти України, активна фаза якої розпочалася у 2014 році, призвела до суттєвого погіршення динаміки соціально-економічних процесів та прискорення міграційних процесів, порушення цілісності економічної та митної території, а також втрати частки економічного потенціалу й виробничих потужностей нашої держави. Використання в ході агресії «вузьких» місць економіки України, насамперед – високої залежності, зокрема, на низці сегментів енергетичного ринку, суттєво підвищило негативні наслідки для економічного й соціального розвитку держави, а також погіршило умови розвитку та фінансування важливих проектів національної безпеки.

Ситуація навколо України вже давно вийшла за межі регіонального протистояння та має далекосяжні наслідки для всієї європейської системи міжнародної безпеки. «Український фронт» гібридної війни РФ має за мету не перемогу над ЄС та НАТО, як такими, а радше зменшення їхньої ролі та впливу, демонстрація неспроможності ЄС та НАТО захистити Європу¹.

В умовах ескалації агресії незалежно від стану оголошення війни, суверенітет та територіальна цілісність держави можуть підпасти під дію суспільно небезпечних подій, явищ та процесів, які, в тому числі, генеруються в економічній сфері та реалізуються економічними інструментами².

Одним із таких інструментів виявилось *вимушене збільшення країнами власних оборонних витрат*, а це мільярди доларів, які вилучаються з економік, незважаючи на об'єктивну необхідність державної підтримки економіки і охорони здоров'я, пов'язаних із пандемією COVID-19.

Необхідність нейтралізації загроз з боку Росії обумовила підвищення обсягів державних витрат на потреби безпеки і оборони як в

¹ Світова гібридна війна: український фронт: монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017. – 496 с.

² Економічні інструменти протидії гібридній агресії: аналіт. доп. / за ред. А. Ю. Сменковського. Київ: НІСД, 2020. 69 с.

Україні (видатки МОУ на 2021 р. становлять 116,2 млрд грн або 2,58 % ВВП), так і в країнах-членах НАТО (у останньому статистичному звіті НАТО, опублікованому напередодні саміту глав держав альянсу 14 червня 2021 р. в Брюсселі, сумарні оборонні витрати всіх 30 країн НАТО виростуть на 4,1% в 2021 році і складуть 1,049 трлн. дол. США).

Після подій 2014 року на Україні на саміті НАТО в Бухаресті було прийнято рішення, що до 2024-го всі країни доведуть свої оборонні витрати до 2% ВВП. Додаткове прискорення зростання військових асигнувань отримано в 2016-м після приходу в США до влади президента Д. Трампа. Виступаючи в грудні 2019 року на саміті організації в Лондоні, він запропонував, щоб члени альянсу не тільки виконували це зобов'язання (2% ВВП), але й збільшили ці витрати до 4% ВВП. Водночас, доведення бюджетів країн навіть до встановленого нормативу у 2% від ВВП країни зажадає десятків мільярдів дол., при тому, що у більшості країн внаслідок пандемії COVID-2019 економічні показники знизилися, що призвело до скорочення обсягів їх валового внутрішнього продукту.

Європейські члени НАТО з 2015 року послідовно збільшують військові бюджети - в 2020-м на 4,3% (у постійних цінах 2015 го). Найбільші темпи зростання військових витрат за останні шість років спостерігаються в країнах Балтії та Східної Європи, керівні органи яких неодноразово заявляли про загрозу безпеці з боку Російської Федерації: Литві (179,9%), Латвії (165,6%), Румунії (110,6%), Словаччини (100,5%), Угорщини (73,8%), Болгарії (62,7%), Чехії (61,5%), Естонії (39,9%).

Високу динаміку нарощування оборонних витрат з 2014 року також показують Туреччина – 52,9% і Канада – 43,8%. У той же час їх підвищення за цей період у Італії склало лише 16,9%, Греції – 12,9%, Бельгії – 11,8%, Франції – 11,1%, Великобританії – 9,7%.

Нарощування оборонних асигнувань тягне за собою зростання частки військових витрат на душу населення, які в середньому по країнах НАТО з 2015 року підвищилися на 10,8% – з 970 до 1087 дол. на людину. До числа країн-лідерів також відносяться Норвегія – 1444 дол., Великобританія – 1001, Данія – 793, Нідерланди – 656, Німеччина – 636 дол. (усереднений показник для Європи і Канади – 507 дол.).

Слід зазначити, що існують суперечливі думки щодо взаємозалежності величини оборонних витрат і економічним зростанням країн. До позитивного їх впливу на економічне зростання відносять: забезпечення мирного середовища для інвестиційної та виробничої діяльності, для внутрішніх та іноземних інвесторів; залучення ресурсів, зокрема населення, до науково-дослідної та дослідно-конструкторської

діяльності; одержання технічних навичок, навчальної підготовки то-що¹. Інші науковці довели існування негативного впливу збільшення оборонних витрат на економіку: можливе витіснення приватних інвестицій, негативний платіжний баланс та знищення капіталу (фізичного та людського)². Існують також дослідження, які доводять, що зв'язок між економічним зростанням та оборонними витратами мізерний³.

Досвід України, починаючи з 2014 року засвідчує значний приріст витрат на оборонну функцію держави в заміन видатків на розвиток економіки, соціальної інфраструктури, зростання оплати праці та інші заходи економічного розвитку країни, що підтверджує висновок, що примушування країни до значного збільшення своїх оборонних витрат можна розглядати як інструмент гібридної війни.

Козьма В. В.

доктор політичних наук, доцент,
Національний педагогічний університет
імені М.П. Драгоманова

ІНФОРМАЦІЙНА ЗБРОЯ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ЯК ЧИННИК СУЧАСНОЇ ГЕОПОЛІТИКИ

Проблема підтримки безпеки була актуальною протягом всієї світової історії. Це завдання є актуальним і в наші дні. Забезпечення на-

¹ *Ando S.* (2009). The impact of defense expenditure on economic growth: Panel data analysis based on the.

Feder Model. *International Journal of Economic Policy Studies*. Vol. 4(1). P. 141–154; *Benoit E.* (1978). Growth and defense in developing countries. *Economic Development and Cultural Change*. Vol. 26(2). P. 271–280.

² *Hou N., Chen B.* (2014). Military spending and economic growth in an augmented solow model: A panel data investigation for OECD countries. *Peace Economics, Peace Science and Public Policy*. Vol. 20(3). P.395–409;

Shahbaz M., Afza, T., Shabbir, M. S. (2013). Does defence spending impede economic growth? Cointegration and causality analysis for Pakistan. *Defence and Peace Economics* Vol. 24(2). P. 105–120.

³ *Huang C., Mintz A.* (1990). Ridge regression analysis of the defence-growth tradeoff in the United States.

Defence Economics. Vol. 2(1). P. 29–37. doi:10.1080/10430719008404676; *Mintz A., Stevenson, R. T.* (1995). Defense expenditures, economic growth, and the “peace dividend”: A longitudinal analysis of 103 countries. *Journal of Conflict Resolution*. Vol. 39(2). P. 283–305.

ціональної безпеки України є складним і багатовимірним процесом. Складність цього завдання зростає при розгляді його в нових геополітичних умовах. У сучасному світі наростають суперечності геополітичного характеру, посилюється конкуренція між країнами.

Інформаційний чинник відіграє дедалі більшу роль в політичних потрясіннях і конфліктах, що виникають в різних регіонах світу. Кризи в сучасному суспільстві різноманітні й можуть зачіпати всі без виключення сфери суспільного розвитку. Вступ сучасного суспільства в інформаційну фазу розвитку створив умови для виникнення суспільних криз, пов'язаних з інформаційною сферою життєдіяльності людей.

В політичних конфліктах все частіше використовуються сили й засоби інформаційного протиборства. На підставі цих процесів виникають кризи нового формату, які раніше, до настання епохи інформаційного суспільства, були просто неможливі. Слід зазначити, що інформаційно-політична криза – це суспільно-політичне явище, для якого характерні перенесення політичної боротьби в інформаційну сферу та використання в політичних конфліктах засобів інформаційного протиборства, що породжує виникнення серйозних негативних наслідків для національної безпеки держав.

Російська агресія проти України вплинула на переосмислення поняття національної безпеки не лише в середині нашої країни. Для багатьох, особливо пострадянських країн, стало очевидним, що міжнародно-правові методи не завжди дозволяють забезпечити національну безпеку суверенної держави й відвернути воєнне втручання ззовні. В цьому місці доречно буде нагадати деякі прописні істини, які з часом не втрачають своєї актуальності. «Чи вдалося людині, – пише Гюстав Лебон, – скасувати жорстокі стосовно неї закони природи, яким підпорядковані всі живі суспільства? Чи пом'якшила цивілізація хоч трохи відносини між народами? Чи стала боротьба серед людства менш гострою, ніж між різними видами? Історія показує нам протилежне. Вона каже, що народи перебували в постійній боротьбі й, що з початку світу, право сильного було завжди єдиним вершителем долі. Цей закон існував в стародавньому світі так само як і в сучасному. Ніщо не вказує на те, що він не буде існувати в майбутньому...».

Важливим напрямком впливу глобалізації на військово-політичну сферу світової спільноти й на процеси забезпечення міжнародної безпеки є військові конфлікти в сучасному світі. У локальних збройних конфліктах відбувається суттєва трансформація арсеналів ведення війни. У наші дні ці конфлікти набули нових особливостей. Тепер всі без виключення конфлікти, в якості важливої складової частини, ма-

ють в собі протиборство конфліктуючих сторін в інформаційному просторі. Таке протиборство стає одним з найважливіших напрямків протидії сторін одна одній при виникненні міжнародних конфліктів і часто переростає в інформаційну війну. За своєю суттю, інформаційна війна це форма цілеспрямованого силового інформаційного впливу на хід соціально-політичного розвитку країни відповідно до інтересів і цілей суб'єктів геополітичної конкуренції. Однак, попри те, що сьогодні відбувається трансформація характеру війни її природа залишається незмінною. Війна продовжує бути спрямованою на досягнення політичних цілей, хоча і не завжди ефективна в цьому. Одними військовими засобами неможливо досягти політичних цілей. Навіть сучасні високотехнологічні війни не завжди приводять до досягнення політичних цілей, адже факт залишається фактом, будь-які технології не в змозі виправити помилкові політичні рішення. Гармати – лише **Ultima ratio regum** (*Останній аргумент короля*).

Інформаційне протиборство відбувається в іншому просторі, ніж протиборство із застосуванням традиційних видів озброєнь. Це інформаційний простір, який відрізняється глобальним характером, практично необмеженою кількістю інформаційних ресурсів, можливістю їх копіювання і майже миттєвого переміщення на величезні відстані. Таким чином інформаційний вплив важко ідентифікувати й одразу ж відповісти на нього. У зв'язку з зазначеними особливими властивостями інформаційного простору в ньому застосовується й особливий вид зброї. Такі засоби як пропаганда, дезінформація, руйнування управлінських структур протиборчої сторони, застосовуються у війнах уже давно. Але поняття інформаційної зброї з'явилося лише у другій половині ХХ століття. Наскільки небезпечною зброєю може стати інформація, фахівці знають давно, однак пересічному громадянину або навіть не підготовленому в цій сфері політичному керівнику усвідомити таку загрозу складно. Тому сам термін «інформаційні війни» досить часто сприймається скептично. Помилково вважається, що для перемоги над супротивником достатньо лише сильної армії й нового озброєння. Але дозволимо собі нагадати ще одну прописну істину висловлену досвідченим політиком та державним діячем Отто фон Бісмарком: «Успіх у війні вирішують два фактори: зброя нового зразка і шкільний учитель» [3, с. 11]. Без сумніву, в наш час інформаційну зброю, у зв'язку з величезними масштабами її застосування і розміром шкоди який вона може заподіяти, слід відносити до зброї масового ураження.

Свідомий інформаційний вплив на супротивника, наявність необхідних даних, вміння їх обробляти й приймати на їх основі оперативні рішення завжди були важливими чинниками перемоги в міжнародних конфліктах. Однак якщо у війнах минулого недоліки тактичної інформації можна було компенсувати залученням додаткових сил, то сьогодні інформаційна перевага багато в чому зумовлює результат збройного протистояння. В умовах циркуляції інформації в режимі реального часу перевагу отримує та сторона, яка володіє найбільш розвиненою інформаційною інфраструктурою і здатна донести до світової спільноти відомості про конфлікт під вигідним для себе кутом зору.

В сучасних умовах інформаційна безпека розглядається як важлива складова системи забезпечення національної безпеки особистості, суспільства і держави. Вітчизняними фахівцями сформовані теоретичні основи цього питання, активно обговорюються загрози й небезпеки, які виникають в інформаційному просторі у зв'язку з російсько-українським військово-політичним конфліктом. Однак, роль і місце інформаційної безпеки в політичному житті суспільства і політичному курсі держави, направленому на захист національних інтересів, вимагає подальшого осмислення. Стає очевидним факт інтеграції політичної та інформаційної сфер суспільного життя. По-перше, постійно зростає роль інформаційного чинника в політиці. Традиційні друковані та електронні засоби масової інформації мають значний вплив як на масову політичну свідомість, так і на погляди політичних еліт. Таким чином ЗМІ безпосередньо впливають на прийняття важливих політичних рішень, на хід політичних процесів, на функціонування базових політичних інститутів тощо. По-друге, в останні роки стрімко зростає вплив Інтернету й зокрема соціальних мереж на політичний розвиток суспільств та народів.

Підсумовуючи зазначимо, що особливе значення для сталого функціонування політичної системи має безпека її інституційної складової. Основними небезпеками для політичної системи можуть бути навмисні або ненавмисні дії різних соціально-політичних суб'єктів (інших держав або будь-яких зовнішніх структур, партій, рухів, еліт, прошарків суспільства, соціальних груп, особистостей всередині країни), спрямовані на дестабілізацію політичної системи, підлив влади, політичного режиму. Таким чином, коли говоримо про політичну безпеку, необхідно під цим мати на увазі захищеність політичної системи від деструктивних і дестабілізуючих внутрішніх і зовнішніх впливів, що в свою чергу має сприяти проведенню такої політики, що

відповідає інтересам стабільного й стійкого розвитку країни, суспільства та громадян.

Події, пов'язані з українською політичною кризою 2013-2014 рр., наочно підтверджують наявність серйозних загроз національній безпеці нашої країни. У зв'язку з цим, сьогодні для України особливої актуальності набуває здатність органів державної влади забезпечувати суверенітет, цілісність і незалежність держави, проводити виважену внутрішню та зовнішню політику, виходячи з національних інтересів, активно й на рівноправних засадах брати участь в міжнародних відносинах виборюючи лідируючі позиції в регіональній геополітичній конкуренції.

Мельніченко О. А.

Департамент контррозвідувального захисту
інтересів держави у сфері інформаційної безпеки,
Служба безпеки України

ОСНОВНІ НАПРЯМКИ ДЕСТРУКТИВНОЇ ДІЯЛЬНОСТІ РОСІЙСЬКИХ СПЕЦСЛУЖБ В ІНФОРМАЦІЙНІЙ ВІЙНІ ПРОТИ УКРАЇНИ

Восьмий рік продовжується гібридна війна Російської Федерації проти нашої держави, у якій збройна агресія – це лише один з інструментів досягнення кінцевої мети країни-агресора – підкорення України, повернення її до сфери геополітичного впливу країни-агресора, зміна влади на «проросійську», стримування розвитку її відносин із західними військовими та політичними блоками (НАТО, ЄС тощо), примус відмовитись від намірів щодо деокупації АР Крим.

Російська гібридна агресія проти нашої держави ведеться одразу на кількох напрямках: воєнному, політичному, економічному, соціальному, гуманітарному та інформаційному. Але саме інформаційна агресія наразі становить одну з найбільших загроз суверенітету та незалежності України, оскільки пропаганда, що базується на брехні, маніпуляціях та підміні понять, заперечення самого факту війни та участі РФ у ній; звинувачення України у власних злочинах, спотворення української історії; кібератаки та спроби дестабілізувати критичну інфраструктуру – все це призводить до поступової трансформації українського суспільства та зміни самоідентичності української нації. Адже російські пропагандисти крок за кроком виробляли

ідеологічну платформу та створювали потужне підґрунтя для подальшої інформаційної агресії. Зазначене, зрештою, знайшло своє відображення у Стратегії національної безпеки РФ, введений в дію указом президента РФ 2 липня п.р., одним із головним напрямків подальших кроків РФ в інформаційному просторі якої вважається розширення впливу на світовому рівні, формування осередків лобіювання інтересів РФ у світі, пропагування російської ідеології, а засобами досягнення цієї мети є інформаційна агресія, метою якої є маніпулювання суспільною, груповою чи індивідуальною свідомістю українських громадян у вигідному РФ напрямку, створення важелів впливу на ухвалення рішень на державному рівні.

Суб'єктами проведення деструктивного інформаційного впливу проти України є оперативні підрозділи ФСБ РФ, підрозділи інформаційно-психологічних спеціальних операцій Головного розвідувального управління Генштабу Міністерства оборони РФ, підрозділ спеціальних заходів впливу Служби зовнішньої розвідки РФ.

Інструментами ж, за допомогою яких РФ здійснює свій деструктивний вплив на інформаційний простір, є інформаційні та психологічні операції, у ході яких здійснюється приховане впровадження підготовлених та вигідних країні-агресору наративів і меседжів з метою загальної дестабілізації ситуації, формування вигідної РФ громадської думки.

Тактичні цілі проведення Російською Федерацією інформаційних та психологічних операцій проти нашої держави умовно здійснюються за трьома основними напрямками:

- розраховані на громадян України (за винятком жителів ТОТ Донецької та Луганської областей), та направлені на формування у патріотично налаштованого прошарку населення відчуття зневіри та безперспективності «західного напрямку»; посилення у проросійськи налаштованого населення бажання відновити діалог з РФ на умовах Кремля; повернення окупованих РФ територій (за винятком Криму) до України на умовах Кремля; відмова України від повернення Криму; зміна діючої влади та політичної еліти на проросійську;

- розраховані на жителів ТОТ Донецької та Луганської областей і направлені на формування у населення цих територій відчуття неможливості повернення в Україну при прозахідному курсі; формування ненависті до діючої влади України; формування ненависті до НАТО, ЄС та Заходу в цілому; покладання провини за соціально-економічні проблеми на Україну; створення позитивного іміджу РФ та її керівництва; сприяння інтеграції окупованих територій у мов-

ний, інформаційний та культурний простір РФ; створення передумов для повернення до складу України після зміни влади на проросійську;

– розраховані на громадян ЄС, США і країн-паркетів України та направлені на формування іміджу України як «неспроможної держави»; створення антиукраїнського дискурсу в західних медіа; формування інформаційного тренду історичної приналежності України до «руського миру»; спонукання західних урядів до послаблення чи скасування антиросійських санкцій, пропагування проросійського світогляду; виведення проблеми окупації українських територій за межі суспільно-політичного порядку денного.

На противагу інформаційним операціям, психологічні розраховані на здійснення саме психологічного впливу як на людину зокрема з метою спонукання до певних дій, формування того чи іншого світогляду, зміни її психологічних характеристик (поглядів, думок, ціннісних орієнтацій, настроїв, установок, мотивів, стереотипів поведінки), так і суспільство загалом задля формування масових настроїв, суспільної свідомості в цілому.

Для організації та реалізації деструктивних інформаційних та психологічних операцій проти нашої держави в інформаційному просторі російськими спецслужбами все частіше використовуються можливості ІТ-гігантів (сервісів і платформ компанії «Google, LLC»), через технічні можливості яких здійснюється розповсюдження дезінформації з метою здійснення маніпулятивного впливу на користувачів українського сегменту Інтернет. Так, можливості Google Play та App Store використовуються РФ для поширення заборонених мобільних додатків компаній і організацій, стосовно яких запроваджено санкції. Через YouTube, Twitter, та Facebook здійснюється поширення інформаційного контенту російських та сепаратистських суб'єктів, які перебувають під санкціями. Через Google Maps здійснюється внесення змін в оригінальні назви державних установ України та дипломатичних представництв іноземних держав в нашій державі.

Наряду із вищезазначеним, країною-агресором для інформаційних операцій проти вищого військово-політичного керівництва держави, пропаганди сепаратизму, поширення деструктивної інформації тощо все частіше використовується месенджер Telegram. Цьому сприяє унеможливлення ідентифікації користувачів, що призводить до уникнення ними кримінальної відповідальності за поширення деструктивної інформації, а можливість анонімізації поширювачів деструктивну застосовується для створення та використання каналів зв'язку між радикальними та терористичними організаціями, їх чле-

нами, а також як засіб поширення сепаратистами, радикалами та терористами своїх вимог до широкого кола користувачів.

Таким чином, інформаційна агресія, як складова гібридної загрози з боку РФ проти нашої держави створює пряму загрозу суверенітету та територіальній цілісності України від країна-агресора. Тому окреслення основних напрямків деструктивної діяльності російських спецслужб у інформаційній війні проти України, визначення суб'єктів поширення негативного контенту щодо нашої держави, тактичних та стратегічних цілей РФ як стосовно України, так і на світовому рівні, дозволяє Службі безпеки України адекватно протидіяти реальним загрозам та прогнозувати потенційні.

Гладких Д. М.

доктор економічних наук, доцент,
Національний інститут стратегічних досліджень

ЗАБЕЗПЕЧЕННЯ ВАЛЮТНО-КУРСОВОЇ ТА ІНФЛЯЦІЙНОЇ СТАБІЛЬНОСТІ УКРАЇНИ В КОНТЕКСТІ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Аналіз динаміки розвитку економічних процесів у світі та в Україні, починаючи з кінця 2013 р., дає підстави стверджувати, що для досягнення тих чи інших політичних цілей різні держави все більш активно використовують інструменти не військового, а суто економічного характеру, що проявляються, зокрема, у застосуванні заходів санкційної політики, сценаріїв валютних війн, обмеженні фізичного доступу до транзитних шляхів тощо.

Одним із найбільш яскравих прикладів такої поведінки слід вважати рестрикційні заходи щодо України з боку Російської Федерації, які спрямовані, зокрема, на:

- обмеження доступу в країну валютної виручки шляхом впровадження торгівельних обмежень, створення перешкод на шляху експортно-імпортних потоків між Україною та іншими країнами (Китай, Казахстан, інші країни Азії);
- перетворення України на «логістичний тупік» шляхом будівництва дублюючих газопроводів «Турецький потік» та «Північний потік-2», Кримського мосту та нової залізничної гілки, що виключає транзит через Україну потягів між різними регіонами Росії;

- реалізацію політики імпортозаміщення, що поширюється не лише на суто військові компоненти (двигуни для гелікоптерів, турбіни для військових кораблів тощо), але й на широку номенклатуру абсолютно «мирних» товарів (продовольство, сировина і т. ін.).

Загалом це призводить до суттєвого скорочення валютних надходжень в Україну, що вкрай негативно впливає на курсову динаміку національної валюти, обсяг міжнародних резервів (які витрачаються на підтримку відносної стабільності курсу гривні), бюджетну безпеку держави (через скорочення податкових надходжень від експортерів), боргову стійкість країни (внаслідок необхідності нарощення внутрішнього та, особливо, зовнішнього боргу, що, у свою, чергу, також провокує подальше загострення ситуації на валютному ринку). Зокрема, загальна сума надходжень в країну від експорту товарів і послуг за 2020 р. склала лише 60,7 млрд дол. США, що на 26 % менше відповідного показника за 2013 р. (81,7 млрд дол. США) [1].

Українська економіка є відкритою експортоорієнтованою економікою, що значною мірою залежить від світової кон'юнктури та динаміки цін на сировину, особливо в частині енергоносіїв. Саме тому курсова складова інфляції в Україні є надзвичайно вагомою, а волатильна курсова динаміка гривні вкрай негативно впливає на внутрішню цінову стабільність.

Після досягнення у 2020 р. цільового показника у 5 % рівень інфляції в країні з початку 2021 р. демонструє негативну динаміку. Зокрема, у травні 2021 року споживча інфляція в річному вимірі прискорила до 9,5 % (з 8,4 % у квітні). У місячному вимірі ціни зросли на 1,3 % [2]. У межах боротьби з інфляцією НБУ був змушений піти на підвищення рівня облікової ставки до 7,5 % річних, що, очевидно, негативно вплине на вартість кредитних ресурсів та стане одним із чинників «охолодження» економіки.

У ситуації, що склалася, Україна має здійснювати наступні заходи, спрямовані на забезпечення валютно-курсowej та інфляційної стабільності як необхідної передумови успішного протистояння зовнішнім гібридним загрозам:

- послаблення імпортозалежності національної економіки з метою поліпшення стану торговельного балансу та посилення внутрішніх чинників реалізації національного економічного потенціалу. Значна імпортозалежність є перманентним девальваційним чинником та може спричинитися до імпорту інфляції, а також ускладнює доступ вітчизняних виробників до ресурсів внутрішніх ринків. Отже, вихід з цієї «пастки» вимагатиме запобігання недобросовісній конкуренції імпортерів (у т. ч. протидію контрабанді) на внутрішньому ринку,

сприяння доступу до внутрішніх ринків суб'єктів малого бізнесу, зниження енергоємності економіки (зважаючи на значну частку імпорту в енергетичному балансі), сприяння залученню вітчизняних компаній до участі у публічних закупівлях та інвестиційних проектах;

- поліпшення структури експорту. Переважання товарів з нижчою доданою вартістю в експорті та товарів з вищим рівнем переробки в імпорті закладає підґрунтя перманентного дефіциту зовнішньої торгівлі. Отже, потребує активізації підтримка експортної діяльності вітчизняних товаровиробників, виходу на зовнішні ринки нових учасників ЗЕД, освоєння нових зовнішніх ринків та розширення кола зовнішньоторговельних партнерів України;

- забезпечення відповідності обмінного курсу гривні параметрам, що закладені у Державний бюджет, шляхом недопущення неочікуваної ревальвації, що стимулює зростання імпорту, погіршує показники експорту, податкові та митні надходження;

- корекція режиму інфляційного таргетування через збільшення ваги немонетарних інструментів антиінфляційної політики та послабленні інфляційного потенціалу монетарних стимуляторів внаслідок удосконалення трансмісійних механізмів;

- посилення ролі облікової ставки як орієнтира для здешевлення кредитних ресурсів для реального сектору економіки, при збереженні її додатного рівня відносно прогнозованої базової інфляції, що має стимулювати депозитну активність вкладників та сприятиме зниженню девальваційних та інфляційних очікувань;

- диференціація норми резервування залучених коштів у національній валюті залежно від строковості банківських пасивів: нульова або мінімальна ставка резервування має застосовуватись тільки для довгострокових пасивів;

- запобігання зниженню конкуренції на ринку банківських послуг внаслідок їх надмірної концентрації, що потребуватиме проведення НБУ «антимонопольних» регуляцій, зокрема встановлення граничних значень процентів по кредитах і депозитах як відхилень від облікової ставки;

- сприяння зниженню попиту на готівку через поширення безготівкових форм отримання доходів, підвищення вартості отримання готівки, зниження граничної суми розрахунків готівкою;

- поетапне переведення всіх отримувачів пенсійних та інших соціальних виплат на безготівкову форму оплати шляхом оформлення платіжних карток у відділеннях одного з державних банків, що сприятиме зростанню банківських пасивів, активізації безготівкових розрахунків та зниженню частки тіньової економіки в країні;

– забезпечення збалансованої валютної структури банківських кредитів і депозитів за рахунок зниження доларизації кредитного та депозитного портфелів банківської системи до рівня, нижчого за 35 % у середньостроковій перспективі.

Література

1. Додаток до Макроекономічного та монетарного огляду, травень 2021 року [Електронний ресурс] – Режим доступу: <https://bank.gov.ua/ua/news/all/makroekonomichniy-ta-monetarniy-oglyad-traven-2021-roku>.
2. Коментар Національного банку щодо рівня інфляції у травні 2021 року [Електронний ресурс] – Режим доступу: <https://bank.gov.ua/ua/news/all/komentar-natsionalnogo-banku-schodo-rivnya-inflyatsiyi-v-travni-2021-roku>.

Закіров М. Б.

доктор політичних наук, доцент,
Служба інформаційно-аналітичного забезпечення,
Національна бібліотека України імені В. І. Вернадського

ВИКОРИСТАННЯ ГЛОБАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ У МОНІТОРИНГОВИХ МАТЕРІАЛАХ СІАЗ

Прискорення процесів глобалізації внаслідок розвитку цифрових інформаційних технологій зумовило виникнення глобального інформаційного простору. Цей простір розвивається під впливом удосконалення системи соціальних інформаційних комунікацій глобального значення і формує нову ієрархію міждержавних відносин, заснованих на відповідних рівнях розвитку інформаційної діяльності та інформаційних технологій. У цих умовах суттєво актуалізується проблема збереження балансу між ефективним використанням глобального знання і наступністю наукових, моральних і політико-культурних традицій розвитку суспільства. Розв'язання цієї проблеми сьогодні неможливе без наукового переосмислення ролі системи наявних вітчизняних інформаційних центрів, підвищення їх значення в наповненні сучасних інформаційних комунікацій суспільно значущою інформацією, задоволення запитів громадян і держави у доступі до неї¹.

¹ Горовий В. М. Національні інформаційні процеси в умовах глобалізації. Київ, 2015. 332 с.

Глобалізаційні процеси, що протікають у сучасному світі, потребують конструктивної взаємодії на всіх рівнях регуляції соціальних процесів. Розвиток подібної взаємодії сприяє прогресу соціуму, адже громадянське суспільство та інформаційна сфера взаємно доповнюються і в разі порушення цих зв'язків несуть втрати. Цей нерозривний зв'язок полягає в тому, що головна мета діяльності будь-яких інформаційних структур – це формування громадської думки, яка знаходить свій прояв у соціальній активності.

У даний час всі держави усвідомлюють, що поряд із розважальним потенціалом, глобальні інформаційні ресурси несуть в собі можливість для політичних маніпуляцій, і будь-яка група впливу або держава не обходить своєю увагою їхні потенційні можливості¹.

Задане інформатизацією прискорення суспільного розвитку обумовлює необхідність використання двох основних джерел інформаційного забезпечення: власного інфотворення, якісного введення в обіг вже наявних у розпорядженні суспільства об'ємів інформації, і обов'язкового використання необхідних для національного розвитку потенціалу глобальних інформаційних ресурсів. Роль глобальних інформаційних ресурсів суттєво зростає в умовах інформаційної війни як однієї з основних складових війни гібридної.

Сучасні розробники методів протидії негативному інформаційному впливу наголошують на складності і масштабності роботи, що потребує залучення значної кількості фахівців із різних сфер гуманітарного і технічного спрямування, об'єднаних у центр інформаційної боротьби. Серед основних завдань такого центру, дослідники виокремлюють наступні: моніторинг медіа-ресурсів на предмет наявності матеріалів, які містять згубний інформаційний вплив, викриття неправдивих інформаційних повідомлень, а також доведення результатів у доступній формі до населення; донесення до мешканців країни, яка чинить деструктивний інформаційний вплив, правдивої інформації та створення умов для критичного аналізу громадянами цієї країни відомостей з відповідних медіа тощо².

Прикладом використання інструментів інформаційно-психологічних впливів як інструменту гібридної війни можуть слу-

¹ Могилевская Г. И. Информационная война в социальных сетях [Електронний ресурс] Молодой ученый. Режим доступу: <https://moluch.ru/archive/95/21400/>.

² Носов В., Манжай О. Окремі аспекти протидії інформаційній війні в Україні. [Електронний ресурс]. Режим доступу: univd.edu.ua/scienceactivity/index.php?usid=192&fid=898.

жити маніпулятивні технології іноземних видань: створення інформаційної хвилі або певних асоціацій, анонімний авторитет, принцип контрасту, коментарі, постановка риторичних запитань, констатація факту, класифікатори, вибіркова правда, дезінформування тощо. Ці техніки були виявлені та проаналізовані в проекті «Україна у фокусі іноземних ЗМІ», що реалізовується Службою інформаційно-аналітичного забезпечення органів влади та Національною юридичною бібліотекою НБУВ¹.

Служба інформаційно-аналітичного забезпечення органів державної влади (СІАЗ) – структурний підрозділ Національної бібліотеки України імені В. І. Вернадського, що забезпечує інформаційну підтримку діяльності органів державної влади; науково-дослідна інституція, предметом спеціальної наукової уваги якої є дослідження електронних інформаційних технологій у бібліотечній сфері. Практична діяльність СІАЗ полягає у підготовці інформаційно-аналітичної та аналітико-прогностичної продукції на основі використання глобальних інформаційних ресурсів із відповідною верифікацією отриманої інформації за допомогою інформації, що міститься у фондах найбільшої наукової бібліотеки України.

Аналогічні інформаційно-аналітичні підрозділи працюють у багатьох великих зарубіжних бібліотеках. Зокрема: дослідницька служба Конгресу Бібліотеки Конгресу США, Бюро дослідницької та правової інформації Національної парламентської бібліотеки Японії, Довідковий відділ з права й ухвалення рішень Національної бібліотеки Китайської Народної Республіки тощо.

Серед замовників інформаційно-аналітичної продукції СІАЗ – управлінські структури загальнодержавного та регіонального рівнів, наукові установи, громадські організації, а також широке коло користувачів, що цікавляться питаннями суспільного управління.

Відповідно до запитів різних категорій замовників СІАЗ розробляє необхідну інформаційно-аналітичну продукцію, що включає огляди періодичні видання, бюлетені, дайджести тощо. Служба динамічно і оперативно реагує на еволюцію інформаційного поля і потреби користувачів. Повний архів видань СІАЗ зберігається на сторінці «Інформаційно-аналітичні проекти» сайту Центру досліджень соціальних комунікацій НБУВ.

¹ Національна юридична бібліотека НБУВ / Україна у фокусі іноземних ЗМІ [Електронний ресурс]. – Режим доступу: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2818:ukrajina-ufokusi-inozemnikh-zmi-lyutij-2017-r&catid=76&Itemid=387.

Основним періодичним виданням Служби є інформаційно-аналітичний журнал «Україна: події, факти, коментарі», зареєстрований як друковане видання у 2001 р. У журналі публікуються підготовлені фахівцями СІАЗ аналітичні матеріали, що відображають актуальні важливі події в житті України та навколо неї, оціночні та прогностичні матеріали, а також довідкова інформація, орієнтована на управлінські структури. Електронна версія журналу надсилається користувачам у регіони (в обласні, міські, регіональні адміністрації).

Останнім часом основні сили працівників Служби зосереджені на підготовці трьох збірників моніторингових матеріалів з використанням глобальних інформаційних ресурсів для вищих органів влади України:

1. Працівники відділу на основі аналізу інформаційного простору здійснюють підготовку моніторингових матеріалів з аналізом інформації Інтернет-видань про роботу державних органів влади та політичні і соціально-економічні події в Україні, США, Російській Федерації і країнах Європи. Зібрані у щотижневик «Суспільно-політичні події у відображенні електронних ЗМІ» дані компонуються згідно визначених рубрик, що містять анотації повідомлень, статті й аналітичні матеріали. У середньому кожний випуск містить до 450 повідомлень і повнотекстових матеріалів, підготовлених на основі аналізу понад 50 зарубіжних і українських Інтернет-видань. Усього підготовлено 74 випуски.

2. Щотижневик «Домінуючі теми суспільно-політичного характеру у відображенні електронних ЗМІ» містить результати кількісного аналізу повідомлень з української тематики на вітчизняних і зарубіжних Інтернет-ресурсах. Результати моніторингу представлені у таблиці, що містить рубрики: робота Уряду, ситуація навколо Криму, міжнародні події, діяльність Президента, робота Верховної Ради тощо. В окремих таблицях представлені кількісні показники домінуючих тем критичного характеру і домінуючих тем з української тематики в зарубіжних ЗМІ. Зміни у популярності певних повідомлень протягом тижня також представлені у щотижневику інфографікою, яка наочно демонструє динаміку суспільного інтересу і відображення тих чи інших подій світу у глобальних інформаційних мережах. У процесі підготовки щотижневика «Домінуючі теми суспільно-політичного характеру у відображенні електронних ЗМІ» в середньому обробляється понад 7000 повідомлень.

3. Аналіз електронних ЗМІ «Події. Персони: регіональний зріз». На основі щотижневого моніторингу понад 500 регіональних ЗМІ і Ін-

тернет-видань усіх регіонів України та окупованих територій проводиться систематизація матеріалів за рубриками, ідентифікація за тональністю (негативні, нейтральні, позитивні), результати зводяться до Google-таблиці та представлені в інфографіці. Таким чином, користувач отримує актуальну інформацію щодо топ-новин і топ-персон в окремих регіонах України на поточний тиждень. Усього під час підготовки щотижневика «Події. Персони: регіональний зріз» обробляється понад 25-30 тисяч повідомлень.

Отже, як показує досвід СІАЗ, за своїми масштабами ефективна робота з використання глобальних інформаційних ресурсів виходить далеко за межі індивідуальних можливостей і потребує долучення значних і добре організованих сил і засобів. У реалізації даних завдань наявні невикористані ресурси вітчизняної бібліотечної системи, українських ЗМІ, науково-інформаційних центрів. Однак, для їх продуктивного підключення до роботи по захисту інформаційного простору України видається за доцільне ввести в дану роботу практику державного замовлення.

Горовенко В. К.

Національний інститут стратегічних досліджень

ДЕЯКІ ФОРМИ І СПОСОБИ ЗАБЕЗПЕЧЕННЯ ОБОРОНИ ДЕРЖАВИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Гібридна війна стала нині одним з основних об'єктом наукових досліджень у сфері національної безпеки. Властивість і характеристика цього складного суспільно-політичного явища обумовили виведення згаданих досліджень далеко за рамки суто воєнної науки. Причина в тому, що гібридна війна за своїм змістом істотно відрізняється від класичної війни, в якій основним і вирішальним засобом була збройна боротьба.

Головна ознака гібридної війни – це поєднання широкого арсеналу воєнних і невоєнних засобів впливу, різноманітність форм і способів їх застосування.

Її концепція ґрунтується на особливостях сучасного періоду, якими є стрімкий розвиток технологій, особливо інформаційно-комунікаційних, наростання глобалізаційних процесів. В результаті держави сучасного світу стають більш зв'язаними між собою і взаємозалежними. За таких умов зростає їх вразливість від політичних, економічних та інших невоєнних засобів впливу.

Ми стаємо свідками того, що в сучасних міждержавних конфліктах все більше мають місце факти досягнення потрібних стратегічних і геополітичних результатів за допомогою широкого інструментарію невоєнних методів і засобів: явної та таємної дипломатії, економічного тиску, завойовування симпатій місцевого населення тощо.

Поряд з цим, не відійшла в минуле і практика реалізації багатьох положень теорії класичної війни, хоча в багатьох випадках в модифікованому виді. Серед них військова сила, яка залишається вагомим аргументом у міждержавних відносинах.

Одним з важливих результатів наукових досліджень особливостей гібридної війни, перш за все на прикладі російської агресії проти України, стало уведення в перелік документів планування у сфері оборони плану оборони. Його визначення дається, як відомо, в Законі «Про оборону України».

***Довідково.** Стаття 1 Закону України «Про оборону України»: «План оборони України – складова частина оборонного планування, що містить сукупність документів, які визначають зміст, обсяги, виконавців, порядок і строки здійснення політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту».*

Підготовлені зміни до згаданого Закону (реєстр. № 4210 від 12.10.2020), якими передбачається уточнити визначення плану оборони, мають однозначно віднести його до категорії документів планування оборони.

***Довідково.** План оборони України – сукупність документів, які визначають зміст, обсяги, виконавців, порядок і строки здійснення політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів щодо збройного захисту держави у разі збройної агресії або збройного конфлікту.*

Варто нагадати, що планування оборони – функція державного управління, яка передбачає планування дій, безпосередньо спрямованих на відбиття збройної агресії. На відміну від нього оборонне планування переважно зачіпає розвиток сил оборони та інших оборонних ресурсів.

Судячи зі структури плану оборони, затвердженої Указом Президента України від 3 березня 2020 року № 61, він різниться за своїм змістом від визначеного законом. План оборони за нинішньою його

структурою обмежується плануванням заходів невоєнних засобів протидії агресії та реалізації правоохоронних функцій забезпечення оборони держави. Воєнні заходи щодо збройного захисту держави залишаються предметом Стратегічного плану застосування Збройних Сил України та інших складових сил оборони. Ці два документи планування оборони взаємопов'язані та взаємоузгоджені між собою, але все ж окремі. Зведення їх в єдиний документ, як це передбачено законом, потребуватиме певного часу і відповідної роботи. Для цього потребують невідкладного вирішення наступні питання.

По-перше. Подальша розробка теорії форм і способів застосування невоєнних засобів боротьби, особливо політичних і економічних, з урахуванням досвіду західних держав та потенційних можливостей України.

По-друге. Опрацювання теорії спільних операцій із застосуванням воєнних і невоєнних засобів, з реалізацією в них форм і способів інтегрування їх спроможностей.

По-третє. Впровадження системи управління обороною держави, яка б дозволила реалізувати оптимальне поєднання централізації і децентралізації управління усім комплексом воєнних і невоєнних засобів боротьби.

Однією із характерних ознак гібридної війни, методи якої преважують в російській агресії проти України, є стимулювання виникнення в державі, обраній для агресії, внутрішнього збройного конфлікту. Для цього держава-агресор здійснює політичну та інформаційну підтримку сепаратизму, фінансує та матеріально забезпечує створення незаконних збройних формувань. В якості організаційного ядра при створенні таких формувань виступають, як правило, диверсійні групи агресора, що нібито складаються з добровольців. Однією з таких груп, яка проявила себе на сході України весною 2014 року була група, очолювана офіцером ФСБ Росії Гіркіним (Стрелковим).

У подальшому, за безпосередньою участю країни-агресора і під керівництвом її державних органів і посадових осіб, створюються військові формування, які відіграють основну роль військового інструмента агресії.

При таких методах гібридної війни країна-агресор намагається залишатися публічно непричетною до розв'язаного воєнного конфлікту. Однак, де-факто, за своїм змістом він є особливою формою агресії. У випадку подальшої ескалації Росією агресії проти України, можна очікувати в її діях інспірування збройного конфлікту в інших регіонах нашої держави.

У Стратегії воєнної безпеки України, затвердженій Указом Президента України від 25 березня 2021 року № 121, одним із ймовірних сценаріїв, які потребуватимуть застосування сил безпеки і сил оборони України для виконання завдань з оборони України, визначено: «спровокований та підтриманий ззовні збройний конфлікт у межах території України, що може супроводжуватися масованим застосуванням засобів збройного насильства, незаконних збройних формувань (приватних військових кампаній), міжнаціональною, міжконфесійною або соціально-політичною нестабільністю». Ймовірність виникнення такого сценарію обумовлює необхідність створення в Україні цілісної системи реагування на такі збройні конфлікти, в рамках якої реалізується комплекс політичних, економічних, соціальних, правових, інформаційних, воєнних та інших заходів держави щодо запобігання їм, ліквідації у разі їх виникнення та стабілізації ситуації у постконфліктний період. Ці питання різнобічні і достатньо складні.

Одним із можливих елементів такої системи може бути превентивна операція. Вона має розпочинатися вже на етапі активізації акцій безпосереднього протесту (мітингів, демонстрацій, регіональних страйків), коли переговори з протестуючими і певні правоохоронні заходи не дали бажаного результату в урегулюванні конфлікту. Операція спрямовується на попередження агресивних проявів у діях протестуючих, які провокуються агентами впливу - масових безпорядків, блокування або захоплення окремих будівель органів державної влади і місцевого самоврядування тощо. І, безумовно, попередження переростання конфлікту у збройне протистояння.

З огляду на мету і зміст превентивної операції вона повинна включати в себе дві компоненти - несилову (гуманітарну) і силову.

Несилова компонента (центральні та місцеві органи виконавчої влади) реалізує заходи політичного, економічного, соціального та інформаційного характеру, які спрямовані на вирішення проблем, що експлуатувалися агентами впливу при провокуванні масових виступів. Це має розкрити суспільству агресивну мету їх діяльності і таким чином позбавити підтримки з боку населення.

Силова компонента (органи управління військовими формуваннями, спеціальними, розвідувальними та правоохоронними органами) у першу чергу спрямована на позбавлення агресора оперативних та ресурсних можливостей розпочати збройний конфлікт у певному регіоні України. Це реалізується шляхом здійснення оперативно-розшукової діяльності, проведення комплексу оперативних і режимних заходів, а також інших заходів правоохоронного та окремих заходів військового характеру. Такими заходами, зокрема, можуть бути:

виявлення та затримання осіб, які підозрюються в організації масових безпорядків, створенні терористичних груп (організацій) і незаконних воєнізованих або збройних формувань;

виявлення та ліквідація тайників зброї, боєприпасів та вибухових речовин, а також баз підготовки членів воєнізованих або збройних формувань;

посилення охорони військових складів та інших місць зберігання зброї, боєприпасів і вибухових речовин, особливо важливих державних об'єктів;

перекриття каналів фінансування, постачання зброї, боєприпасів, військового спорядження та продовольства, яке може бути використано для забезпечення незаконних збройних формувань, а також прибуття на територію України іноземних військових спеціалістів, агентів спецслужб та найманців;

виявлення та ліквідація розвідувальної мережі російських спецслужб.

Отже, розробка теорії проведення превентивної операції та підготовка до її проведення – найактуальніші завдання забезпечення оборони України.

Горова С. В.

доктор наук із соціальних комунікацій, доцент,
Національна бібліотека України імені В. І. Вернадського

ЕТНОНАЦІОНАЛЬНА ПРОБЛЕМАТИКА ІНФОРМАЦІЙНОЇ ВІЙНИ

Не зважаючи на зростаючу внутрішню організаційність російської пропаганди, її аргументація в інформаційній війні проти України базується на спрощених уявленнях, що значно знижують ефективність її впливу і на українських громадян, і на населення власної країни, і на глобальний інформаційний простір в цілому. В Україні вона розрізняє, власне, два види об'єктів свого впливу: за мовною ознакою - російськомовне населення, що за уявленням російських політтехнологів становить історично вмотивовану переважну більшість на території нинішньої української держави, й інше населення, що ґрунтується навколо галицького етносу і знаходиться при владі в нинішній українській державі. Такі спрощенні уявлення, звичайно, значно

полегшують російським політтехнологам організацію пропагандистської діяльності, однак при цьому, не співпадаючи з реаліями суспільного життя, зменшують дієвість інформаційних впливів.

Насамперед, при цьому, йдеться про педалювання мовного питання: насильницьку українізацію в країні, утиски російській мові і культурі, ставлення до російськомовного населення як до громадян другого сорту. Даний посил російської пропаганди знаходить відгук лише у частини аудиторії, оскільки сучасна українська мова побутувала на території нашої країни протягом тривалого історичного періоду, літературно була високо розвинутою, поряд із російською мовою загальносоюзного спілкування широко використовувалась як державна і в управлінській діяльності, і у науці, освіті, культурі і побуті. Її розуміла, знала переважна частина населення, за виключенням хіба що вузької частини національно стурбованих російських націоналістів.

Російські політтехнологи спрощено підходять і до теоретичного обґрунтування історичних аспектів освоєння територій сучасної України пращурами нинішніх її громадян, і до цивілізаторської місії Росії на території бувшої союзної держави, і до її ролі в Другій Світовій війні, і до всього іншого комплексу проблем суспільного розвитку. Підкреслено велекороський підхід до всієї проблематики україно-російських відносин взамін спокійному, науково обґрунтованому підходу до об'єктивного аналізу міжнаціональних взаємин.

У наших роботах раніше вже підкреслювалась специфіка розвитку глобалізованого інформаційного суспільства, пов'язана з активізацією національних процесів в багатонаціональних державах, і, тим більше, оживленню етнічних факторів у національному вимірі. Це обумовлено розвитком на базі електронних інформаційних технологій системи соціальних інформаційних комунікацій, що забезпечують інформаційний розвиток не лише націй, але й етносів. Більше того, якщо національний розвиток зав'язаний на територіальну ознаку, то ментальні особливості етносів є глобальними ознаками історичної приналежності до певних спільнот людей на психобіологічному рівні. Цей рівень в індустріальному суспільстві старанно камуфлювався національними ознаками і лише у сучасному, інформаційному суспільстві одержав інформаційну підтримку для свого прояву на новому рівні. Більше того, на сучасній інформаційній базі, як це сьогодні спостерігається, він став опорою активізації національних меншостей в багатонаціональних країнах.

Прояв даної закономірності сучасності покищо повною мірою не враховується російською пропагандою і в інформаційній війні з Україною, і в розробці сучасної національної політики РФ. У навколоукраїнському контексті покищо дана ситуація консервується Мінськими домовленостями, що, фактично, ігнорують основні інтереси учасників конфлікту і не можуть бути реалізовані без повної капітуляції однієї із сторін-підписантів. Більш вразливою ситуація може стати, якщо російські політтехнологи звернуться до пропаганди досвіду міжнаціональної співдружності, історичних традицій успішного будівництва спільної держави для багатьох націй і етносів на російських орієнтирах розвитку. На сьогодні ці орієнтири дуже не виразні, на політичну активізацію накладається проблема ковіду і пов'язанні з нею прояви економічної, обумовленої її розвитком кризи. Однак, посилення етнонаціональної турбулентності, викликане стрімкою активізацією глобальної інформатизації, обумовлює необхідність пошуку і оперативного впровадження якісно нових механізмів міжнаціонального, етнонаціонального співробітництва, що значною мірою обумовлюватиме суспільний прогрес.

Дана обставина обумовить пошук ефективних рішень і в організації російсько-української інформаційної війни. У зв'язку з цим, можна прогнозувати «подолання болісної нерішучості російського керівництва», за виразом відомої російської журналістки Маргарити Симонян, більш диференційованого підходу до населення України в пропагандистських впливах. Крім розширення підтримки збройних угруповань ОРДЛО (в контексті резонансного призову тієї ж М. Симонян «Росія – матушка, верни нас обратно») російські політтехнологи можуть звернути увагу на етнонаціональну специфіку світогляду східноукраїнської частини громадян. Ця частина населення чисельно більша від західноукраїнського національного активу, не захоплена національним радикалізмом і може бути більш вразливою до російської пропаганди, ніж населення західних областей. Вони можуть також звернути увагу на наявність на російській території, за різними підрахунками, близько 3 млн. українських заробітчан і розробити обґрунтування для їх активізації в політичному житті України. Від них можна очікувати вироблення прийнятних орієнтирів майбутнього для середнього класу українського суспільства. Ця, найбільш суспільно активна частина громадян значною мірою підтримувала Майдан, сподіваючись, що заміна Януковича змінить політику утисків і обмежень для середнього класу – стабілізаційної сили демократичних пе-

ретворень. Однак, пізніше вона зіткнулися з новими економічними й іншими проблемами, втратила надію на можливості підтримки своїх інтересів і може бути благодатним полем для зовнішньої пропаганди.

Реальність таких передбачень досить вірогідна, оскільки опирається на прояв сучасних закономірностей розвитку глобального суспільства. Дії на упередження, при цьому, можуть, значною мірою, ослабити негативні інформаційні впливи з за кордону. Крім активізації вже розроблених і впроваджуваних заходів протистояння агресивним діям противника в гібридній війні видається за доцільне розвиток культурологічних заходів, що мають емоційний вплив на ментальну сферу українців. При цьому, видається важливим:

- стимулювання вітчизняної гуманітарної науки в аналізі якісно нової суспільної ситуації, пов'язаної з розвитком глобальної інформатизації. Визначення і обґрунтування місця України в сучасній системі ціннісних орієнтирів. Вироблення в нових реаліях міжнародного співробітництва чітких орієнтирів національного розвитку в сучасних умовах і організація роз'яснення їх змісту серед всіх категорій громадян;

- на базі сучасних духовно-ціннісних орієнтирів, пропаганди суспільних духовних традицій українського народу вироблення системи святково-обрядових урочистостей, що мають відображати суспільне значення всіх важливих подій у житті громадян, формувати суспільну єдність і приналежність до спільної духовно-цілісної основи національного розвитку;

- розвиток контактів із національно-культурними організаціями та налагодження інформування етнічних українців в місцях соціального проживання (Новосибірський регіон, Тюменський ареал та ін.) про можливі позитивні зрушення в реалізації планів українського керівництва;

- вивчення культурологічних запитів етнічних українців за кордоном (в тому числі: розсіяної еміграції), організація їх задоволення і інформування про це.

Зважаючи на важливість розробки даної проблематики, видається за необхідне підтримка її розвитку державними замовленнями.

Куровська І. А.
кандидат юридичних наук,
старший науковий співробітник,
Інститут законодавства Верховної Ради України

РЕАЛІЗАЦІЯ ПРИНЦИПУ ВЕРХОВЕНСТВА ПРАВА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Доктрина верховенства права на тлі недосконалості системи міжнародної безпеки та завдання шкоди державному суверенітету й територіальній цілісності України, в умовах загострення геополітичного протистояння в новітню епоху гібридних війн набула особливого значення. Її реалізація необхідна для: підтримки міжнародного та національного правопорядку країн світової спільноти; удосконалення правового регулювання конституційно-правових основ державної безпеки України (далі – ДБУ) як складової національної безпеки України (далі – НБУ); реформування вітчизняного сектору безпеки в контексті пріоритетності неухильного дотримання прав і свобод людини й громадянина.

Верховенство права в онтологічному його розумінні стосується виконання владних повноважень і взаємовідносин між особою та державою. Однак останніми роками, завдячуючи глобалізації та дерегуляції, з'явилися нові міжнародні й транснаціональні гравці, а також гібридні та приватні гравці (ТНК, НУО, політичні партії, антиглобалісти, соціальні мережі тощо), що мають велику владу над урядами держав і пересічними громадянами. Верховенство права повинно стримувати дії таких органів і традиції можновладців на державному рівні.

Захист оборонного потенціалу України, законних потреб держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру й безпеки людства все ж тісно пов'язаний із протидією загрозам воєнного характеру. Так, засвідчуючи зазначене, В. Горovenko, А. Місюра, С. Кошовий стверджують, що саме на спеціальні служби РФ покладено завдання із планування, організації та реалізації комплексу заходів щодо створення необхідних умов у країні – об'єкті агресії на підготовчому «передвоєнному» етапі. На їхнє переконання, провідною залишається їхня роль і впродовж активної фази гібридної війни. Погоджуємось із тим, що для країни-агресора особливого значення набуває своєчасне

отримання актуальної розвідувальної інформації щодо обставин у країні – об’єкти агресії, стану справ у сфері НБУ, боєздатності силових структур¹.

О. Резніков, В. Тютюнник, В. Цюкало, зі свого боку, пропонують готувати силову відповідь агресору через формування нової якості СБОУ. Вони наполягають на необхідності суттєвих зрушень у безпечовому елементі цього сектору. Окреслюючи участь у відсічі воєнних загроз СБУ, зазначені науковці констатують, що для приведення діяльності спецслужби у відповідність до реалій оперативних обставин та підвищення ефективності протидії новим загрозам вжито низку організаційних заходів, зокрема:

- проведено роботу з удосконалення правового забезпечення діяльності в умовах військової агресії РФ;
- значна частина співробітників набула досвіду проведення оперативно-розшукових та контррозвідувальних заходів у зоні ведення бойових дій, в умовах активної діяльності диверсійно-розвідувальних груп противника;
- посилено контррозвідувальний режим;
- запроваджено систему військово-цивільних адміністрацій як тимчасових державних органів, які діють на території Донецької та Луганської областей у складі Антитерористичного центру при СБУ².

Цим згадані експерти фактично вказали на широке поле діяльності СБУ як суб’єкта забезпечення ДБУ, що охоплює, зокрема, протидію воєнним загрозам.

Зауважимо, що поєднання воєнного та антитерористичного компоненту в спектрі організаційних заходів СБУ невинноватиме, адже гібридна війна РФ проти України здійснює узгоджений, гнучкий та динамічний вплив через комплекс сучасних військових, терористичних, інформаційних методів тощо, а також через ненормативні інноваційні підривні технології державного перевороту в умовах штучно створеної політичної нестабільності на основні елементи системи національної безпеки країни-жертви³. Отже, протидія тероризму теж пов’язана із припиненням військових загроз.

¹ Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. К.: НІСД, 2017. С. 270-276.

² Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. К.: НІСД, 2017. С. 312-321.

³ Гибридная война: Российская Федерация против стран Балтии : обзорное издание / сост. С.Л. Фальченко, В.Н. Гребенюк. 2-е изд., пер. с укр. Киев : НА СБУ, 2020. 168 с.

Відповідно до цього контексту, постанова ВРУ «Про рекомендації парламентських слухань на тему: «Обороздатність України в ХХІ столітті: виклики, загрози та засоби їхнього подолання» від 12.08.2014 р. № 1639 визнала входження нашої держави в нову епоху неklasичних, гібридних воєн, які водночас є основною формою реалізації воєнно-політичних інтересів РФ щодо України¹.

Основною формою гібридної війни проти України Концепція розвитку Сектор безпеки й оборони України, затверджена Указом Президента України від 14.03.2016 р. № 92/2016, визначає комбінацію різноманітних і динамічних дій регулярних сил РФ, що взаємодіють зі злочинними озброєними угрупованнями та кримінальними елементами, діяльність яких координується та здійснюється за єдиним замислом і планом з активним застосуванням засобів пропаганди, саботажу, навмисного завдання шкоди, диверсій і терору².

На сьогодні загрозу російської воєнної агресії визнають не лише українські законотворці та вчені.

Так, британські експерти Chatham House в аналітичному звіті «Російський виклик» (The Russian Challenge) від 04.06.2015 р. метою російської геостратегії визначили відновлення ексклюзивного впливу Росії на пострадянському просторі. Політику умиротворення назвали неефективною та запропонували заходи протидії, з-поміж яких: відновлення механізмів стримування, дослідження процесів у РФ, вироблення об'єктивних прогнозів їхнього розвитку, підготовка до будь-яких змін російського політичного режиму³.

Фахівці НАТО в концепції НАТО «NATO's Bi-Strategic Command Capstone Concept» теж визнали факт існування «гібридних загроз», назвавши його реальністю сьогодення⁴.

¹ Про Рекомендації парламентських слухань на тему: «Обороздатність України у ХХІ столітті: виклики, загрози та шляхи їх подолання» // Постанова Верховної Ради України від 12.08.2014 р. № 1639-VII. URL: <https://zakon.rada.gov.ua/laws/show/1639-18#Text>.

² Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» // Указ Президента України від 14.03.2016 р. № 92/2016. URL: <https://zakon.rada.gov.ua/laws/show/92/2016#Text>.

³ The Russian Challenge. Keir Giles, Philip Hanson, Roderic Lyne, James Nixey, James Sherr and Andrew Wood. London, The Royal Institute of International Affairs. 2015. 58 p. P. 11-36.

⁴ Гибридные войны в стратегии США и НАТО. URL: <https://topwar.ru/60101-gibridnye-voyny-v-strategii-ssha-i-nato.html>.

Наголосимо, що Україна перебуває в авангарді відбиття загроз воєнного характеру євроатлантичній стабільності, організаційною формою чого стали антитерористична операція та операція об'єднаних сил. Тому демілітаризація суб'єктів сектору безпеки визнана не виправданою. Її реалізація буде можлива лише після припинення війни (конфлікту), зникнення потреби у військовому компоненті спеціальних служб.

Ковальчук І. М.

кандидат економічних наук, доцент,
Головне управління контррозвідувального захисту
інтересів держави у сфері економічної безпеки,
Служба безпеки України

**ЩОДО ПИТАНЬ ПРОТИДІЇ
СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ
ЕКОНОМІЧНОМУ ТЕРОРИЗМУ ЯК ЗАГРОЗІ
СТАБІЛЬНОМУ ФУНКЦІОНУВАННЮ
КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ
В УМОВАХ ГІБРИДНОЇ ВІЙНИ**

На сьогодні Служба безпеки України спільно з іншими заінтересованими державними органами бере активну участь у створенні засад державної системи захисту критичної інфраструктури, опрацюванні механізмів налагодження дієвої взаємодії між усіма її суб'єктами для протистояння новітнім викликам і загрозам гібридного типу.

Проведена попередня робота сприяла ухваленню 2017 року резолюції Ради Безпеки ООН S/RES/2341 про захист критичної інфраструктури від терористичних атак, схваленню Кабінетом Міністрів України Концепції створення державної системи захисту критичної інфраструктури від 06.12.2017 № 1009-р та закріпленню за СБУ завдання із контррозвідувального захисту об'єктів критичної інфраструктури (ст. 19 Закону України «Про національну безпеку України»).

Спільно з іншими державними органами взято участь у розробці законопроектів «Про критичну інфраструктуру та її захист², які вже надавались до Верховної Ради України (від 27.05.2019 № 10328) та на сьогодні пройшли перше читання (від 09.03.2021 № 5219).

Водночас у складній безпековій ситуації для ефективного протистояння новітнім викликам і загрозам гібридного типу залишається невирішеним нормативне врегулювання питання забезпечення стійкого функціонування об'єктів критичної інфраструктури, їх надійного захисту від різних видів небезпек, у т. ч. терористичного характеру.

Зокрема, Служба безпеки України в ході контррозвідувального забезпечення об'єктів критичної інфраструктури постійно зіштовхується з різноманітними проявами тероризму: міжнародним, релігійним, інформаційним, технологічним та економічним.

Проте сьогодні терористичні прояви не обмежуються лише класичними формами. Під виглядом зовні незагрозливих дій реалізуються багатоходові комбінації, які можуть нести загрози вітчизняній критичній інфраструктурі, призводити до знищення або блокування діяльності таких об'єктів, зміни економічного курсу країни, формування передумов до втрати ознак державності, інспірування в Україні внутрішніх протиріч та конфліктів тощо.

Для реалізації цих задумів використовується комплекс підливних, технологічних, економічних, соціальних, дипломатичних, політичних, кібернетичних та інформаційних важелів впливу.

Специфіка такого поєднання полягає в тому, що кожний із військових і невійськових способів ведення гібридного конфлікту може використовуватись на шкоду національним інтересам.

Разом із тим чинні нормативно-правові акти у сфері боротьби з тероризмом свідчать про відсутність у законодавстві України такого поняття, як «економічний тероризм», хоча в умовах посилення загроз гібридного типу зазначена небезпека, на нашу думку, є домінантною.

Закон України «Про боротьбу з тероризмом» містить поняття «тероризм», під яким слід розуміти суспільно небезпечне діяння, що полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, катувань, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози скоєння протиправних дій з метою досягнення злочинних цілей.

На думку наукової спільноти, економічний тероризм є різновидом суспільно небезпечної діяльності, спрямованої на дестабілізацію та (або) завдання іншої шкоди економіці з метою примушування органів публічної влади, міжнародних організацій, юридичних чи фізичних осіб учинити певні дії або утриматися від їх учинення всупереч національним інтересам у сфері державної безпеки.

Підґрунтям економічного тероризму є різноманітні скоординовані дестабілізуючі дії для ослаблення економічної безпеки чи фінансової стабільності держави. На відміну від диверсії, прояви якої охоплюють руйнування або пошкодження об'єктів народногосподарського чи оборонного значення (ст. 113 КК України), діяння економічного тероризму (на відміну від класичного тероризму) не завжди є насильницькими, а їх наслідки можуть бути віддалені в часі.

Прикладами таких дій є запровадження економічних санкцій, ембарго, створення неконкурентних умов для окремих категорій суб'єктів господарювання (обмеження участі у процедурах закупівель, надання дотацій тощо), створення штучних перепон функціонуванню морських торговельних портів (як приклад можна навести фактичне блокування РФ під приводом воєнних навчань перевалки вантажів з портів Маріуполя та Бердянська) чи інших об'єктів критичної інфраструктури, лобіювання питань будівництва продуктопроводів та міжнародних транспортних коридорів в обхід України, «інвестування» в Україну капіталів сумнівного походження тощо, що зумовлює необхідність ужиття додаткових заходів забезпечення економічної безпеки. Кінцевою метою економічного тероризму є зміна економічних відносин суспільства, перерозподіл власності та обраного курсу країни.

Під «економічним тероризмом» як доктринальним поняттям теорії економічної безпеки науковці розуміють:

- 1) різновид форми суспільно небезпечного діяння, яким є «тероризм»;
- 2) форму деструктивного економічного впливу на особистість, суспільство і державу;
- 3) небезпечні діяння з інформаційного впливу на окремі групи осіб, у тому числі й на тих, хто приймає управлінські рішення, пов'язані з викривленням об'єктивної інформації, що спричиняє виникнення економічних кризових ситуацій у державі, нагнітання страху і напруженості в суспільстві;
- 4) новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу об'єктів критичної інфраструктури держави або її елементів, а також на протиправне використання економічної інфраструктури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особи, суспільства і держави;
- 5) множину економічних війн та спецоперацій, у тому числі пов'язаних із спецслужбами іноземних держав;

б) намагання вплинути на економічну сферу з боку національних або транснаціональних кримінальних структур;

7) ідеологічно обґрунтовану практику впливу, спрямованого на залякування населення, на прийняття рішення або вчинення дії (бездіяльність) органом влади, органом місцевого самоврядування, міжнародною організацією, соціальною групою, юридичною особою або фізичною особою в межах національної економіки або економічного простору.

На нашу думку, «економічний тероризм» як термін потребує додаткового доктринального опрацювання і доповнення. Зокрема, вважаємо, що в ньому, крім уже відомих, мають бути враховані ще такі складові:

- економічна експансія, що проводиться з метою набуття домінуючого становища, створення важелів впливу й лобі в державних органах влади для подальшого зниження рівня економічної протидії загрозам;

- соціальні чинники (передумови і причини, що призвели до поглиблення і настання кризових явищ в економіці держави, інспірування акцій громадської непокори, спричинення хаосу і паніки, виникнення джерел підбурювання певних верств населення [професій] до вчинення протиправних діянь [саботаж і шкідництво]), що в сукупності порушують усталене й безпечне функціонування національної економіки;

- корпоративні чи завчасно узгоджені за попередньою змовою дії окремих суб'єктів господарювання, прояви недобросовісної конкуренції, що спричиняє і поглиблює деструктивні економічні процеси в державі;

- економічне шпигунство як підґрунтя для вчинення акту економічного тероризму;

- релігійний фактор, що може стати важелем впливу на економічну ситуацію в державі й унаслідок реалізації якого може кардинально змінитися економічний курс країни;

- створення в Україні економічних бар'єрів та перешкод для виходу на світові ринки збуту, запровадження заборон на здійснення окремих експортно-імпортних операцій;

- розхитування і дестабілізація міжнародних фінансових та економічних відносин України з іншими державами;

- протиправний перерозподіл власності та доходів шляхом створення атмосфери страху за допомогою насильства і злочинів проти людини та руйнації сфер її життєзабезпечення.

Оскільки економічний тероризм є загрозою, що завдає шкоди стабільному і штатному функціонуванню державних або міжнародних економічних систем чи фінансових об'єктів, посягає на економіку держави або групи держав і супроводжується похідними суспільно небезпечними діями для досягнення певної мети, то його можна класифікувати як кримінально каране діяння. При цьому економічний тероризм доцільно класифікувати як окремий вид тероризму.

У контексті реформування сектору безпеки, з огляду на суттєві зміни в розвитку ситуації (агресія РФ, поширення вітчизняного та міжнародного тероризму та ін.), визначення нового зовнішньополітичного вектора України (вступ до ЄС та НАТО), відсутність визначення терміну «економічний тероризм» в українському законодавстві та, як наслідок, відповідальності за його вчинення, існують передумови до зниження ефективності реагування на загрози, спричинені економічним тероризмом.

З урахуванням стратегічних цілей державної політики у сфері захисту державної безпеки України, а також об'єктів критичної інфраструктури, з метою наближення діяльності вітчизняної спецслужби до європейських і світових стандартів актуальним постає питання щодо створення чітких правових підстав для протидії Службою безпеки України загрозі економічного тероризму.

Шемаєв В. М.

доктор військових наук, професор,
Національний інститут стратегічних досліджень

Толок П. О.

кандидат економічних наук,
Заслужений економіст України,
Центральний науково-дослідний інститут
озброєння та військової техніки Збройних Сил України

СТВОРЕННЯ АГЕНСТВА З РОЗВИТКУ ОБОРОННИХ ТЕХНОЛОГІЙ – ОСНОВА АСИМЕТРИЧНИХ МОЖЛИВОСТЕЙ УКРАЇНИ У ГІБРИДНІЙ ВІЙНІ

Сучасний світ характеризується надзвичайно динамічними змінами, коли відбувається швидке впровадження в практику життя новітніх досягнень науки, що стають вирішальним чинником впливу на світові та регіональні геополітичні ландшафти. Внаслідок створення

та розповсюдження нових технологій створюються нові ризики, що вимагають механізмів реагування. Для ефективного протистояння сучасним викликам в умовах обмежених ресурсів для симетричного протистояння сучасним викликам її незалежності, Україна вимушена демонструвати більшу гнучкість, бути більш інноваційною та технологічно стійкою¹. Новітні технології, при цьому, можуть стати основою формування асиметричного потенціалу протидії агресору.

В сучасних умовах російський військовий потенціал за кількісними і якісними показниками значно перевищує відповідні показники України. До того ж, розрив у їх якісних параметрах має тенденцію до зростання: в останні роки Росія прискорено оновлює арсенал звичайних засобів збройної боротьби. Так, за останні роки загальна оснащеність російських збройних сил сучасними зразками озброєння і військової техніки (ОВТ) зросла до 61 % (у сухопутних військах – 48,3 %, у повітряно-космічних силах – 74 %, у військово-морському флоті – 62,3 %, у повітряно-десантних військах – 63,7 %).

Але Російська агресія призупинила довготривалу стагнацію Збройних Сил та інших складових сил оборони України, у тому числі в питаннях оснащення ОВТ. В Україні створено Міністерство з питань стратегічних галузей промисловості України, яке розпочало активно формувати оборонно-промислову політику нашої держави. Більш ніж у 3 рази зросли обсяги фінансування Збройних Сил України, а витрати на розвиток ОВТ – майже у 9 разів. Проривними напрямками у цієї сфері є створення вітчизняних БПЛА, окремих зразків ракетної зброї тощо.

Однак, основні фінансові, матеріальні і виробничі ресурси у 2014-2021 роках переважно зосереджені на ремонті, відновленні боєздатності та частковій модернізації наявного озброєння і військової техніки. Виробництво нових їх зразків здійснюється в обмеженій кількості, без належної системності.

Відтак оборонна промисловість України у більшості випадків була змушена орієнтуватися на виконання низькотехнологічних (low-tech) робіт, пов'язаних лише з ремонтом та частковою модернізацією озброєння. Така спрямованість зусиль вітчизняної оборонної промисловості, об'єктивно обумовлена російською агресією і довготривалим періодом стагнації сил оборони, негативно позначилася на інноваційній діяльності. А головне, в Україні наразі *відсутня ефективна сис-*

¹ Горбулін В. Як перемогти Росію у війні майбутнього. – К.: Брайт Букс, 2020. – 256 с.

тема наукових досліджень і впровадження новітніх технологій для створення сучасних ОВТ.

Це суттєво знижує спроможності наших сил оборони, обмежує можливості опанування ними нових форм і способів ведення збройної боротьби, у тому числі з асиметричної протидії російській агресії. А саме це є однією з основних умов для стримування значно переважаючого за чисельністю та оснащенням противника від подальшої ескалації збройного конфлікту, а також здійснення ним повномасштабної агресії проти України.

З огляду на зазначене, з метою впровадження ефективної системи організації та проведення наукових досліджень зі створення інноваційних оборонних технологій для розробки на їх основі високотехнологічних озброєнь, вважається за доцільне створення *Агентства з розвитку оборонних технологій* (далі – Агентство) за прикладом Управління перспективних дослідних проектів міністерства оборони США (англ. Defense Advanced Research Projects Agency, DARPA). Питання щодо доцільності створення Агентства було порушене Національним інститутом стратегічних досліджень спільно з Українським інститутом безпекових досліджень ще в жовтні 2019 року.

Передбачається, що діяльність Агентства сприятиме значному скороченню часу від виникнення інноваційних наукових ідей до реалізації на їх основі конкретних систем ОВТ.

Агентство відповідно до покладених на нього завдань, зокрема:

- здійснюватиме аналіз наукового і технологічного потенціалу України щодо створення ОВТ;
- здійснюватиме міжнародне співробітництво та реалізацію зовнішньої політики, зокрема державної військово-технічної політики у межах своєї компетенції;
- визначатиме пріоритетні напрями наукових досліджень, відбір передових ідей та інноваційних проектів для прискореного розвитку ОТ;
- здійснюватиме заходи щодо організації розробок перспективних ОТ, стимулювання розвитку та впровадження їх у конкретні зразки ВТО;
- організовуватиме взаємодію підприємств оборонно-промислового комплексу на засадах державно-приватного партнерства, наукових установ, навчальних закладів, неурядових організацій для розробок ОТ на договірній основі.

Доцільно передбачити можливість комплектування Агентства як державними службовцями, так і військовослужбовцями і науковими працівниками. Це дозволить у процесі відбору інноваційних проектів

та формулюванні завдань на розробку перспективних ОТ об'єктивно визначати цінність наукової ідеї та можливість її реалізації в перспективне озброєння з урахуванням сучасного і прогнозованого характеру збройної боротьби.

Фінансування Агентства як органу, діяльність якого належить до сфери оборони, здійснюватиметься за рахунок Державного бюджету України. При цьому доцільно визначити незнижуваний мінімум фінансування у процентному відношенні до загального обсягу фінансування потреб національної оборони на кожний рік. Крім того, слід передбачити, що відповідно до статті 55 Бюджетного кодексу України видатки на забезпечення діяльності Агентства мають бути захищеними. Зазначене дозволить гарантувати стабільне фінансування діяльності Агентства.

Зважаючи на положення Закону України «Про оборону України», фінансування Агентства може здійснюватися додатково за рахунок благодійних пожертв фізичних та юридичних осіб, а також інших не заборонених законодавством джерел у порядку, визначеному Кабінетом Міністрів України.

Фінансування розробок перспективних оборонних технологій, організацію яких ініціюватиме Агентство, доцільно здійснювати також за рахунок грантів Національного фонду досліджень України на умовах, визначених Законом України «Про наукову і науково-технічну діяльність».

Таким чином, утворення Агентства з розвитку оборонних технологій забезпечить умови для формування ефективної системи наукових досліджень, розробок і виробництва озброєння і військової техніки, налагодження державно-приватного партнерства у цій сфері.

Желай О. П.

кандидат наук із соціальних комунікацій,
Служба інформаційно-аналітичного забезпечення,
Національна бібліотека України імені В.І. Вернадського

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОГО ОБСЛУГОВУВАННЯ УПРАВЛІНСЬКИХ СТРУКТУР АКТУАЛЬНОЮ СУСПІЛЬНО ЗНАЧИМОЮ ІНФОРМАЦІЄЮ

Впровадження електронних інформаційних технологій в бібліотечну сферу сприяло трансформації традиційних функцій бібліотек і розвитку нових форм діяльності. Комп'ютеризація бібліотек і підк-

лючення їх до Інтернету перетворило ці установи, по крайній мірі провідні з них, в інформаційні центри сучасного інформаційного комплексу. Новий статус бібліотечних установ обумовлює їх зростаючу роль у розвитку національних інформаційних процесів як центрів акумуляції, структуризації, збереження і організації використання інформаційних ресурсів розвитку, а також їх зростаючі можливості в організації безпеки національного інформаційного комплексу.

Бібліотеки, вводячи якісний суспільно значимий інформаційний ресурс у систему соціальних інформаційних комунікацій, сприяють вдосконаленню змістовних характеристик інформаційних обмінів в українському суспільстві, сприяють забезпеченню зростаючого впливу системи стратегічних комунікацій, протистоянню в цих комунікаціях змісту негативних матеріалів нашого супротивника в інформаційній війні.

Важливим напрямом вдосконалення сучасної інформаційної діяльності бібліотеки є розвиток дистанційних форм обслуговування електронними ресурсами, що стало можливим лише при освоєнні електронних інформаційних технологій. У відповідності з теорією розвитку інформаційного суспільства розвиток дистанційних форм обслуговування користувачів є перспективним напрямом наближення актуальних інформаційних ресурсів розвитку безпосередньо до користувача. Таким чином, інноваційна інформація, наукова, науково-технічна, інформація, що відображає зміст передових технологій, може потрапляти до користувача-практика, може успішно впроваджуватися у виробництво, суспільно корисну діяльність. Практика аналітичних структур провідних зарубіжних бібліотек і досвід аналітичних підрозділів НБУВ протягом більше ніж двох десятиріч років підтверджує правильність такої організації бібліотечної діяльності. В основу цієї діяльності покладено ще запит Адміністрації Президента Л. Кравчука: лист АПУ № 12-9/148. Реалізація цього запиту була продовжена надалі.

Протягом наступних років дана діяльність набувала розвитку.

На даний час служба інформаційно-аналітичного забезпечення органів державної влади (СІАЗ) з разом із суміжними структурами: Фондом Президентів України (ФПУ) та Національною Юридичною Бібліотекою (НЮБ) в постійному режимі обслуговує різні категорії користувачів системою спеціалізованих видань (журнальні, тематичні, оглядові, інформаційно-аналітичні, інформаційні): «Шляхи розвитку української науки»; «Суспільно-політичні події у відображенні електронних ЗМІ»; «Домінуючі теми суспільно-політичного характе-

ру у відображенні електронних ЗМІ»; «Україна: події, факти, коментарі»; «Події. Персоналії: регіональний зріз»; «Адаптація переселенців в Україні»; «Проблеми інформатизації»; «Інформаційні технології в державному управлінні: ініціативи Президента України»; «Стратегія сталого розвитку України-2030»; «Громадська думка про правотворення»; «Конституційний процес в Україні»; «Інститут президентства в зарубіжних ЗМІ» та ін. Розсилка інформаційно-аналітичних матеріалів здійснюється на електронні адреси центральних органів влади і посольств України за кордоном, громадських організацій; на електронні адреси місцевих органів влади і самоврядування: обласні й районні ради (570 email), обласні й районні державні адміністрації (405 email), територіальні громади (1095 email); на електронні адреси бібліотек мережі УБА (996 email), УСПП (223 email) – загалом розсилка охоплює понад дві тисячі електронних адрес.

Оскільки по статусу ми входимо в число академічних інституцій і фінансуємося як наукова установа НАНУ, то ми також розробляєм наукову проблематику, пов'язану із розвитком електронних інформаційних технологій, із трансформацією національного інформаційного простору, з проблемами інформаційної безпеки у контексті інформаційної війни, в якій змушена брати участь Україна. Наша науководослідна діяльність відбувається у межах завдань, визначених затвердженими плановими науковими темами, зокрема: «Оптимізація інформаційно-аналітичної діяльності бібліотек в умовах інтенсифікації інформаційних обмінів» (2013–2015 рр.); «Шляхи підвищення ефективності функціонування соціальних комунікацій в умовах посилення глобальних інформаційних впливів» (2016–2018 рр.); «Стратки як каркас національного інформаційного простору. Адаптація технологій стратегічних комунікацій відповідно до соціокомунікативних структур суспільства й держави» (2019–2020 рр.); «Особливості інформаційних обмінів на рівні стратегічних комунікацій. Державна інформаційна політика в міжнародних інформаційних обмінах (2021–2023 рр.).

Результати НДР відображаються у монографіях, статтях, доповідях на конференціях. Варто відзначити такі колективні монографії: «Технології розвитку і захисту національного інформаційного простору» (2015 р.), «Соціокультурні механізми формування ментального імунітету проти зовнішніх маніпуляцій свідомістю населення України» (2015 р.), «Проблеми суспільної безпеки в процесі розвитку соціальних мереж» (2015 р.), «Інформаційно-культурне забезпечення інтеграції регіонів України» (2018 р.), «Розвиток інформаційної культу-

ри як умова єдності українського суспільства» (2017 р.), «Формування стратегічного наративу інформаційного забезпечення реінтеграції тимчасово окупованих територій у загальноукраїнський контекст» (2017 р.).

При введенні наукової тематики інформаційно-аналітична робота СІАЗ розглядається як науково-практична, як робота з практичного впровадження результатів наукового дослідження. З усіма формами нашої діяльності можна ознайомитися на нашому сайті nbuv.gov.ua – Центр досліджень соціальних комунікацій НБУВ: СІАЗ, НЮБ, ФПУ (ЦДСК НБУВ: СІАЗ, НЮБ, ФПУ).

На закінчення хотілося б зауважити про таке: ми сьогодні обслуговуємо основну масу управлінських структур до громад включно, значну частину економічних структур, об'єднаних в УСПП, велике число бібліотечних установ, маємо спеціалізований постійно підтримуваний сайт з нашим доробком для всіх. Таке обслуговування ведеться у щоденному режимі. Цей механізм міг бути більш повно задіяний у роботі з інформаційної безпеки. Така активність могла б бути реалізована при більшій зацікавленості замовника, при спеціальному державному замовленні, орієнтованому на актуальні запити інформаційної безпеки.

Мірошниченко О. П.

Головне науково-експертне управління
Апарату Верховної Ради України

ПРІОРИТЕТНІ НАПРЯМИ ПРОТИДІЇ ЕКОЛОГІЧНИМ ЗАГРОЗАМ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ УКРАЇНИ

Відповідно до ст. 16 Конституції України, якою визначено, що «забезпечення екологічної безпеки і підтримання екологічної рівноваги на території України, подолання наслідків Чорнобильської катастрофи – катастрофи планетарного масштабу, збереження генофонду Українського народу є обов'язком держави» [3]. Державна політика у сферах національної безпеки і оборони спрямована на захист: людини і громадянина – їхніх життя і гідності, конституційних прав і свобод, безпечних умов життєдіяльності; суспільства – його демократичних цінностей, добробуту та умов для сталого розвитку; держави – її конституційного ладу, суверенітету, територіальної цілісності та недото-

рканності; території, навколишнього природного середовища – від надзвичайних ситуацій (ч. 1 ст. 3 Закону України «Про національну безпеку України» від 21.06.2018 [5]). **Свою чергою, державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо (ч. 4 ст. 3 Закон України «Про національну безпеку України» [5]). Отже, екологічна безпека є невід’ємною і важливою складовою національної безпеки України.**

Останнім часом неабиякої актуальності та гостроти набуває проблема забезпечення екологічної безпеки та протидії екологічним загрозам та викликам на тимчасово окупованих територіях України (далі – ТОТ). Видається, що сучасний стан екологічної безпеки України повинен розглядатися в тісному взаємозв’язку із техногенними та іншими екологічними загрозами, які пов’язані із бойовими діями у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії РФ у Донецькій і Луганській областях, відсутністю належного державного контролю (моніторингу) за станом навколишнього природного середовища на ТОТ, зокрема, в окремих районах Донецької та Луганської областей.

Як зазначається в Стратегії національної безпеки України, схваленій Указом Президента України № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» [7], реалізація пріоритетів національних інтересів України та забезпечення національної безпеки забезпечуватиметься серед іншого за такими напрямками як забезпечення екологічної безпеки, створення безпечних умов життєдіяльності людини, зокрема на територіях, що постраждали внаслідок бойових дій, розбудова ефективної системи цивільного захисту (п. 6 Стратегії національної безпеки України).

Зазначимо, що відповідно до п. 4 Рішення РНБО України «Про виклики і загрози національній безпеці України в екологічній сфері та першочергові заходи щодо їх нейтралізації» від 23.03.2021[4], передбачено, що «для розв’язання екологічних проблем, відновлення та збереження навколишнього природного середовища Донбасу: а) розробити та затвердити у тримісячний строк концепцію стабілізації екологічної ситуації та забезпечення екологічної безпеки на території Донецької та Луганської областей; б) забезпечити вжиття у 2021 році

заходів щодо залучення міжнародних організацій до моніторингу стану навколишнього природного середовища і додержання вимог екологічної безпеки на тимчасово окупованих територіях України». Разом з тим, слід констатувати, що наразі проблема протидії екологічним загрозам і викликам на ТОТ України не отримала належного системного та комплексного вирішення, зокрема, в законодавчій площині.

При розв'язанні зазначеної вище проблеми, на нашу думку, слід враховувати, що збройний конфлікт на сході України відбувається у найбільшому в Європі вугледобувному районі, в якому розташовано значну кількість потенційно небезпечних об'єктів. До початку збройного конфлікту на території Донецької області було зосереджено п'яту частину промислового потенціалу нашої держави, 78 % якого припадає на екологічно небезпечні виробництва. Так, зокрема, в регіоні зосереджено 5,5 тис. промислових підприємств та об'єктів інфраструктури, які, у разі ушкодження, стануть джерелом значної шкоди для населення та навколишнього природного середовища [1]. Військовими діями, руйнацією інфраструктури та екологічно небезпечних підприємств на ТОТ порушено екологічну рівновагу, що призвело до небезпечних змін стану довкілля, спричинило шкоду здоров'ю та порушило безпеку життєдіяльності для п'яти мільйонів населення на території близько 30 тис. км².

Основними загрозами на ТОТ, зокрема, в окремих районах Донецької та луганської областей, є: затоплення шахт та можливість виходу токсичних шахтних вод на поверхню, проникнення у підземні води; загроза потрапляння їх до річки Сіверський Донець та Азовського моря; припинення роботи очисних споруд та пошкодження сховищ токсичних та радіоактивних відходів; пошкодження територій природно-заповідного фонду; забруднення атмосферного повітря та ґрунтів хімічними продуктами внаслідок вибухів боєприпасів; знищення ландшафтів та рослинності у зв'язку з використанням військової техніки та будівництвом оборонних споруд; знищення значних площ лісів унаслідок викликаних воєнними діями пожеж та неконтрольованих рубок [1].

Так, за оцінкою експертів Програми ООН з навколишнього середовища (ЮНЕП), в результаті конфлікту на Донбасі зруйновані екосистеми на території щонайменше 530 тис. га, у тому числі у 18 природних заповідниках загальною площею 80 тис. га [1]. Крім того, від пожеж значно постраждало 150 тис. га лісів на території, прилеглій до зони бойових дій. Слід також враховувати, що зона бойових дій, у

тому числі сільськогосподарські угіддя, значно насичена боєприпасами, що не вибухнули, розмінування та ліквідація яких потребуватиме років або навіть десятиліть.

Отже, дані ООН свідчать, що Донбас перебуває на порозі екологічної катастрофи, причиною якої є забруднення повітря, ґрунту і води унаслідок вибухів великої кількості боєприпасів та затоплення промислових підприємств і вкрай необхідним є якнайшвидше провести оцінку екологічних збитків, завданих збройним конфліктом, і звести їх до мінімуму [2]. Очевидно, що проведення екологічного моніторингу стану ТОТ, де органи державної влади України тимчасово не здійснюють свої повноваження, з можливим залученням міжнародних екологічних експертів, зокрема, МАГАТЕ, ЮНЕП з метою оцінки екологічної ситуації, стає все більш актуальним.

Таким чином, враховуючи масштаби прояву і комплекс негативних екологічних наслідків для окремих районів Донецької та Луганської областей, можна вважати, що проблема забруднення і деградації основних складових навколишнього природного середовища на цих територіях з урахуванням довгострокового впливу екологічних і соціальних наслідків має системний характер і може розглядатися як новітня загроза національній безпеці в екологічній сфері. Сучасні виклики та загрози національній безпеці нашої держави вимагають формування нових, нестандартних та ефективних методів для їх протидії та нейтралізації, у тому числі, в екологічній сфері.

Пріоритетними напрямками у протидії екологічним та техногенним загрозам і викликам на ТОТ, мають бути наступні: по-перше, включити до Стратегії національної безпеки України екологічні наслідки збройного конфлікту на сході України до переліку актуальних новітніх загроз національній безпеці в сфері забезпечення екологічної безпеки; якнайшвидше схвалити Стратегію екологічної безпеки України, в якій обов'язково мають бути відображені окремим пунктом екологічні загрози та виклики на ТОТ України та механізми їх протидії та нейтралізації; Уряду України звернутись із запитом до ООН, ОБСЄ та ін. міжнародних міжурядових і неурядових організацій в контексті проведення міжнародної оціночної місії на ТОТ України, із оцінки збитків, що завдані здоров'ю населення та навколишньому природному середовищу. Крім того, очевидно, доцільним вбачається визначити стратегію розвитку нормативно-правового забезпечення подолання наслідків екологічної кризи на ТОТ Донецької та Луганської областей, пріоритетів екологічної політики України у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії

Російської Федерації у Донецькій і Луганській областях, пов'язане із необхідністю розроблення комплексної програми подолання та нейтралізації наслідків бойових дій та ін.

Очевидно, що недооцінка нових екологічних загроз в контексті забезпечення екологічної безпеки нашої держави в найближчій перспективі потенційно може обернутися загальною екологічною катастрофою для України та сусідніх держав. Подолання цих загроз багато в чому залежать від стану чинного законодавства України в частині формування правових засад забезпечення екологічної безпеки України, спроможності органів державної влади України віднайти правові, організаційні та ін. механізми вирішення новітніх екологічних проблем.

Література

1. Донбас на порозі екологічної катастрофи - експерти ООН. URL: <https://news.un.org/ru/story/2018/11/1342192> (дата звернення: 05.07.2021).
2. Іванюта С.П. Пріоритетні напрями протидії екологічним і техногенним загрозам в зоні військового конфлікту на Сході України. URL: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/prioritetni-napryami-protidii-ekologichnim-i-tekhnogennim-zagrozm> (дата звернення: 06.07.2021).
3. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. (в редакції від 01.01.2020). URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 05.07.2021).
4. Про виклики і загрози національній безпеці України в екологічній сфері та першочергові заходи щодо їх нейтралізації: Рішення РНБО від 23.03.2021. URL: <https://zakon.rada.gov.ua/laws/show/n0018525-21#Text> (дата звернення: 07.07.2021).
5. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 07.07.2021).
6. Про Основні засади (стратегію) державної екологічної політики України на період до 2030 року : Закон України; Стратегія від 28.02.2019 № 2697-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2697-19#Text> (дата звернення: 06.07.2021).
7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України: Указ Президента України 392/2020 <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 07.07.2021).

Медведєва А. С.
кандидат наук із соціальних комунікацій,
Національна бібліотека України
імені В. І. Вернадського

ОСОБЛИВОСТІ МОНІТОРИНГУ РЕГІОНАЛЬНИХ ЕЛЕКТРОННИХ РЕСУРСІВ В ОБСЛУГОВУВАННІ УПРАВЛІНСЬКИХ СТРУКТУР

В умовах сучасної російсько-української інформаційної війни вивчення процесу розвитку вітчизняного інфотворення та інформаційних обмінів набуває особливого значення. Рівень важливості даного процесу збільшується через реалізацію політики регіоналізації та набуття регіонами більшої самостійності від центру. Зарубіжні політтехнологи стимулюють завдяки проникливій, на сьогодні, інфосфері розвиток цієї самостійності, роздувають регіональну специфіку проблеми взаємовідносин з центром і намагаються посадити на власний інформаційний гачок та на особисті інформаційні орієнтири регіональних користувачів інформації.

Вітчизняні бібліотечні установи, що згідно з закономірністю мають трансформуватися в сучасні інформаційні центри після своєї комп'ютеризації і включення в інтернет-комунікації, мають дати число комплектування не лише новоствореної книжкової та газетно-журнальної продукції, але їх джерелом комплектування мають також стати електронні ресурси. З огляду на те, що їх функції мають розширитись до аналізу регіонального інфотворення інформаційних обмінів електронними ресурсами, а також до виявлення в цих обмінах шкідливої для розвитку нашого суспільства інформації. Результати цього аналізу мають доводитись до відома управлінських структур, до всіх категорій зацікавлених користувачів та використовуватись при відборі інформації для комплектування різноманітних фондів.

Електронні підрозділи НБУВ здійснюють таку роботу починаючи з 90-х років минулого століття відповідно до запитів вищих органів влади. Особливості цієї роботи удосконалювались із розвитком електронних інформаційних технологій. З початку працівники відділу СІАЗ вели реферативний аналіз регіональної праці. На замовлення владних структур такі аналізи відобразились в бюлетенях інформаційно-аналітичних виданнях щотижневої, а при потребі щоденної періодичності. З розвитком електронних інформаційних обмінів розширювався й асортимент видань з узагальненням регіональної тематики,

відповідно до запитів основних груп користувачів. Саме у таких виданнях представлено проблематику питання інформаційної безпеки у соцмережах, актуальні проблеми децентралізації, адаптації переселенців в регіонах, питання рейдерства під час підприємницької діяльності та інформатизації тощо.

У даний час згідно з запитом замовника проблемна група працівників СІАЗ, залучених працівників Фонду Президентів України та НЮБ здійснюють трудозатратний проект моніторингу всіх областей України по аналізу внутрішньосуспільної проблематики, у т. ч. безпекової в щотижневій періодичності. Ми вивчаємо вплив цього комплексу інформаційних чинників на свідомість громадян в регіонах. Тематика періодичних видань сформульована в усіх видах електронного інформування надзвичайних і резонансних подій, реагування на проблему коронавірусу, на діяльність регіональних управлінських структур, на реалізацію орієнтирів суспільного розвитку та інше. Достовірність даних моніторингу матеріалів проявляється в закономірностях, що підтверджуються перебігом наступних подій, як це було з минулими виборами.

Моніторингові матеріали підготовлені нами переконливо доводять, що регіональні інформаційні джерела у своїй основі підтримують, насамперед, діяльність місцевої влади, створюють їй позитивний інформаційний імідж. Ця діяльність зосереджена на місцевій проблематиці і в ній не простежуються суттєві зарубіжні впливи. Всі види електронного інформування в своїй сукупності підтримують антиолігархічні заходи президента В. Зеленського і цим самим сприяють зростанню його іміджу в суспільній свідомості, що в областях, які прилягають до зони конфлікту на Сході при наявному впливі російської пропаганди, ця пропаганда уступає інформаційній діяльності українських джерел інформування.

Рейтинги українських політичних діячів є високими і за лінією розмежування. При цьому всьому варто зазначити, що захоплення місцевою проблематикою регіональні інформаційні джерела все ж мало приділяють уваги роз'ясненню важливих документів підготовлених у Києві. Мова йде насамперед про важливі рішення РНБО, документи пов'язані із вирішенням земельного питання, обговорення проблем про вступ у НАТО та інше. Працівники нашої проблемної групи твердо переконані, що будь-яка масштабна інформаційна агресія в регіонах України в рамках нашого моніторингу буде своєчасно помічена і це дасть змогу її вчасно нейтралізувати.

Базиліук Я. Б.
кандидат економічних наук,
Національний інститут стратегічних досліджень

ОСОБЛИВОСТІ СУЧАСНИХ ЕКОНОМІЧНИХ СТРАТЕГІЙ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ВИСНОВКИ ДЛЯ УКРАЇНИ

Досягнення економічними методами цілей агресії – найбільш серйозної і небезпечної форми незаконного застосування сили, явище не нове. Водночас, масштаби поширення цього явища в сучасних міжнародних відносинах, зокрема з боку РФ, вимагають переосмислення уявлень про економічний вимір гібридних конфліктів та розширення переліку операційних просторів сучасної війни.

Дослідженнями злиття економічних та геополітичних інтересів, а також використання економічних (фінансових, технологічних, цифрових та ін.) механізмів для отримання геополітичних переваг й досягнення відповідних цілей, опікується значна кількість експертів та вчених, фахових організацій, а також урядових структур. Серед них слід відзначити М. Фельдштейна [1], М. Леонарда, Ж. Пізані-Феррі, Є. Рібакової, Дж. Шапіро, Г. Вольфа [2], Ж-П. Дарніса [3], документи стратегічного порядку ЄС [4–5], США [6], України [7], РФ [8] тощо. Водночас зберігає невирішеність проблема інтеграції понять та визначення системи забезпечення економічної безпеки в новій цифровій та технологічній парадигмі розвитку.

Економічна сфера, виступаючи невійськовою сферою суспільних відносин, в конфліктах гібридного типу здатна бути перетвореною на широкоформатний операційний простір реалізації агресії як у внутрішньому, так і зовнішньому середовищі (рис. 1).

	Економічні методи впливу (фінансові, торговельні, промислово-технологічні, економічні санкції, економічна допомога та ін.)	Неекономічні методи впливу (військові, політичні, ідеологічні, інформаційні, юридичні, культурні, дипломатичні та ін.)
Економічна сфера суспільних відносин	X	X
Неекономічні сфери суспільних відносин (політична, соціальна, духовна, культурна та ін.)	X	

Рис. 1. Середовище розгортання економічного операційного простору гібридної агресії (складено автором)

Характерними особливостями застосування економічних заходів для досягнення цілей агресії є нанесення економічними інструментами державі-об'єкту агресії збитків, які можуть бути співставними із втратами у період активних бойових дій (депопуляція, згортання ВВП, катастрофічне зниження промислового або воєнно-економічного потенціалу, критичне зростання безробіття тощо) або нагромадження економічних залежностей, які згодом можуть використовуватись для тиску.

Перевагами для держави-агресора є те, що незалежно від масштабів агресивного економічного впливу та ступеню нанесених соціально-економічних збитків, у відповідь не передбачається застосування військових заходів. На теперішній час невідомі приклади доктрин національної безпеки держав, які кваліфікують, навіть суттєву, економічну агресію приводом для військової відповіді.

Підготовка соціально-економічного ландшафту у війнах гібридного типу є важливим складовим елементом, для чого можуть бути використані такі комбінації економічних заходів:

- запровадження економічної блокади (економічної ізоляції країни, що передбачає обмеження або заборону на торгівлю всіма чи окремими товарами);
- розгортання торговельної війни через впровадження дискримінаційних умов торгівлі (застосування тарифних (торговельних, санітарних та фітосанітарних бар'єрів, технічних вимог тощо) і нетарифних методів). Торговельна війна може розгортатись *локально* (у форматі двосторонніх економічних відносин, і як правило, засновується на витісненні товарів та послуг виробників держави-об'єкта агресії з внутрішнього ринку держави-суб'єкта агресії під приводом «захисту» внутрішнього ринку) та *глобально* (у форматі жорсткого конкурентного протистояння на ринках третіх країн);
- припинення дії торговельних угод, спільних проектів та промислових програм у певних сферах, зокрема у сфері безпеки та оборони;
- заборона трансферу технологій, прав на об'єкти права інтелектуальної власності;
- припинення надання економічної допомоги;
- реалізація заходів з концентрації економічного контролю над економічною та фінансовою сферами держави-об'єкта агресії (концентрація економічної власності у стратегічних галузях економіки держави-об'єкта агресії, в тому числі економічної інфраструктури (транспортної, інформаційної, зв'язку (мобільні оператори та Інтернет)); посилення залежності держави-об'єкта агресії від постачання стратегічної сировини (енергоресурсів, ядерного палива та ін.); концентра-

ція контролю над банківським сектором держави об'єкта агресії та нагромадження її суверенного боргу) тощо.

Відповідна агресія може бути реалізована через централізовані та децентралізовані канали, державними та недержавними агентами у формах:

- економічних маніпуляцій (економічного шантажу, тиску, примушення);

- підготовки та реалізації економічних злочинів (привласнення економічних активів, шахрайство, рейдерство тощо);

- організації нелегальної економічної діяльності (розширення потоків контрабанди; відмивання грошей; організації на території держави-об'єкта агресії інноваційних децентралізованих фінансових мереж для фінансування тероризму, сепаратистських рухів, НКО, які здійснюють підривну діяльність тощо та ін.);

- підривання інституційних основ функціонування легального сектору економіки через хабарництво, системну корупцію тощо;

- використання корупційних каналів впливу в економічній сфері для досягнення цілей агресії (укладання економічно недоцільних, екологічно- та технологічно шкідливих економічних контрактів; вплив на управлінські рішення в економічній сфері з метою стримування економічного, воєнно-економічного та інноваційно-технологічного розвитку, пригнічення зовнішньоторговельного потенціалу та блокування диверсифікації зовнішньоторговельних зв'язків держави-об'єкта агресії тощо);

- формування мереж організованої злочинності національного та транснаціонального характеру;

- здійснення актів економічного тероризму (організація широко спектру економічних заходів на економічних об'єктах держави-об'єкта агресії, які призводять до зупинки їх фінансово-господарської діяльності, доведення до банкрутства, розмивання частки акцій, істотного підвищення соціального напруження внаслідок скорочення працівників (насамперед на системоутворюючих підприємствах; отримання інсайдерської інформації та конфіденційної інформації про акціонерів тощо) та погіршення умов їх праці тощо; диверсії проти економічної інфраструктури; кібер-атак на фінансову та економічну інфраструктуру; створення небезпеки і/або завдання суттєвої майнової шкоди державі та громадянам внаслідок викрадення та маніпуляцію персональними даними тощо);

- шпигунства (промислового, технологічного, патентного тощо).

Для України гібридний конфлікт з РФ з високою ймовірністю зберігатиме актуальність у довгостроковій перспективі. Протидія гібридній агресії для України значною мірою залежить від успішності мобілізації зусиль для економічного захисту суверенітету, ідентифікації та неухильного дотримання національних економічних інтересів, модернізації системи формування та імплементації санкцій, які забезпечують інтереси національної безпеки та участь у системі міжнародної взаємодії й колективного захисту від російської агресії.

Водночас, помітна чутливість української економіки до впливу гібридної агресії обумовлена, зокрема збереженням достатньо суттєвих економічних залежностей від РФ. Зокрема, для України РФ зберігає роль одного з найбільших торговельних партнерів, попри понад п'ятикратне згортання двостороннього товарообороту з 37,9 млрд дол. США у 2013 р. до 7,2 млрд дол. США у 2020 р. За обсягом зовнішньоторговельного обороту України в 2020 р. РФ посідає четверте місце, попри зниження частки з 27,4 % у 2013 р. до 7,0 %. У 2020 р. з рекордно низьким товарооборотом між Україною та РФ (експорт товарів в РФ склав 2,7 млрд дол. США, імпорт з РФ становив 4,5 млрд дол. США), від'ємне сальдо склало 1,8 млрд дол. США.

І хоча впродовж гібридної війни національна економіка повільно, але системно відновлюється, компенсуючи відчутні наслідки втрати та зміцнюючи співробітництво на позаросійському напрямку. Збереження достатньо високого рівня економічних залежностей від РФ, обумовлює небезпечний потенціал руйнування суверенітету та національних інтересів особливо за умов ескалації агресії.

Для України протидія гібридній війні з боку РФ повинна включати більш широке використання засобів невійськового характеру, якими має утворюватись відчутна економічна мотивація щодо деескалації конфлікту та його превентивного стримування. Пріоритетними напрямками економічної стратегії України в умовах гібридної війни доцільно визначити:

- заходи щодо кардинального прискорення економічного зростання та зміцнення конкурентоспроможності національної економіки на інноваційній основі, що дозволить посилити матеріальну базу відповіді на гібридну агресію;

- посилення інституціональної спроможності протидії деструктивному впливу в економічній, фінансовій, цифровій, технологічній, промисловій та інфраструктурній сферах на основі регламентації іноземного впливу та застосування симетричних дій у разі вчинення деструктивних зовнішніх дій;

- зосередження в Україні виробництва і/або диверсифікації джерел постачання передових технологій та товарів критичного імпорту;
- системне зміцнення наукової, дослідницької, технологічної та інноваційної бази;
- захисту національних активів, які мають вирішальне значення для національної безпеки, від іноземного деструктивного втручання у процесі володіння, розпорядження та використання;
- забезпечення національного контролю над морською, енергетичною та цифровою інфраструктурою за активної підтримки міжнародної спільноти;
- забезпечення контролю над інвестиціями у таких чутливих для сучасної економіки сферах як: інфраструктура 5G, хмарні технології, збереження даних, операційні системи, доступ до космосу та ін.

Література

1. *Martin Feldstein*. Economics and American National Security URL: <https://www.project-syndicate.org/commentary/economics-american-national-security-strategy-by-martin-feldstein-2017-12>.
2. *Mark Leonard, Jean Pisani-Ferry, Elina Ribakova, Jeremy Shapiro and Guntram Wolf*. Redefining Europe's economic sovereignty / Policy Contribution Issue n 9. June 2019 URL: https://www.bruegel.org/wp-content/uploads/2019/06/PC-09_2019_final-1.pdf
3. *Jean-Pierre Darnis*. A COVID-19 Moment for Technological Sovereignty in Europe? URL: <https://www.iai.it/en/pubblicazioni/covid-19-moment-technological-sovereignty-europe>.
4. The European economic and financial system: fostering openness, strength and resilience Brussels, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. 19.1.2021 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0032&from=EN>.
5. European Commission. 2020 Strategic Foresight Report. Charting the Course Towards a More resilient Europe. URL: https://ec.europa.eu/info/sites/info/files/strategic_foresight_report_2020_1.pdf.
6. *Interim National Security Strategic Guidance*. President Joseph R. Biden, Jr. March 2021. URL: <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>.
7. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» № 392/2020 від 14.09.2020 URL: <https://zakon.rada.gov.ua/laws/show/392/2020#n5>.
8. Указ Президента Российской Федерации от 13.05.2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года». URL: <http://kremlin.ru/acts/bank/41921>.

Вдовенко С. Г.
Ганенко С. О.
кандидат технічних наук
Гульков М. О.
Національний університет оборони України
імені Івана Черняхівського

ІНФОРМАЦІЙНЕ ПІДГРУНТЯ ГІБРИДНОЇ ВІЙНИ РФ ПРОТИ МІЖНАРОДНОГО ПОРЯДКУ

Гібридна війна є високотехнологічним конфліктом, продовженням політики держав (коаліцій, політичних угруповань, транснаціональних корпорацій тощо) з метою нав'язування опонентам своєї волі за допомогою комплексних адаптивних і асиметричних синхронізованих впливів на них у різних просторах та сферах з поєднанням конвенційної і неконвенційної складових, забезпеченням багатовимірності, мультиплікативності та синергетичності результатів і високого рівня невизначеності для опонентів щодо кінцевих цілей і шляхів їх досягнення.

Гібридна війна не оголошується і тому не може бути завершена в класичному розумінні завершення воєн і воєнних конфліктів. Це перманентна війна змінної інтенсивності. Деструктивні впливи в ній супроводжуються, як правило, ланцюговими ефектами і синергетичними наслідками. У гібридних війнах в тій чи іншій мірі свідомо чи несвідомо задіяне не тільки все населення країни, яка стала об'єктом агресії, а й міжнародне співтовариство. У гібридних конфліктах військові дії поєднуються з іншими, головним чином економічними, політичними, дипломатичними, інформаційними, психологічними, кібернетичними, когнітивними й іншими діями, які комплексно призводять до системної дестабілізації в усіх сферах життя і діяльності держави, яка є об'єктом агресії.

Гібридна війна, яка йде на території України, фактично охоплює все більше учасників у всьому світі. Це конфлікт, в якому стираються відмінності між безпосередньо війною в її класичному розумінні, і політикою та економікою, між військовими й іншими її учасниками та мирним населенням.

За висновками сенатської комісії США *Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S.*, зробленими у 2018 р., головним інструментом гібридної війни в російській операції

в Україні є кібератаки, які направлені на всі сектори суспільства та економіки, зокрема такі як медіа, фінанси, транспорт, політика, енергетика і військова справа. РФ з 2014 р. невпинне й різноманітно використовує кіберпростір України в якості театру кібердій та полігону для випробовування російської кіберзброї.

За поглядами фахівців РФ на природу гібридної війни впливають ідеологічне забарвлення міжнародних політичних процесів та різниця у поглядах Росії та колективного Заходу щодо відновлення багатоплярності світового устрою, звісно звинувачуючи у цьому США. При цьому вважається, що саме можливості сучасних інформаційних технологій надають спроможностей протиборчим сторонам щодо викривлення та спотворення інформації, розповсюдження фейків, фальсифікації історії.

Воєнна доктрина (2014) та Доктрина інформаційної безпеки (2016) РФ визначають можливість застосування сил інформаційних операцій (дії в кіберпросторі не відокремлюються) в інформаційній війні з метою створення системи неядерного стримування та запобігання конфліктам, для оборони, а також з метою нападу. Війська інформаційних операцій МО РФ створені на підставі указу президента РФ у лютому 2014 року та налічують близько 1000 військовослужбовців, їх фінансування – на рівні 18 млрд руб. (\$300 млн.). Основну частину активних дій покладено на «добровольців», «хактивістів» та інші «підконтрольні» невійськові сили та засоби.

Недосягнення кінцевої мети РФ у ході гібридної війни в Україні призвело до необхідності перегляду та затвердження Указом президента РФ від 02.07.2021 № 400 нової «Стратегії національної безпеки РФ». На відміну від попередньої Стратегії (2015), згідно якої інформаційна безпека входила в розділ «наука, технології та освіта», вона вперше виділена як окремий пріоритетний напрям, що за поглядами керівництва РФ обумовлено більш активним, ніж раніше, проявом інформаційних та кіберзагроз, зокрема:

- використання інформаційних та кібертехнологій для втручання у внутрішні справи Росії;

- прагнення транснаціональних корпорацій закріпити контроль над інформаційними ресурсами в інтернеті;

- значне збільшення числа комп'ютерних атак на російські інформаційні ресурси;

- масштабне поширення недостовірної інформації і зростання числа злочинів, скоєних із застосуванням цифрових технологій.

У Стратегії наголошується, що сучасний світ переживає період трансформації і поява нових центрів світового економічного і політичного розвитку призводить до формування нових правил і принципів світового устрою. Зростання нестабільності в світі може призвести до спроб вирішити міждержавних протиріч за рахунок «пошуку внутрішніх і зовнішніх ворогів, до руйнування економіки, традиційних цінностей і ігнорування основних прав і свобод людини». Метою забезпечення інформаційної безпеки в Стратегії заявлено зміцнення суверенітету Росії в інформаційному просторі, а досягнення цієї безпеки має здійснюватися шляхом реалізації державної політики, спрямованої на вирішення низки тематичних завдань.

Пермяков О. Ю.

доктор технічних наук, професор,
заслужений діяч науки і техніки України,
Національний університет оборони України
імені Івана Черняховського

Корольок Н. О.

кандидат технічних наук, доцент,
Харківський національний університет
Повітряних Сил імені Івана Кожедуба

Фараон С. І.

Національний університет оборони України
імені Івана Черняховського

ІНФОРМАЦІЙНІ ТА ЕКОНОМІЧНІ АСПЕКТИ Й ЕКСПАНСІЙНИХ МЕХАНІЗМІВ У ДОСЯГНЕННІ ВІЙСЬКОВО-ПОЛІТИЧНИХ ЦІЛЕЙ РФ У ГІБРИДНІЙ ВІЙНІ

Для України у середньостроковій перспективі найбільш актуальними загрозами визнані: агресивні дії Росії, розвідувально-підривна і диверсійна діяльність РФ та інших держав. Визнається уразливість об'єктів економіки, критичної інфраструктури та їх систем управління, а саме: урядових структур; установ сектору безпеки і оборони; науково-дослідного сектору; кредитно-фінансової і банківської системи, сфер соціального захисту, цивільної оборони, енергетики, хімічної та харчової промисловості, транспорту, комунального господарства, водопостачання, телекомунікацій, сільського господарства, закладів охорони здоров'я, що є стратегічно важливими для функціонування

економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв.

Сучасне суспільство практично повністю залежить від стану безпеки інформаційної інфраструктури. Не лише урядові структури держав, але й злочинні та терористичні організації отримали можливість використання глобальної мережі для досягнення своїх цілей. Проникнення інформаційних технологій в усі сфери життя людини та суспільства дозволило розглядати інформаційну зброю, як зброю першого удару. Згідно концепції Уордена-Бойда (John Ashley Warden III, John Boyd) в «операціях на основі ефектів» (ЕВО – Effect-based-Operations), що ставили за мету системні порушення управління та функціонування держав противника до кризового рівня (рис. 1), в якості цілей для ураження або взяття під контроль стали розглядатися не лише збройні сили, населення і керівництво держав але й об'єкти економіки, інфраструктура та комунікації протиборчої сторони.

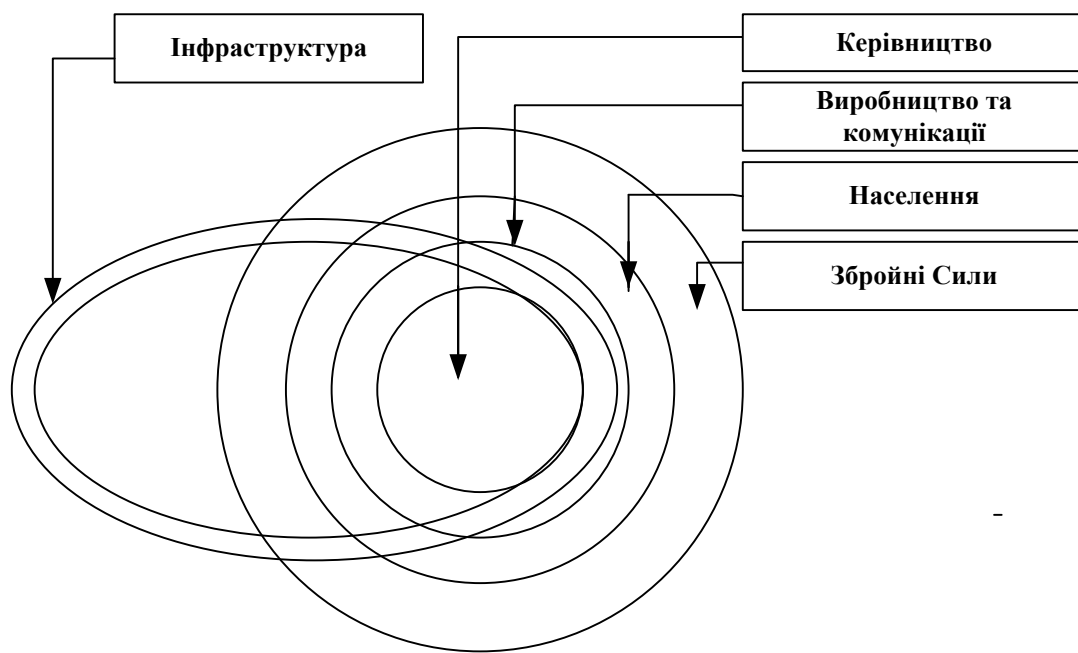


Рис. 1. Модифіковані кільця Уордена (Цілі ЕВО – атак)

Сучасна геополітика вимагає цілеспрямованої активної діяльності держав, щодо пошуку ефективної моделі запобігання та протидії гібридній війні, підвищення ролі і значення державних інституцій щодо реалізації заходів протидії та їх забезпечення. У гібридних війнах в тій чи іншій мірі свідомо чи несвідомо задіяне не тільки все на-

селення країни, яка стала об'єктом агресії, а й міжнародне співтовариство. У гібридних конфліктах військові дії поєднуються з іншими, головним чином економічними, політичними, дипломатичними, інформаційними, психологічними, кібернетичними, когнітивними й іншими діями, які комплексно призводять до системної дестабілізації в усіх сферах життя і діяльності держави, яка є об'єктом агресії.

Гібридна війна, яка йде на території України, фактично є високотехнологічним конфліктом, в якому стираються відмінності між безпосередньо війною в її класичному розумінні, і політикою та економікою, між військовими й іншими її учасниками та мирним населенням. Нові вразливості національної критичної інфраструктури, які проявляються паралельно з бурхливим розвитком технологій, породжують нові небезпеки, загрози й ризики в інформаційному та кіберпросторах та вимагають вирішення питань щодо їх запобігання, стримування та нейтралізації. Кібератаки стали комплексними, взаємоузгодженими, організованими, охоплюючими технічну, соціотехнічну та соціальну сфери та більш руйнівними для державних установ, підприємств, економіки, транспорту, електроенергетики, об'єктів критичної інфраструктури. Кібератаки можуть бути направлені як на об'єкти генерації енергоресурсів, так і на об'єкти їх транспортування та споживання. Існує велика ймовірність щодо проведення кібератак одночасно на всі об'єкти та системи будь-якого сектору економіки, зокрема, наприклад енергетика або транспорт.

Характер та метод їх застосування може мати гібридний розподільно-зосереджений вплив з ланцюговим ефектом, які розповсюджують деструктивну хвилю на взаємодіючі об'єкти та системи. Кібердії можуть здійснюватися послідовно-паралельно, з використанням методів організації розподільно-зосереджених дій, які полягають в зосередженні кібервпливів на найбільш вразливих елементах об'єкта (системи) та тих, сукупність одночасних та (або) послідовних впливів на які забезпечує отримання синергетичного ефекту в апріорі непередбачуваних місцях (елементах, системах, сферах) на які безпосередній вплив може і не спрямовуватися, а результат виникає за рахунок системи розосереджених впливів на не завжди безпосередньо взаємопов'язані елементи. Вони здатні впливати синхронно, комплексно, одночасно або послідовно, наносити ураження елементам системи та/або виводити її з ладу та можуть досягти критичного рівня, який загрожує національній безпеці і стабільності.

Це питання існування і майбутнього держав у сучасному світі, що перебуває напередодні нового етапу розвитку суспільства – постінформаційного.

Через це забезпечення безпеки інформаційної та кіберінфраструктури об'єктів управління економіки та інфраструктури є надважливою умовою забезпечення обороноздатності держави, її економічного та соціального розвитку.

Виходячи з цього, у держав виникає необхідність утворення ефективної системи кібербезпеки та кібероборони з функціональною спроможністю не нижче гранично необхідного рівня, не залежно від рівня економічного розвитку і стану та науково-технічного прогресу країни, але адекватно до рівня загроз, що притаманні світові у першій чверті ХХІ століття, а у стратегічній перспективі – до середини століття.

Князєв С. О.

кандидат юридичних наук, професор,
старший науковий співробітник,
Національна академія СБ України

СУЧАСНІ ТЕНДЕНЦІЇ ВЕДЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

Теперішній розвиток світового суспільства супроводжується масовим впровадженням інформаційних технологій у різні сфери життя. Інформаційно-комунікативні технології суттєво спростили можливість різноманітного спілкування між людьми. Саме завдяки цьому фактору кордони між країнами стали майже прозорими для різноманітних видів зв'язку, а відстань для спілкування взагалі перестала відігравати роль перепони.

Facebook, Twitter, Youtube, Instagram зараз мало хто може не знати ці назви. Різноманітні соціальні мережі об'єднали мільйони користувачів у всьому світі відповідно до їх уподобань, інтересів, поглядів, ділових стосунків, знайомств тощо.

Швидка та доступна можливість отримати майже будь-яку інформацію у «світовій павутині» з використанням різних пошукових систем, баз даних, електронних видань дозволяє припустити, що паперові видання, найближчим часом можуть стати раритетними спогадами.

Разом з тим, поряд з вагомими перевагами, які отримує від інформаційних технологій людство, з'явилися, активно розвиваються і поширюються новітні загрози як для життєдіяльності самої людини, так і для безпечного існування цілих держав.

Зокрема, цілеспрямована шкода окремій людині може бути завдана завдяки використанню спеціальних комп'ютерних програм, які призводять, наприклад, до обнуління банківських рахунків, несанкці-

онованому використанню персональних даних і т.п. Інший спосіб – удар по іміджу та репутації важливої посадової особи тощо.

Можливості негативного використання інформаційних технологій у контексті проведення інформаційних війн були висвітлені американським футурологом Елвіном Тоффлером в його «Метаморфозах влади» ще у 1990 році. «Інформаційні війни, - підкреслював Тоффлер, - вирують в наших душах, адже мова йде про те, як люди думають, як приймають рішення та яку використовують систему знань і уявлень. Уява при цьому є настільки ж важливим чинником, як і інформація взагалі».

Як зазначають аналітики, з масовим впровадженням інформаційних технологій і використанням інформації як зброї, метою війни стало не знищення супротивника, а цілеспрямоване керування ним. Іншими словами, інформаційні технології в наш час зробили, як видавалось, не можливе – «дистанційне управління противником» при мінімальному насильстві і кровопролитті. Тепер завдання знешкодження супротивника полягає не в знищенні живої сили, а в підриві світогляду населення, руйнуванні інфраструктури держави, зокрема збройних сил, у підриві авторитету керівництва держави тощо.

Причини проведення інформаційної війни можуть бути різні. Зокрема, територіальні зазіхання. Масована, цілеспрямована пропагандистко-підривна інформація, врешті решт повинна спровокувати місцеві референдуми, відокремити частину території від своєї країни, а далі поглинання території інформаційною країною-агресором.

Сучасна швидкість розповсюдження, подачі інформації, завдяки інформаційним технологіям та ефективність її сприйняття, дозволяє наслідки від «розкидання з літаків пропагандистських листівок» помножити у мільйони разів.

Тепер перекручування, підміна змісту інформації, трактування подій і фактів на певну користь стає основою страшної, руйнівної зброї, спрямованої на маніпулювання свідомістю як населення окремої країни, так і взагалі світової спільноти.

Широкомасштабне, цілеспрямоване проведення таких дій на державному рівні разом з іншими руйнівними заходами дозволяє стверджувати, що інформаційна війна стала невід'ємною складовою гібридної війни.

Загрози від проведення інформаційної війни з боку РФ спричинили появу серйозних викликів для України як цілісної, незалежної держави.

Аналізуючи останні події, котрі відбуваються в Україні, вітчизняні аналітики схожі у думці у тому, що інформаційна війна заповнила медіа-простір. Її методика є досить унікальною і спрямована на

знищенні усієї інформаційної інфраструктури або ж окремих елементів. Джерелом та потенційною зброєю є саме інформація. Під час ведення такого роду війни може не бути жертв, руйнувань, голоду, але у більшості випадків ці наслідки є рівнозначними.

Не даремно, представники вітчизняних інформаційних груп стверджують, що Кремль здійснюючи постійні інформаційні атаки, підтримує напругу та ескалацію конфлікту на сході України, чинить тиск на українське керівництво з метою змусити його приймати московський сценарій з урегулювання конфлікту. Експерти виокремлюють й основні напрями, на яких ця атака зосереджується:

- нав'язування точок зору про неспроможність української влади керувати державою та приймати раціональні рішення;
- створення уявлень про те, що наразі для української еліти більш важливими є вирішення політичних питань, ніж події на Сході України;
- формування негативних суджень про воєнно-політичне керівництво України та про те, що хаотичні бойові дії призводять до невинуватених жертв, у тому числі серед мирного населення;
- поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до керівництва;
- нав'язування думки про те, що Україна не зможе прожити без російського газу тощо.

На закінчення варто навести думку німецького філософа і психолога Еріха Фромма (1900-1980), який у своїй фундаментальній праці «Анатомія людської деструктивності» (1973 року), звернув увагу на те, що людині, як істоті, важливо опиратись на певну систему моральних координат - розділяти добро і зло, щоб протистояти зовнішнім загрозам.

Коли людина чітко ідентифікує себе з певним суспільством, бачить себе частиною групи, єдиної держави, вона «обростає моральним корінням», оскільки суспільство пропонує їй певну систему координат, яка допомагає всім колективно вижити в найскладніших ситуаціях. Адже не дарма найменше піддаються маніпулюванню люди з чітко вираженою соціальною і політичною позицією, оскільки маніпулятивні дії невід'ємно співвідносяться із соціокультурною ідентичністю, освіченістю, груповою солідарністю тощо. Саме тому у виробленні колективного, загальнодержавного спротиву в умовах інформаційної війни особливе значення має система виховання і освіти, яка розвиває громадянські якості, патріотизм, любов до Батьківщини.

Авдошин І. В.
доктор юридичних наук,
старший науковий співробітник
Коваленко С. М.
старший науковий співробітник,
Національна академія СБ України

ВНУТРІШНЬО ПЕРЕМІЩЕНІ ОСОБИ – ДЕСТАБІЛІЗАЦІЙНИЙ ЧИННИК УКРАЇНСЬКО-РОСІЙСЬКОЇ «ГІБРИДНОЇ» ВІЙНИ

Вже майже сім років Україна веде затяжну опозиційну війну з одним із найбільш підступних і потужних противників у світі Росією. В результаті цієї війни в глибині українських територій опинилися сотні тисяч українських громадян, які набули статусу внутрішньо переміщених осіб. При цьому, зважаючи на незначні матеріальні і фінансові можливості української держави щодо облаштування і адаптування цих осіб до нових умов проживання, можливі ситуації коли середовище переміщених осіб, при добре організованій підривній роботі з ними може бути використане для дестабілізації внутрішньополітичної обстановки в нашій державі.

Тому необхідність захисту власної безпеки вимагає від нашої держави вжиття усіх необхідних заходів протидії внутрішнім та зовнішнім загрозам, що не суперечать міжнародним принципам і нормам. Разом з тим, до цього часу відсутні системні дослідження основних чинників і намірів (цілей) ініціаторів дестабілізації політичної системи, які можуть використовувати середовище переміщених осіб та її можливих наслідків, які б дозволили визначити ознаки, характерні для тих чи інших типів її дестабілізації. Як правило, при прийнятті державно-управлінських рішень в умовах дестабілізації політичної системи, практично не береться до уваги й важливість забезпечення для її стійкості, збалансованості та взаємоузгодження морального, юридичного та концептуального рівнів упорядкування її структурних елементів, не аналізуються фактори, які є характерними для тих чи інших рівнів соціального збурення в середовищі переміщених осіб, а також не визначені й складові комплексного підходу щодо дослідження факторів дестабілізації внутрішньополітичної системи (ситуації) в цілому.

З огляду на викладене вище, а також те, що пріоритетним завданням Служби безпеки України у сфері державної безпеки є утримання політичної системи у стані, за якого загрози національній безпеці бу-

дуть мінімізовані, актуальною науковою проблемою є визначення ознак, які б дозволили оперативним підрозділам контррозвідки запобігати дестабілізації політичної системи спровокованої соціальним збуренням серед переміщених осіб в глибині українських територій та приймати відповідні управлінські рішення. Вирішення цієї проблеми є також важливим у контексті розробки методологічних основ формування ефективної системи державного управління у сфері державної безпеки, оскільки це створює додаткові можливості для вказаної системи щодо здійснення оперативного пошуку та реалізації стратегічних державно-управлінських рішень, адекватних загрозам життєво важливим національним інтересам під час дестабілізації внутрішньополітичної ситуації в нашій державі.

У цьому контексті саме розвідувально-підбивна діяльність російських спецслужб зі створення агентурних позицій у середовищі переміщених осіб, має розглядатись як найбільш гостра форма особливо небезпечних правопорушень проти нашої держави.

Крім того, необхідно відмітити, що в діяльності російських спецслужб все активніше запроваджується практика використання акцій розвідувально-інформаційного впливу (проявляється у формах ідеологічного впливу та психологічного тиску для формування суспільнополітичної обстановки в державі або її дестабілізацію).

У сучасних умовах все частіше акції розвідувально-інформаційного впливу російські спецслужби здійснюють у військовій, політичній та економічній сферах. Таку динаміку впливу можна прослідкувати у конкретних діях Росії задовго та під час анексії українського Криму й окупації українських територій на сході нашої держави.

Тому цілком слушною є позиція науковців, що ідеологічний вплив здійснюється шляхом створення спецслужбами РФ ідейнополітичного впливу на громадян нашої країни з метою примушення їх до вчинення протиправних і суспільно небезпечних дій з ослаблення і підризу політичного і суспільного ладу своєї країни. При цьому ідеологічний вплив може здійснюватися, наприклад, шляхом руйнування стійких поглядів і переконань громадян і нав'язуванням чужої для них ідеології, вигідних для іноземної держави стереотипів мислення та поведінки, примушенням до анти суспільних, ворожих настроїв і емоцій.

До методів ідеологічного впливу відносяться також поширення тенденційної та фальсифікованої інформації, проголошення ворожих лозунгів та призивів, пряме підбурювання до вчинення антигромадських діянь.

Об'єктами ідеологічного впливу, у тому числі, є: середовище переміщених осіб стосовно якої проводиться підривна (розвідувально-підривна) діяльність. При цьому ідеологічний вплив на ті чи інші об'єкти здійснюється диференційовано, з урахуванням їх соціального і політичного положення, віку, особливостей національного характеру, релігійних поглядів тощо.

У цілому ж гібридні технології, які використовують спецслужби РФ для дестабілізації внутрішньополітичної системи (ситуації) та ініціювання соціальної кризи в нашій країні сьогодні поєднують цивілізаційний та геополітичний підходи, оскільки спрямовані на підрив політичної стабільності та цілеспрямованого генерування загроз національній безпеці.

Це в свою чергу вимагає від органів і підрозділів української контррозвідки виробити необхідні правові та організаційні форми протидії таким проявам, у тому числі, в середовищі переміщених осіб. Розробка і реалізація таких правових і організаційних форм забезпечить у подальшому передумови для формування дієвого контррозвідувального режиму на території України як структурного елемента в механізмі забезпечення державної безпеки.

Благодарний А. М.

доктор юридичних наук,
старший науковий співробітник,
Національна академія СБ України

ОСОБЛИВОСТІ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ЯК СКЛАДОВІЙ ГІБРИДНОЇ ВІЙНИ

Найчастіше гібридна війна (англ. Hybrid warfare) визначається як сукупність заздалегідь підготовлених і оперативно реалізованих державою дій військового, дипломатичного, інформаційного характеру, спрямованих на досягнення стратегічних цілей [1]. Гібридна війна – це військова стратегія, яка об'єднує звичайну війну, малу війну і кібервійну. Держава, яка веде гібридну війну, співпрацює з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок із якими формально повністю заперечується [2].

Тобто, гібридна війна – війна, яка поєднує в собі принципово різні типи і способи ведення війни, а саме: класичної війни з використанням армії та озброєння, дезінформації населення та агітації за до-

помогою співпраці з нерегулярними збройними формуваннями (повстанці, терористи, партизани), інформаційної та кібервійни [3, с. 49].

Успіх гібридної війни досягається завдяки не лише докладно розробленому плану дій, а й слушно обраному моменту для його реалізації, зокрема:

- ослаблення центральної влади та часткове «безвладдя» на тлі зміни влади;
- зростання суперечностей (актуалізація вже наявних) між центром і регіонами;
- незадовільний психологічний і матеріально-технічний стан структур безпеки;
- антагонізм між різними силовими структурами;
- активна інформаційно-пропагандистська робота протягом довгого періоду часу [4].

Хоч військовий складник конфлікту об'єктивно залишається основним чинником його розгортання, масштаби застосування інформаційного складника стають дедалі більшими [5, с. 395]. Інформаційний фронт «гібридної війни» розгортається одразу на кількох напрямках. Передусім: серед населення в зоні конфлікту; серед населення країни, проти якої здійснюється агресія, однак, територія якої не охоплена конфліктом; серед громадян країни агресора і серед міжнародного співтовариства [4].

Важливою складовою ведення такої війни є вплив на інформаційну сферу суспільства. Зокрема, прояв інформаційної агресії до населення країни, яка є об'єктом гібридної війни. Сучасна людина піддається інформаційній агресії щоденно сотні раз. Інтернет, радіо, телебачення, газети й журнали нав'язують своє розуміння життя, що завдяки своєму маніпулятивному ефекту впливає і на наш світогляд. Основна мета інформаційної агресії – це вплив не тільки на свідомість, а й на підсвідомість, щоб «скоригувати» громадську думку всередині як країни-жертви, так і країни-агресора. Все це робиться для того, щоб основна думка цієї маніпуляції залишила незгладимий слід у свідомості особи і надійно закріпилася в ній. Процеси маніпулювання масовою й індивідуальною свідомістю за допомогою засобів масової інформації, особливо електронних, шляхом інформаційної агресії набувають усе більш широкого розмаху [6, с. 171].

Загалом можна виокремити такі основні властивості інформаційної агресії:

- 1) несиловий характер (за рахунок ЗМІ);
- 2) швидкість розповсюдження;

3) пандемічність, опосередкований характер і потаємність впливу (інформаційна дія має глобальний характер й на відміну від фізичного впливу, може бути абсолютно непомітною);

4) віртуальний характер дії (крихкість інформаційного світу, легкість доступу, можливість зламу інформаційних систем) [6, с. 171].

Зазвичай інформаційна агресія відбувається у три етапи:

1. Створення ядра. З'являється досить велика кількість людей, які не сприймають стан речей, що склався, які мають цінності, несумісні з панівним світоглядом, і незадоволені своєю пасивною роллю в системі відносин, що сформувалася, причому налаштованих при цьому зовсім непримиренно. Це робиться якомога агресивніше, щоб не загубитися в навколишньому інформаційному шумі, з помітним акцентом на заперечення фактичного стану речей; альтернативу, зазвичай, окреслюють досить схематично. Ідеологи інформаційного протистояння на цьому етапі орієнтуються на тих, хто потерпає від відсутності інформації та від її нерозуміння. Найголовніше завдання цього етапу вони вбачають у тому, аби показати, що альтернатива не тільки можлива, а й неминуча, що її прихильники діють; озброїти словом і надією тих, хто цього потребує.

2. Створення середовища. Люди різних опозиційних настроїв поєднуються для того, щоб підтримувати одне одного. При цьому організовуються вони на цьому етапі не за принципом «за», а за принципом «проти». Найголовніша мета полягає в тому, щоб створити альтернативний інформаційний простір, зі своїми установками і табу, аж до рефлексів, й реалізувати відповідну інформаційну агресію, що переважає агресію супротивника.

3. Створення атмосфери. Створити певну інформаційну атмосферу, змінюючи суспільну думку спрямованими точковими ударами з різних боків. Як тільки кількість активістів і симпатиків стане достатньою для того, щоб забезпечити масованість і постійність цих ударів, щоб інформаційну битву було виграно [7].

Щоб не допустити реалізацію інформаційної агресії на території своєї країни потрібно вміти як попередити її, так і оборонятися від неї. Оскільки її метою є маніпулювання людською свідомістю і створення хаосу серед населення для полегшення керування ним, протидія цій агресії потребує також міцного інформаційного фундаменту в національній свідомості й поглядах населення.

Згідно стратегії гібридної війни та ознак і методів інформаційної агресії як її складової, можна виділити такі аспекти протидії:

1. постійний контроль інформаційного простору (преса, телебачення, радіо, інтернет);
2. недопущення створення на своїй території недержавних військових організацій для знищення людського, економічного та інфраструктурного потенціалу держави чи регіону;
3. обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією (агресія зачіпає інформаційний простір держави-жертви не цілком, а тільки його частину) [8, с. 99];
4. посилення авторитету своєї влади та уряду, армії серед населення країни, щоб перешкодити переходу на бік ворога та підтримці ідей, які він нав'язує;
5. ефективна інформаційна політика: повсякденний контекст, стратегічна спрямованість та зворотний зв'язок із суспільством [9].

Література

1. Гібридна війна: як це працює [Електронний ресурс]. – Режим доступу: <http://www.csr.org.ua>.
2. Корнієнко С. Путін веде в Україні гібридну війну [Електронний ресурс]. – Режим доступу: <http://www.radiosvoboda.org/content/article/>.
3. Організаційні аспекти протидії інформаційній агресії як складовій гібридної війни / А.М. Благодарний, О.В. Штельмах // Інформаційна безпека людини, суспільства, держави. – 2015. – № 3(19). – С. 48–54.
4. Горбулін В. “Гібридна війна” як ключовий інструмент російської геостратегії реваншу [Електронний ресурс]. – Режим доступу: <http://gazeta.dt.ua/internal/gibridna-viyna>.
5. Штельмах О. В. Організаційні аспекти протидії інформаційній агресії як складовій гібридної війни // Актуальні проблеми управління державною безпекою : зб. матер. наук-практ. конф. (Київ, 19 березня 2015 року). – К.: Центр навч., наук. та період. видань НА СБ України, 2015. – 512 с. – С. 393-396.
6. Проблема агресії і насильства: світоглядно-інформаційний вимір / В. Г. Пилипчук, О. П. Дзьобань // Український науковий журнал “Освіта регіону”. – 2012. – № 2. – С. 171–177.
7. Мироненко В. Інформаційна агресія й інформаційне протистояння [Електронний ресурс]. – Режим доступу: <http://personal.in.ua>.
8. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. пос. / В. А. Ліпкан, Максименко Ю. Є., Желіховський В. М. – К.: КНТ, 2006. – 280 с.
9. Брецько Ф. Російська гібридна війна проти України і світу [Електронний ресурс]. – Режим доступу: <http://rionews.com.ua>.

**ЗАГАЛЬНІ ЗАСАДИ ФОРМУВАННЯ ЗОН
КЕРОВАНОГО ХАОСУ У СОЦІАЛЬНИХ СИСТЕМАХ
ЗА ДОПОМОГОЮ ІНСТРУМЕНТІВ ІНДУСТРІЇ 4.0
ТА НАПРЯМКИ ПРОТИДІЇ ТАКИМ ДІЯМ**

На сьогодні основними акторами міжнародних відносин використовується концепція, яка допомагає контролювати деякі країни та регіони, тобто концепція керованого хаосу, що виникла в глибоку давнину. Зокрема, її елементи можна побачити в стратегії Римської імперії епохи завоювань Галлії, Британії, Дакії. Відомо, що римські полководці цілеспрямовано створювали військово-політичний і соціально-економічний хаос у майбутніх провінціях Риму, нацьковуючи між собою племена та їх вождів, а також позбавляючи противника ресурсів, продовольства та води [1].

В літературі можна зустріти й інші назви концепції «керованого хаосу», а саме: теорія «керованої критичності» або «м'якої сили». Тепер коротко розглянемо, що являє собою вказана теорія. Так, теорія керованого хаосу спирається, перш за все, на реально існуюче суспільне невдоволення в країні через відсутність нормальних каналів взаємодії по лінії «влада – суспільство», коли негативне самовідчуття населення викликає усвідомлений соціальний дискомфорт і нездатність влади функціонувати в колишньому режимі стає загальновизнаною в суспільстві. При цьому повинна існувати якась організаційна група, здатна впливати на внутрішньополітичний процес у цій країні. Для геополітичної експансії потрібен також певний соціальний шар або співтовариство, яке можна використовувати в якості «інкубатора революційних настроїв» (наприклад, «опозиційну інтелігенцію»). Ця спільнота повинна об'єктивно відіграти роль «п'ятої колони». Першим кроком у цьому напрямі є дискредитація, а потім і знищення традиційних цінностей нації. Для того, щоб зовнішня інформаційна агресія сприймалася масовою свідомістю безболісно, це представляється як рух по шляху прогресу. Створюються конфліктні ситуації, які незабаром переходять у збройні конфлікти, локальні війни, перевороти та «кольорові революції». Таким чином, формується хаос на певній території, в умовах якого розмивається національний суверенітет, стає незрозумілим, хто є керівником держави [1; 2].

Проаналізувавши зміст теорії керованого хаосу ми бачимо, що вона спрямована на конкретну соціальну систему. Що у свою чергу, забезпечує її найбільш ефективний вплив. Тому, доцільно зазначити, що являє собою соціальна система. Так, соціальна система – це цілісне, впорядковане соціальне утворення, єдність взаємопов'язаних інститутів, груп, організацій, спільнот, котрі, взаємодіючи, забезпечують матеріальні та нематеріальні потреби та інтереси людей [3]. Наприклад: громадяни певної країни, військовослужбовці, співробітники конкретного підприємства, студенти тощо.

Концепція керованого хаосу використовується, в основному, на рівні окремо взятої держави. Однак досвід ведення гібридної війни Російської Федерації проти України свідчить, що дана концепція може застосовуватися на регіональному рівні, частини якого становлять уже глобальний керований хаос [1]. Варто зауважити, що в ХХІ столітті відбувається перенесення агресії з військово-географічного простору в інформаційний, тобто створення зон керованого хаосу набуває значно більшого масштабу, адже цьому сприяє науково-технічний розвиток людства.

Так, одночасно із завершенням «третьої промислової революції», яка характеризується розвитком інформаційно-комунікаційних технологій, частковою автоматизацією та роботизацією виробничих процесів, розпочалася «четверта промислова революція». У свою чергу, остання передбачає повністю автоматизовані виробництва, на яких керівництво всіма процесами здійснюється в режимі реального часу і з урахуванням мінливих зовнішніх умов. Кіберфізичні системи створюють віртуальні копії об'єктів фізичного світу, контролюють фізичні процеси і приймають децентралізовані рішення. Вони здатні об'єднуватися в одну мережу, взаємодіяти в режимі реального часу, самоналагоджуватися і самонавчатися. Важливу роль відіграють інтернет-технології, що забезпечують комунікації між персоналом та машинами [4]. Цей процес отримав назву «Індустрія 4.0». Внаслідок, створення нових кіберсистем та штучного інтелекту виникають й нові інструменти за допомогою, яких можна створювати «зони керованого хаосу».

Зони керованого хаосу у соціальних системах створюються за допомогою інструментів Індустрії 4.0 за наступними методами:

1. поширення дезінформації або викривлення інформації;
2. створення програмного забезпечення з вмонтованою відслідковуючою системою;

3. проведення соціологічних та політичних опитувань за допомогою Інтернет-ресурсів, внаслідок чого стає відоме позитивне ставлення населення до конкретного явища, події, персони тощо;

4. відслідковування дій інтернет-користувачі з метою виявлення їхнього прихильного ставлення;

5. проведення кібератак та впровадження вірусів в державні інформаційно-телекомунікаційні системи задля паралічу державної діяльності.

Знаючи, якими методами та інструментами створюють зони керованого хаосу можна виокремити загальні засади їх формування. Тобто, те заради чого вони безпосередньо створені. Відповідно, до загальних засад формування зон керованого хаосу відносять:

1. створення військово-політичної та соціально-економічної дестабілізації;

2. дискредитація, а згодом і знищення традиційних цінностей нації;

3. дискредитація керівництва країни і його політики;

4. здобуття панівної позиції й потужного впливу на адміністративну та інтелектуальну еліти держави, проникнення в ЗМІ і встановлення контролю над ними;

5. надання зовнішній інформаційній агресії ярлика руху по шляху прогресу;

6. створення конфліктних ситуацій, які незабаром переходять у збройні конфлікти, війни;

7. розмиття національного суверенітету.

Необхідно зауважити, що керований хаос, як система показує тонку залежність від початкових умов, тобто невеликі зміни будь-яких умов на вході призведуть до масштабних відхилень на виході.

Задля недопущення створення зон керованого хаосу необхідно протидіяти поширенню дезінформації через ЗМІ та Інтернет, адже, як наслідок відбувається дискредитація традиційних цінностей нації, керівництва країни і його політики тощо. Так, наприклад, у державах-членах ЄС діє механізм боротьби з дезінформацією за допомогою штучного інтелекту. Литовські програмісти навчили штучний інтелект шукати фейки в Інтернеті. В основі технології знаходяться комп'ютерні алгоритми здатні здійснювати пошук в контенті певних меседжів та наративів. Ця система щодня проводить моніторинг більше ніж 10 тисяч матеріалів з 500 литовських та російських Інтернет-доменів. Дана технологія потребує допомоги людей лише для перевірки матеріалів котрі відібрані штучним інтелектом [5].

Також, необхідно інформувати населення про застосування теорії керованого хаосу агресором. Потрібно унеможливлювати формування мережі агентів впливу для організації хаосу й наступного перехоплення управління країною. Лобіювання традиційних цінностей нації та збереження її історії. Підтримання вітчизняної науки і освіти. Посилення авторитету керівництва країни серед населення та зворотний зв'язок із ним. Також, проведення інформаційних кампаній для підвищення рівня патріотичності громадян.

Література

1. Рябінін Є. Концепція керованого хаосу в контексті побудови сучасного світового порядку / Є. Рябінін // Зовнішні справи. - 2013. - № 11. - С. 32-37. - Режим доступу: http://nbuv.gov.ua/UJRN/zovsp_2013_11_11 (дата звернення 07.06.2021).
2. Сенченко О. Інформаційно-мережеві війни: феномен «керованого хаосу» / О. Сенченко // Вісник Книжкової палати. - 2017. - № 4. - С. 31-37. - Режим доступу: http://nbuv.gov.ua/UJRN/vkp_2017_4_8 (дата звернення 07.06.2021).
3. Соціальна система. URL: <https://cutt.ly/cnTtdCX> (дата звернення 08.06.2021).
4. Індустрія 4.0. URL: <https://www.it.ua/knowledge-base/technology-innovation/industry-4> (дата звернення 08.06.2021).
5. Литва закликала партнерів по ЄС посилити боротьбу з російською пропагандою. URL : <https://www.dw.com/uk> (дата звернення 09.06.2021).

Герман Л. В.

кандидат психологічних наук,
старший науковий співробітник,
Національна академія СБ України

ТЕРОРИЗМ ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ

Військова агресія Росії проти України, яка почалась у 2014 році, та стала прямим викликом міжнародному співтовариству, характеризується суттєвим відходом від традиційних форм і способів ведення війни. На сьогодні спостерігається суттєва ескалація терористичної діяльності на Сході України, адже подібні дії можуть нанести значно сильнішого удару ніж масштабне військове вторгнення.

Варто зазначити, що використання терористичних актів з метою зміни соціально-політичної або економічної ситуації в країні явище досить розповсюджене у світовій історії. Протягом всього свого існу-

вання людство стикалось з явищем тероризму у різних формах і проявах. З моменту зародження людської цивілізації правляча верхівка застосовувала фізичне насилля та морально-психологічне залякування для досягнення своїх цілей.

Для результативної боротьби з терористичною загрозою необхідне всебічне та системне дослідження природи тероризму, причин його виникнення, закономірностей розвитку тощо. Будь-яке явище не виникає саме по собі, поза навикишньою дійсністю, а навпаки – пов'язане з нею, породжене конкретними чинниками й обставинами, тобто детермінантами (причинами, умовами, корелятами), взаємозалежними, інтегрованими в утворення більш складного рівня організації.

Причини терору криються у зростанні кризових явищ в економіці, нездатності суспільства регулювати складні соціально-політичні процеси, швидкій зміні системи загально людських цінностей та ідеалів.

Ще Карл Маркс у своїх працях наголошував, що суспільство не може існувати без конфлікту. Ця думка знайшла своє відображення у роботах ряду[1,2,3] науковців, які вважають, що в умовах індустріального та постіндустріального суспільства основний конфлікт виникає тоді, коли йдеться про перерозподіл влади. З метою отримання, утримання або поліпшення позицій певних соціальних груп, які ведуть боротьбу за владу, зіткнення інтересів неодмінно призводить до масштабних соціальних конфліктів. Тому прояви тероризму є логічним продовженням такої конфронтації.

Відомий політолог та соціальний психолог Д.В. Ольшанський [2] зосереджує увагу на основній ознаці тероризму, розглядаючи його, як *своєрідний вид діяльності із застосуванням насилля, особливістю якої є висока емоційна напруженість*, що визначається високим ступенем ризику, як для суб'єктів, так і для об'єктів, на яких спрямовані ці дії. Адже, зазвичай, виконавці терористичних актів знаходяться під дією сильних емоцій та почуттів (гнів, ненависть, лют, несамовитість). В той час, як у жертв насилля виникають протилежні емоційні реакції: горе, страх, паніка, жах, відчай тощо. На думку дослідника, головною метою терористів є відповідний емоційний стан їх жертв, який досягається в тому випадку, коли жертва вірить у реальність небезпеки, яка їй загрожує. Тому загроза здійснення терористичного акту повинна чергуватись з його реалізацією. На цьому постулаті базується запропонований ним *психологічний механізм тероризму*: для формування переконаності населення у реальності терористичної загрози, яка може бути застосована до будь-кого, терористи регулярно та систематично застосовують насильницькі дії, які різняться за масштабом, об'єктами, часовими проміжками тощо. Як наслідок, вини-

кає масова загроза стабільності та безпеці, за рахунок чого швидко розповсюджується атмосфера паніки і жаху серед населення, що паралізує волю та здатність до спротиву, та викликає певну трансформацію свідомості суспільства.

Зауважимо, що більшість дослідників притримуються згоди в тому, що будь-який акт насилля може називатись терористичним, лише в тому випадку, якщо він здійснений для залякування.

Терористичні дії не тільки наносять шкоду людям, які потрапили в зону терористичної агресії, а й впливають на психіку широкого кола інших осіб, які стали свідками зазначеного чи просто отримали відповідну інформацію. У таких осіб формується почуття незахищеності, високий рівень тривожності та інші негативні психоемоційні стани, відбуваються дестабілізація нормального перебігу життєдіяльності. Такі наслідки тероризму дозволяють стверджувати, що його метою виступає залякування, привернення уваги громадськості, провокування до певних дій чи бездіяльності, тобто, здійснення психологічного впливу на якомога більшу аудиторію.

Підсумовуючи все вищезазначене, можемо зробити висновки, що:

- кожен терористичний акт спрямований передусім не на фізичне знищення, а на залякування всіх осіб, які не згодні з терористами;
- головною метою будь-якої терористичної акції є не саме нанесення матеріальної та фізичної шкоди, а, в першу чергу, психологічний тиск, який повинен посіяти паніку та страх у свого супротивника, в ролі якого можуть виступати певні соціальні групи, верстви населення, окремі державні інститути або держава в цілому;
- ефективна боротьба із явищем тероризму неможлива без глибокого вивчення його психологічної складової.

Література

1. Горбунов К.Г. Терроризм: социально-психологическое исследование: монография / К.Г. Горбунов. – Омск: Изд-во Ом. гос. ун-та, 2010. – 384 с.
2. Ольшанский Д.В. Психология терроризма / Д.В. Ольшанский. – СПб.: Питер, 2002. – 288 с.
3. Терроризм: теоретико-прикладні аспекти: навч. посіб. / кол. авторів; за заг. ред. проф. В.К. Грищука. – Львів: ЛьвДУВС, 2011. – 328 с.

КОНЦЕПЦІЯ «ГІБРИДНОЇ ВІЙНИ» ТА РОЛЬ СПЕЦІАЛЬНИХ СЛУЖБ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ У ЇЇ РЕАЛІЗАЦІЇ ЩОДО УКРАЇНИ

Під впливом російсько-українсько конфлікту, який розпочався у 2014 році, серед військових експертів та науковців набула поширення концепція «гібридної війни», якою вони намагаються пояснити всі особливості вказаного конфлікту.

Слід зазначити, що дискусії щодо нових типів війни, трансформації самого поняття «війна», її суті та особливостей серед фахівців ведуться щонайменше останні десятиріччя. Це викликано декількома чинниками:

- наявність нових потужних видів зброї (в т. ч. масового знищення), що робить класичні війни вкрай небезпечними, як для самого агресора, так і для всього світу. Адже це призведе до масових жертв серед мирного населення, з'являться масштабні потоки біженців, руйнуватимуться транспортні та промислові інфраструктури (включно з критично-небезпечними ядерними та хімічними об'єктами), розірвуться існуючі торгівельно-економічні зв'язки тощо;

- бажання агресора применшити свою роль у розв'язанні конфліктів задля уникнення санкцій з боку інших країн та міжнародних організацій, а також для недопущення втрати свого авторитету та позицій на світовій арені;

- намагання країн-агресорів встановити свій контроль над об'єктами агресії (в т. ч. інтегрувати їх до своїх політичних, економічних та безпекових систем) без надмірних для них збитків, що можуть зашкодити нападникам у реалізації власних геополітичних та економічних інтересів;

- на полі бою в сучасному збройному конфлікті поряд з регулярними військами з'являється безліч нових дійових осіб – іррегулярні формування повстанців і бойовиків, кримінальні банди, міжнародні терористичні мережі, приватні військо-промислові компанії та легіони іноземних найманців, підрозділи спецслужб різних країн світу, а також військові контингенти міжнародних організацій.

Концептуальним обґрунтуванням нового типу війни протягом ХХІ ст. займалися, насамперед, американські військові теоретики

Р. Глен, Дж. Гордон, Д. Кілкаллен, Дж. Маккуен, Дж. Маттіс, Дж. Мацумура, У. Немет, Е. Сімпсон, Р. Уїлкі, Н. Фрейєр, Ф. Гофман, норвезький фахівець Г. Карлсен, нідерландський – Франк ван Каппен та ін.

Новий тип збройного конфлікту не отримав загальновизнаного визначення та усталеного поняття. Для характеристики нового типу збройних конфліктів застосовуються такі поняття, як «неконвенційна війна» (*unconventional warfare*), «нерегулярна (нестандартна) війна» (*irregular warfare*), «змішана війна» (*compound warfare*), нелінійна війна (*non-linear war*), гібридна війна (*hybrid warfare*) тощо. Незалежно від використаних дефініцій, головною особливістю війни відзначається домінування невійськових компонентів при вирішенні військових завдань.

У квітні 2014 року колишній радник НАТО з питань безпеки генерал-майор Франк ван Каппен одним з перших серед західних аналітиків заявив, що «Путін веде в Україні гібридну війну». З того часу в західних та вітчизняних дослідженнях новий тип війни, з яким зіштовхнулася Україна та світ у 2014-му, все частіше називають «гібридною війною» (*hybrid warfare*). Вочевидь, термін «гібридна війна» є найбільш адекватним визначенням одного з різновидів більш широкого поняття війни нового покоління та найбільш повно відображає особливості даного явища - широке застосування політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів для досягнення політичних та військових цілей.

Особливістю нового типу війни є:

- активна роль невоєнних засобів у досягненні політичних та стратегічних цілей, які за своєю ефективністю переважають силу зброї;
- зникає різниця між станом війни та миру;
- противник намагається сформувати союзників із числа місцевого населення, які прихильні до сепаратистських ідей або в яких преvalюють матеріальні інтереси;
- противник не оголошує про стан війни та приховує наявність своїх військ на окупованій території;
- активно використовується внутрішня опозиція для послаблення супротивника та маніпулювання транснаціональними фінансовими можливостями (комерційними зв'язками з провідними західними компаніями);
- масштабне використання методів та засобів інформаційної війни, в т. ч. з використанням світових ЗМІ;

- зростання ролі спеціальних служб у підготовці та реалізації технологій «гібридних війн».

Специфіка засобів “гібридної” війни суттєво підвищує **роль і значущість спеціальних служб** у її веденні. У певному сенсі «гібридну» війну в тій формі, яку вона має в Україні, можна розглядати як низку заздалегідь підготовлених послідовних таємних операцій, підпорядкованих єдиній логіці та поєднаних єдиним задумом. Вони включали у себе багаторічну підготовчу роботу російських спецслужб як на територіях майбутнього вторгнення, так і серед українських владних та силових структур, що включало вербування командного складу Збройних Сил, органів внутрішніх справ, СБУ, прикордонної служби, продуману систему інформаційно-психологічної обробки населення південно-східних регіонів, введення своєї прямої агентури та агентів впливу в середовище політичних партій, релігійних конфесій, а також націонал-демократичних та націоналістичних рухів, скупку існуючих та створення нових інформаційних ресурсів з російським капіталом і т.п.

Таким чином, саме на спеціальні служби РФ було покладено завдання із планування, організації та реалізації комплексу заходів щодо створення необхідних умов (політичних, економічних, ідеологічних тощо) в країні – об’єкті агресії на підготовчому, «довоєнному» етапі. Провідною залишається їх роль і протягом активної фази гібридної війни.

Кузьменко В. В.

Сидоренко С. М.

Національна академія СБ України

АНТИУКРАЇНСЬКІ МІФИ В ІНФОРМАЦІЙНІЙ ВІЙНІ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Однією з ключових складових інформаційної війни Російської Федерації проти України є поширення фейків, симулякрів та міфів, що становить загрозу національній безпеці та використовується спецслужбами Російської Федерації в якості елементів «гібридної війни» проти України.

Найчастіше поширювані з них:

- міф Російської Федерації про те, що росіяни і українці – одна нація;
- про те, що Україна – держава, яка не відбулася;
- про історичну приналежність Криму Росії;

- про те, що Україна – суцільна «Чорнобильська зона»;
- про неканонічність Православної Церкви України;
- про порушення в Україні прав російськомовного населення;
- про непричетність Росії до погіршення відносин з Україною;
- про громадянську війну на сході України;
- про зрив Україною Мінських домовленостей;
- про непереможність російської армії;
- про відсутність військової техніки і військовослужбовців Російської Федерації на, тимчасово неконтрольованій Україною, території Донбасу.

Ці міфи є базовими у свідомості не тільки російських політичних еліт, а й пересічних росіян, а також значної частини європейців.

Певною мірою це результат візії нашої держави Заходом. І ґрунтується він на міфологічних уявленнях про Україну, спровокованих як російськими політтехнологами, так і російським істеблішментом.

Найбільш активним, агресивним та неправдивим антиукраїнським пропагандистом є президент Російської Федерації Володимир Путін. Саме він задає тон у формуванні та впертому просуванні антиукраїнських міфів в інформаційний простір Росії, України та інших держав.

В тому числі, і завдяки їм, вдається згуртувати більшість російського населення навколо кремлівського керівництва, яке заради міфічної імперської величі, практично не зважає на зниження свого життєвого рівня та згортання демократичних свобод, в умовах вигаданої загрози Росії з боку України.

Одночасно, основний російський іміджмейкер намагається посіяти недовіру та розбрат серед українців, надломити нашу волю до опору російській агресії, послабити солідарність з Україною світової спільноти.

Як приклад, одного з найбільш часто повторюваних міфів російської пропаганди, є твердження В. Путіна, що українці та росіяни – один народ. Тезу було спростовано ще на початку минулого століття. І сьогодні, за умов існування розвиненої української мови, культури, державності, після ґрунтовного дослідження джерел реанімації цього антинаукового міфу, воно виглядає взагалі безглуздо [2].

Інший приклад. Російська пропаганда постійно доводить, що Україна – «штучна» країна, створена Володимиром Леніним та його прибічниками, монументи яким, «невдячні» українці знищують у рамках процесу декомунізації. Хоча твердження спростоване як у самій

Росії, так і за кордоном, російський президент у своїх виступах вперто тримається саме цієї точки зору.

Наступний приклад антиукраїнської міфологізації. Фахові пропагандисти російських медіа, блогери, російські автори коментарів на сайтах невпинно звинувачують українців у «відреченні» та «зраді слов'янської єдності». При цьому відбувається підміна понять, яку переважна частина росіян не помічає – еталоном і «слов'янства», і «православності» за умовчанням проголошуються росіяни.

Таким чином, практично усі сучасні російські міфи про Україну є не тільки неправдивими, а й шкідливими, що не заважає більшості росіян вірити в них.

Це пояснюється як загальною запрограмованістю російської масової свідомості на міфологізоване сприйняття оточуючого світу і місце своєї країни у ньому, так і особливою увагою, яку могутня російська пропагандистська машина приділяє створенню, поширенню та закріпленню у свідомості своїх громадян міфів про міжнародне оточення Росії загалом і Україну, зокрема.

Куцій М. С.

Національна академія СБ України

ФЕНОМЕН WAR WEARY ЯК СТАН ЕЛЕМЕНТІВ ГІБРИДНОЇ ВІЙНИ

Активне застосування інформаційно-телекомунікаційних технологій в сучасній бойовій обстановці надає збройному конфлікту нові властивості за рахунок з'явлення воєнних операцій принципово нового типу. Метою їх проведення є інформаційне руйнування соціально важливих сфер об'єкта нападу – суміжної держави через інформаційно-психологічний тиск на особовий склад її збройних сил та населення для надлому (зламання) їх волі ще до застосування військовими зброї.

Передусім залежно від реального стану інформаційно-технологічних факторів на суміжній території здійснюється трансформування війни у нові форми за рахунок поширення кола її суб'єктів, комбінування їх сил та зміни співвідношення застосованих збройних або незбройних засобів у насильницьких діях.

На думку британських дослідників, використання воєнного чи невоєнного інструментарію в інтегрованій кампанії, спрямованій на досягнення несподіваності, захоплення ініціативи, отримання переваг

у дипломатичних діях; масштабні й стрімкі інформаційні, електронні та кібероперації; прикриття та приховування військових і розвідувальних дій із поєднанням з економічним тиском і є *гібридною війною* [1].

Задіяння у конфлікті приватних воєнних компаній, наприклад, Wagner group, рекрутство до незаконних військових формувань криміналітету є характерною рисою найманців як одного із суб'єктів гібридної війни, які за рахунок безкарності і можливості застосовувати сучасні технології ураження людей та інфраструктури посилюють на окупованих територіях терористичну загрозу. Вони не уявляють себе у мирному житті, тому серед них панує незацікавленість у завершенні збройного конфлікту.

Цей конфлікт обирає обриси невизначеності й непередбачуваності та, як процес, поступово втрачає керованість з боку очільників квазідержави. На збій її системи управління впливають дії у кіберпросторі через дезінформування та інтернет-тролінг – розміщення в інтернеті та у соціальних мережах, групах новин, у вікі-проектах провокаційних повідомлень із метою викликати т. зв. флейм, конфлікти між учасниками, образи, війну правок, марнослів'я, що спрямовується сепаратистськими осередками проти законної влади. При цьому зовнішні сили використовують проблеми світоглядних орієнтацій різних прошарків населення з метою викликання їх протистояння на релігійному, національному, ідеологічному чи іншому соціальному підґрунті, але внаслідок тривалості конфлікту цей чинник як стан елементів гібридної війни стає повністю вичерпаним, близьким до виснаження або «пригніченим війною» – (англ. war weary) [2].

Необхідність врахування феномену war weary в оперативній діяльності викликана його впливом на непередбачувані елементи гібридної війни унаслідок її різноманітності, достатньої тривалості й невизначеності та широкого кола втягнутих у воєнний конфлікт осіб.

Разом із людським фактором необхідно приділити увагу перегляду або заміні окремих складових ідеологічних концепцій, що визначають мету, завдання, методи і прийоми протидії веденню гібридної війни проти нашої держави.

«Пригнічення війною» як соціальне явище впливає на учасників воєнних і невоєнних форм ведення боротьби та з часом приводить до застарілості технічних засобів її ведення.

За своєю природою явище war weary притаманне кожній стороні конфлікту. Його неможливо повністю припинити або усунути, але на деякий час доступно призупинити настання його негативного впливу на захисників вітчизни.

Література

1. The Military Balance-2015. Editor's Introduction. [Електронний ресурс]. – Режим доступу <https://www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2015-5ea6/mb2015-00b-foreword-eff4> (дата звернення: 17.08.2021).
2. Словник Рейдом Хауз, Інк. 2017. [Електронний ресурс]. – Режим доступу : <http://www.dictionary.com/browse/war-weary> (дата звернення: 17.08.2021).

Липний С. І.

Шепета О. В.

кандидат юридичних наук, доцент,
Національна академія СБ України

ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ: ПРИКЛАДНІ ТА НАУКОВІ АСПЕКТИ

Актуальним завданням для багатьох країн, в тому числі і України, є переоцінка своїх власних зовнішніх та внутрішніх пріоритетів, що зумовлено необхідністю забезпечення національної безпеки в умовах різкого загострення безпекової ситуації в світі.

Стаття 1 Закону України «Про національну безпеку України» визначає загрози національній безпеці України як явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [4].

Стратегічні документи в галузі безпеки та оборони визначені в статті 3 Закону України «Про національну безпеку України» [4]. Так, зокрема, про загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони йде мова у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України [4].

Основним документом щодо національної безпеки є Стратегія національної безпеки України. В цьому стратегічному документі визначені основні напрями державної політики у сфері національної безпеки. Стратегія визначає поточні та прогнозовані загрози націона-

льній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов. Зазначається, зокрема, що Російська Федерація як держава-агресор залишається джерелом довгострокових системних загроз національній безпеці України [7].

Основним джерелом загроз національній безпеці України є і впродовж найближчих років залишатиметься обраний керівництвом Росії курс на закріплення за Росією статусу глобального гравця та визнання так званих «російських інтересів», зроблено фахівцями Служби зовнішньої розвідки України [1]. В інформаційному бюлетені Служби зовнішньої розвідки України «Біла книга» зазначається, що Росія гнучко змінює тактику дій на українському напрямі, проте стратегічна мета залишається незмінною – не допустити успішної західно-орієнтованої України [1]. Гарантією національної безпеки держави в умовах зростання гібридних загроз є забезпечення високого рівня політичної, військової, інформаційної та економічної безпеки.

25 березня 2021 року Президент України своїм Указом № 121/2021 затвердив рішення Ради національної безпеки і оборони України «Про Стратегію воєнної безпеки України». Таким чином, один із головних документів системи планування в сфері національної безпеки і оборони введено в дію. Фактично вперше в Україні підготовлено такий стратегічний документ, який передбачає запровадження комплексного всеосяжного підходу до оборони України в умовах воєнної загрози національній безпеці, пов'язаної з використанням гібридних методів. Положення Стратегії воєнної безпеки України ґрунтуються на тому, що захист суверенітету і територіальної цілісності України є найважливішою функцією держави, справою всього українського народу [5]. Зазначається, що реалізація цієї норми Конституції України в умовах екзистенційної воєнної загрози національній безпеці, зростання дефіциту фінансових ресурсів та дисбалансу воєнних потенціалів України та Російської Федерації обумовлює необхідність розроблення нової стратегії воєнної безпеки, яка базується на всеохоплюючій обороні України [6].

«Гібридна» агресія Росії розглядається військовими фахівцями різних країн як така, що має глобальний характер. А точкою відліку для формування «гібридного» світоустрою стала агресія РФ проти України, яка спричинила руйнівні наслідки для європейської та глобальної безпеки. На думку експертів, Україні необхідно формувати комплексні стратегічні підходи у протидії російській «гібридній» аг-

ресії, створювати гнучкі та ефективні механізми реагування та протистоянням загрозам [2].

Для успішного протистояння гібридній агресії Росії вкрай необхідне перш за все, внутрішнє зміцнення держави. Цього можна досягти шляхом вдосконалення демократичного врядування, нормативно-правової бази та системи політичних і спеціальних інститутів забезпечення безпеки; подолання корупції і забезпечення умов для функціонування організацій громадянського суспільства. Необхідне проведення збалансованої міжетнічної і міжконфесійної політики, широке інформування суспільства про чутливі теми, в тому числі історичні, які використовуються, або можуть використовуватись агресором для досягнення своїх цілей. Такий комплексний всеохоплюючий підхід дозволить консолідувати суспільство і забезпечити його безпеку, може стати зразком для інших країн, які потерпають від гібридних загроз [3].

Література

1. «Біла книга» Служби зовнішньої розвідки України [Електронний ресурс] // Служба зовнішньої розвідки України : [офіційний веб портал]. – Режим доступу: <https://bit.ly/3fQ5uyn>.
2. «Гібридна» війна Росії – виклик і загроза для Європи. Київ, грудень 2016 р. - С. 88[Електронний ресурс] – Режим доступу: <https://bit.ly/3ppWeBd>.
3. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства[Електронний ресурс] – Режим доступу: <https://bit.ly/3ik9IwV>.
4. Закон України «Про національну безпеку України» [Електронний ресурс] // Верховна Рада України : [офіційний веб портал]. – Режим доступу: <https://bit.ly/3z4i4yW>.
5. Конституція України [Електронний ресурс] // Верховна Рада України : [офіційний веб портал]. – Режим доступу: <https://bit.ly/3fSpI7K>.
6. Стратегія воєнної безпеки України [Електронний ресурс] // Верховна Рада України : [офіційний веб портал]. – Режим доступу: <https://bit.ly/3chpS6s>.
7. Стратегія національної безпеки України[Електронний ресурс] // Верховна Рада України : [офіційний веб портал]. – Режим доступу: <https://bit.ly/3pnHAL1>.

ЄВРОПЕЙСЬКИЙ ВЕКТОР ЕКОНОМІЧНОЇ ЕКСПАНСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В ГІБРИДНІЙ ВІЙНІ ПРОТИ УКРАЇНИ

Характерною особливістю ХХІ століття стало переважне використання окремими країнами для досягнення політичних цілей і вирішення міждержавних суперечностей різноманітних форм і методів боротьби, що узагальнено мають назву «гібридні війни».

Механізми такої війни вже не перше десятиліття широко використовує Російська Федерація, зокрема, і проти України, у тому числі в економічній сфері. Так, саме Росія була ініціатором низки торговельних конфліктів з Україною (газових, трубних, м'ясних, молочних, сирних, кондитерських тощо), наслідком яких стало призупинення постачання газу в Україну, спеціальні антидемпінгові розслідування та накладання імпорتنих мит на українські товари у період 2002-2013 років.

Однією з передумов посилення гібридної війни РФ проти Україні в економічній сфері є залежність значної частини Європейського Союзу від поставок російських енергоносіїв.

8 вересня 2005 року глави урядів ФРН та РФ підписали спільну декларацію про наміри побудувати газопровід на дні Балтійського моря. Російську Федерацію це звільняло від плати за транзит через територію України, Білорусі, Польщі та країн Балтії та певного врахування інтересів цих країн, для Німеччини перевагою було гарантоване постачання енергетичного ресурсу.

За канцлерства Ангели Меркель проєкт було реалізовано і розширено. За використання першого потоку з 2011 року щорічно транспортується 55 мільярдів метрів кубічних природного газу з Росії до Європи. У червні 2015 року, незважаючи на анексію Росією Криму і вторгнення на Схід України, на зростання загрози санкцій з боку США, було закладено правові основи для реалізації «Північного потоку-2» (1224 кілометри від російського Выборгу до німецького Грайфсвальда). «Північний потік-2» почали споруджувати у 2018 році і після запланованого завершення у серпні поточного року його експлуатація дозволить подвоїти обсяги експортованого газу. До того ж німецькі компанії отримали економічні вигоди від співпраці з «Газпромом».

Якщо для Німеччини «Північний потік-2» в цілому є позитивним економічним проектом, то для України його завершення зумовить появу нових загроз економічній безпеці. Україна втратить не лише частину доходів від транзиту газу. Росія зможе висувати нові умови для збереження транзиту через Україну – від не вигідних обсягів і цін закупівлі російського газу до зростання обсягів зовнішньоторговельного обороту для забезпечення критичного імпорту, зокрема, титану.

Одним із характерних проявів гібридного характеру війни є поступовість розриву торговельних відносин. За даними Державної служби статистики України Російська Федерація і досі залишається серед основних торговельних партнерів України – питома вага РФ у зовнішньоторговельному обороті товарів і послуг України у 2020 році становила 8,5% [1].

За даними Державної митної служби України РФ увійшла до п'ятірки країн, з якими Україна має найбільші обсяги товарообігу – 6,3% [2].

До негативних наслідків «Північного потоку-2» для нашої країни слід віднести не тільки економічні. Реалізований Російською Федерацією геополітичний проект посилює її вплив на Європейський Союз. Складно не поділяти думку польського міністра Збігнева Рау щодо наслідків завершення проекту «Північний потік-2»: величезний дефіцит безпеки для всього східного флангу НАТО і вакуум безпеки для України. Саме Україна, як жертва російської агресії, повинна отримувати високу компенсацію як у формі політичної підтримки, так і збільшення свого оборонного потенціалу [3].

В умовах гібридної війни Росії проти нашої країни, для України особливо важливим завданням є вибір стратегічних партнерів і союзників, спираючись на допомогу яких можна забезпечити успішну протидію агресії Кремля. Для виживання і тим більше перемоги нашої країни у довгостроковій гібридній війні Україна «повинна посилювати безпекові та оборонні спроможності, забезпечувати для цього розвиток економіки та залучати допомогу міжнародного співтовариства. Як слабша сторона конфлікту Україна максимально зацікавлена у його інтернаціоналізації» [4, с. 48].

Але, приймаючи підтримку країн-партнерів, Україна повинна, насамперед, орієнтуватися на власні сили у всіх сферах забезпечення національної безпеки.

Література

1. Зовнішня торгівля України товарами та послугами у 2020 році. URL: <https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=76438c62-5e54-4931-ad98-7fe59d004a2a&title=ZovnishniaTorgivliaUkrainiTovaramiTaPoslugamiU2020-Rotsi&isSpecial=true> (дата звернення 06.07.2021).
2. Товарообіг України за I кв. 2021 року. URL: [https://customs.gov.ua/news/zagalne-20/post/tovaroobig-ukrayini-za-i-kv-2021-roku-sklav-288-mlrd-458#:~:text=\(дата звернення 06.07.2021\).](https://customs.gov.ua/news/zagalne-20/post/tovaroobig-ukrayini-za-i-kv-2021-roku-sklav-288-mlrd-458#:~:text=(дата звернення 06.07.2021).)
3. Article by Minister Zbigniew Rau in the Frankfurter Allgemeine Zeitung. URL : <https://www.gov.pl/web/diplomacy/article-by-minister-zbigniew-rau-in-the-frankfurter-allgemeine-zeitung> (дата звернення 06.07.2021).
4. Литвиненко О. Тотальна війна по-путінські: «гібридна» війна РФ проти України. «Гібридна» війна Росії – виклик і загроза для Європи. С. 45-48. URL: <https://razumkov.org.ua › GIBRID-WAR-FINAL-1-1>. (дата звернення 06.07.2021).

Мамченко С. М.

доктор педагогічних наук, професор,
Національна академія СБ України

СТІЙКІСТЬ ДЕРЖАВНОЇ СИСТЕМИ ЯК ЧИННИК ПРОТИДІЇ ГІБРИДНІЙ ВІЙНИ

Важливою характеристикою міждержавних стосунків у ХХІ столітті є протиборство різних країн. Враховуючи глобалізацію, котру розуміємо як перманентну взаємодію країн між собою у різних визначальних сферах їх життєдіяльності – економічній, фінансовій, політичній, військовій та ін., держави, з одного боку, мають шукати можливості для співпраці, взаємного розвитку, врахування інтересів партнерів, проте, з іншого боку, нікуди не зникли суперечності, відмінності в концептах розвою, потенціях, ресурсах для задоволення власних потреб та інтересів. Слід також зважати на наявність у низки країн зброї масового знищення, що накладає додаткові обмеження стосовно розв'язання конфліктів, у тому числі й силових.

Зрозуміло, що досвід першої та другої світових воєн показав жахливу ціну силового протистояння – мільйони загиблих, руйнація держав та територій, падіння моралі та психологічні травми націй. Усе це не могло не зумовити потребу пошуку нових концептуальних засад розв'язання прямих і латентних конфліктів між державами та їх військово-політичними блоками.

Поразка Радянського Союзу у холодній війні без прямих військових дій, без розв'язування третьої світової війни у гарячій фазі продемонстрував можливість вирішення конфліктів зі значним руйнівним потенціалом у відносно мирний спосіб. Такий приклад спонукав до розробки нових моделей, заснованих на так званій «м'якій силі», або «смайт-війні». Поняття смайт-війни включає концепцію вирішення конфліктів без силової фази або максимально коротке силове протистояння на завершальному етапі, коли потрібен лише один останній поштовх, і противник впаде, виснажений іншими зовні неагресивними діями, які не пов'язані із безпосереднім застосуванням сили. Таким чином, противник виснажується через неефективне використання сил та засобів, ресурсів. Відбувається своєрідне розхитування противника, як, наприклад, під час тенісної партії, коли один спортсмен постійно посиляє м'ячик у різні кути корту, що швидко виснажує суперника, котрий врешті-решт програє, хоча б і мав ліпшу підготовку.

Ця концепція може бути втілена лише за умови поділу основного задуму на сукупність задумів нижчого рівня, реалізація яких дає змогу досягти основної мети. При цьому йдеться про заглиблення не тільки на перший рівень фрагментації. Даний підхід проводиться й далі, сягаючи глибших рівнів. Слід також зазначити, що при реалізації можливо активувати дії з різних гілок фрагментації, які, на перший погляд, не поєднуються, але за результатом наближають досягнення основної мети. Такий своєрідний оксиморон розглядається як гібридне застосування, гібридні загрози й гібридні війни.

Саме у цьому, на нашу думку, полягає зміст концепту «гібридна війна», яка проводиться Російською Федерацією останніми роками проти України та інших країн, що їх РФ включає до кола своїх геополітичних інтересів.

Звісно, підґрунтям доктрини «гібридна війна» є теорія й відповідна практики державного управління, без якого проведення гібридних акцій не здійсненне. Розробка необхідного для успіху механізму державного управління можлива в суспільстві, інтегрованим усвідомленням єдиної мети існування країни та потребою захисту цінностей, інтересів держави, суспільства й людини. В умовах же нерозвинутої самоорганізації суспільства це призводить до формування авторитарного режиму.

Виникають запитання. А що ж може протистояти такій політиці та методам досягнення поставленої мети на які працює весь державний механізм? Що слід покласти у фундамент системи захисту, розрахованої на певні загрози, які досить швидко виникають, породжені комбінаціями декомпільованих раніше чинників загроз?

Концепція захисту в цьому разі не може забезпечити вирішення вказаної проблеми. Причина полягає у самому розумінні поняття захисту, який завжди орієнтований на конкретні загрози, котрі в нашому випадку мають динамічний характер та відтворюються доволі просто і швидко агресивною стороною.

Розв'язання цієї проблеми має, на наш погляд, ґрунтуватися на стійкості – показнику системи, під яким розуміємо її спроможність виконувати свою основну функцію під впливом негативних чинників. Стійкість системи включає також відновлення підсистем, зруйнованих унаслідок зловмисних атак, реалізації загроз, інцидентів тощо.

Стійкість як атрибутивна характеристика будь-якої системи дозволяє підходити до забезпечення результативного та ефективного функціонування із конкретикою розуміння відбиття атак, у тому числі й гібридних. Розгляд у цьому контексті суспільних і державних інститутів дає змогу визначати й безпекову політику системи державної безпеки. Основу такої політики становитиме критерій стійкості та надійності функціонування, що підвищить життєздатність держави, котра стала об'єктом нападу, застосування гібридних акцій завдання шкоди.

Цільова функція з орієнтацією на забезпечення стійкості дозволить оцінити рівень політики забезпечення державної безпеки та розглядати акції підриву не лінійно, а комплексно, відповідно до можливої шкоди. Цю тезу слід розуміти так, що відповідь на шкідливі інформаційні операції може полягати у протидії в інших сферах, приміром: реальне зниження напруженості у власній країні, виведення з ладу серверів розповсюджувачів негативної інформації, оперативного спростування фейків. Природно, що належить створювати нові, надвідомчі механізми управління, дійової координації дій, взаємодії та обміну інформацією між наявними в країні системами забезпечення безпеки та кризового реагування.

Світовий досвід реагування держав на пандемію Ковід-19 доводить неефективність існуючих систем забезпечення національної (державної) безпеки через непередбачуваність подібної загрози. Наслідком такої раптовості стало застосування середньовічних засобів боротьби із інфекціями, падінням рівня економіки, численні людські жертви.

Насамкінець варто зазначити, що орієнтація у безпековій політиці на поняття стійкості дозволить започаткувати новий етап реформування системи забезпечення національної безпеки України.

**СПРОБИ ВИКРИВЛЕННЯ
ІСТОРИКО-ПРАВОВОЇ РЕАЛЬНОСТІ
ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ:
ВИТОКИ ТА ШЛЯХИ ПРОТИДІЇ**

Історико-правова реальність це термін, який почав вживатися у спеціальній юридичній літературі від початку 2000-х років. Під ним історики права розуміють сукупність усіх державно-правових інститутів і явищ, розвиток яких характеризує певну історичну епоху або конкретний історичний період цієї епохи. Історико-правова реальність включає, таким чином, не тільки норми чинного законодавства, але й практику їх застосування, механізм правового регулювання, фактичний зміст правовідносин тощо.

Останнім часом історико-правова реальність, як і інші складові правової реальності, стає об'єктом гібридної війни з боку Російської Федерації, активно використовується у масштабному інформаційному впливі на українське суспільство.

Поряд з традиційними наративами російської пропаганди і намаганням експлуатувати найбільш заідеологізовані теми спільної історії, такі, наприклад, як діяльність українського національно-визвольного руху періоду 1920-х – 1950-х рр., з'являються і нові тенденції. Так, зокрема в арсеналі пропагандистської машини Кремля, яка працює на викривлення історико-правової реальності, починає використовуватись мікс історичних міфів, які були створені не тільки у радянський період, але й навіть за часів Російської імперії. Головне для агресора, щоб ці міфи виправдовували сучасну експансіоністську зовнішню політику нашого північного сусіда.

Особливо рельєфно вказана тенденція знайшла своє відображення у сумновідомій статті В. Путіна «Про історичну єдність росіян та українців». Спроба позбавлення українців власної національної ідентичності, не нова і активно використовувалась як царським режимом, так і радянською владою. У сучасних умовах вона хоч і виглядає, на перший погляд, дещо абсурдною, втім, з огляду на слабку історичну обізнаність пересічних громадян і стійкість серед певної частини суспільства радянських стереотипів, може мати значні негативні наслідки.

Ще одна міфологема, створена уже сучасною російською неімперіалістичною верхівкою, це твердження про те, що українська держава – це витвір більшовиків, які начебто по клаптиках зібрали її на споконвічних історичних землях Росії. Незважаючи на те, що зазначена теза повністю суперечить історичним фактам і надзвичайно грубо викривляє справжню історико-правову реальність, її вкидання у інформаційний простір теж є небезпечною інформаційною зброєю, спрямованою на розгойдування соціально-політичної ситуації в Україні.

Ці та інші історичні та історико-правові міфи, а таких останнім часом стає все більше, результат штучних маніпуляцій, які здійснюються з кон'юнктурною політичною метою державною владою Російської Федерації з метою деструктивного впливу на нашу країну.

Які ж шляхи протидії спробам викривлення історико-правової реальності вбачаються на теперішній час?

Насамперед, це організація належної контр-пропагандистської діяльності з боку України. Слід відзначити, що в даному напрямку вже зроблені відповідні кроки. Зокрема, 11 березня 2021 р. Указом Президента України при Раді національної безпеки і оборони України створено Центр протидії дезінформації. Однак його функції фокусуються переважно на виявленні та аналізі поточних і попередженні прогнозованих загроз інформаційній безпеці України, і проблематики історичних та історико-правових фальсифікацій торкаються лише побіжно.

Тому в контексті зазначеного, на наш погляд, потрібні заходи більш широкого характеру, і в першу чергу, у сфері освіти та науки. Завдяки саме таким заходам, як видається, створюються можливості не тільки забезпечити поглиблення історико-правових знань в системі підготовки та перепідготовки здобувачів вищої освіти, але й популяризувати ці знання серед широкого загалу, підвищити загальну історико-правову освіченість громадян України.

З цією метою було б доречним запровадження у закладах вищої освіти України історико-правових навчальних дисциплін та спецкурсів або збільшення годин на викладання вже існуючих. Також суттєвим фактором протидії спробам викривлення історико-правової реальності могло б стати належне фінансування історико-правових досліджень з найбільш актуальних проблем вітчизняної історії, які використовуються Російською Федерацією в інформаційній гібридній війні проти України, проведення міжнародних і всеукраїнських наукових конференцій, круглих столів та інших наукових форумів, доведення до суспільства через засоби масової інформації та соціальні мережі їх підсумків.

ДЕСТРУКТИВНА ПРОПАГАНДА РФ ЩОДО ПОЛЬЩІ З ВИКОРИСТАННЯМ РЕЛІГІЙНОГО ЧИННИКА

У гібридній війні проти Польщі Російська Федерація активно апробує різні інструменти і механізми деструктивної пропаганди, спрямовані на дестабілізацію внутрішньополітичної ситуації всередині країни, а також використовує ключові фактори соціально-політичного життя польської держави для реалізації комплексних загроз гібридного характеру. Одним з таких факторів, який займає в житті польського населення одне з ключових місць, є релігія.

Конституція Польщі передбачає свободу світогляду та віросповідання. Відповідно до Основного закону, релігія – це особистий вибір людини, а усі церкви та релігійні організації мають рівні права. Конкордат зі Святим Престолом визначає відносини з Римсько-католицькою церквою. Статути і угоди визначають відносини між урядом і 14 іншими релігійними групами. При цьому, Основний закон забороняє публічні виступи, що ображають релігійні почуття [1].

Станом на 2020 рік майже 85 відсотків населення Польщі ідентифікувало себе з католиками. Другою за величиною релігійною групою були православні та, зокрема, Польська православна церква, яка налічує близько півмільйона членів. При цьому релігійні групи повідомляють, що число православних віруючих збільшилося удвічі з 2014 року завдяки припливу українських робітників. Третьою за чисельністю релігійною групою в Польщі є Свідки Єгови, які нараховують близько 116 тис. осіб. Іншими чисельними релігійними групами є іудеї – орієнтовно 40 тис. осіб та мусульмани – близько 25 тис. осіб [1].

Варто відзначити, що саме по відношенню до самої численної та впливової конфесії Польщі, а саме Католицької церкви, фіксуються неодноразові інформаційні операції та пропагандистські кампанії з боку РФ і підконтрольних їй організацій, експертів та ЗМІ. Вказані операції та кампанії, здебільшого направлені на поширення наративу про секуляризацію польського суспільства та формування негативно-інформаційного фону навколо польської Католицької церкви.

Активізація антикатолицької пропаганди з боку прокремлівських ЗМІ спостерігалася під час вуличних протестів, які почалися у Польщі у жовтні 2020 року, після того, як Конституційний суд визнав неконституційним положення, яке дозволяло проводити аборти у разі

важких дефектів плоду. Варто відзначити, що Католицька церква стала окремим адресатом гніву протестуючих, у зв'язку з тим, що її духовенство підтримало вказане рішення суду про заборону абортів [2]. Восени 2020 року ЗМІ РФ дуже активно висвітлювали провокаційні акції щодо католицької церкви, детально описуючи будь-який, навіть незначний інцидент.

Так, російське електронне інтернет-видання «Лента.ру» в одній зі своїх публікацій так висвітлювало події «... свій гнів протестуючі виливали на церкву: оскільки переважна більшість жителів країни є релігійною, її тиск з подібних питань залишається доволі сильним. Невдоволені зривали служби, вигукували непристойності на адресу священнослужителів, писали на фасадах будівель номери гарячих ліній по абортам» [3]. Прокремлівське пропагандистське видання Вести.ru, у контексті триваючих протестів підготувало статтю «Заборона абортів: поляки масово виходять з католицької віри» з детальним описом процедури виходу з католицької церкви [4].

Крім того, під час протестів проти легалізації абортів, активізувалися і представники Російської православної церкви (РПЦ), які у своїх заявах протиставляли радикальній позиції Католицької церкви Польщі позицію РПЦ, яка, нібито, є більш зваженою і людяною. Варто відзначити, що свою точку зору Російська православна церква ретранслює через Польську Православну Церкву (ППЦ), з якою знаходиться у безперервному спілкуванні. Представники Польської православної церкви, автокефалія якої була визнана визначенням Священного синоду Російської православної церкви від 22 червня 1948 року, та РПЦ підтримують тісні контакти, відправляють взаємні вітання, здійснюють взаємні візити на постійній основі, беруть участь в спільних заходах [5].

Заслуговує на увагу і той факт, що представники ППЦ, виступали проти створення ПЦУ в Україні. Так, у 2018 році Архієрейський собор Польської православної церкви заборонив священникам контакти з УПЦ Київського патріархату і Українською автокефальною православною церквою (УАПЦ) [7]. При цьому Митрополит Варшавський і всієї Польщі Сава направляв листа Константинопольському патріарху, у якому заявляв про відмову визнавати нещодавно створену в Україні церкву [6].

Підбиваючи короткий підсумок, необхідно відзначити, що фактично РФ використовує релігійний фактор як інструмент пропаганди та інформаційно-психологічної гібридної війни з метою створення деструктивних рухів усередині польської держави. Відносно Польщі і її релігійних організацій, особливо католицького спрямування на пос-

тійній основі здійснюються спроби релігійно-політичної пропаганди з метою дискредитації і зменшення ролі в польському суспільстві, які особливо загострилися на тлі протестів 2020 року. При цьому на міжнародній арені здійснюються спроби сформуванню уявлення про падіння авторитету Католицької церкви Польщі і масову відмову від католицької віри її прихожан. Основними суб'єктами, які задіяні в реалізації зазначених механізмів, як щодо Польщі, так і по відношенню до України є проросійські ЗМІ, а також діючі на території Польщі релігійні організації, які тісно взаємодіють з РФ та активно використовуються Росією для досягнення своїх стратегічних геополітичних інтересів.

Література

1. 2020 Report on International Religious Freedom: Poland URL: <https://www.state.gov/reports/2020-report-on-international-religious-freedom/poland/> (дата обращения 12.06.2021).
2. Запрет на аборт расколол Польшу. Чем закончатся протесты?, Би-би-си, 22 ноября 2020, URL: <https://www.bbc.com/russian/features-55011085> (дата обращения 05.06.2021).
3. «Моя матка – это не гроб», 19.12.2020, LENTA.RU, URL: <https://lenta.ru/photo/2020/12/19/poland/> (дата обращения 05.05.2021).
4. Запрет абортов: поляки массово выходят из католической веры, 03 ноября 2020, Вести.ru, URL: <https://www.vesti.ru/article/2480536> (дата обращения 05.06.2021).
5. Православная церковь Польши запретила контакты с Киевским патриархатом, 16.11.2018, РБК.Ru, URL: <https://www.rbc.ru/politics/16/11/2018/5beec3859a794705e7f988e0> (дата обращения 05.06.2021).
6. Польская православная церковь отказалась признать новую на Украине, 03.01.2019, Интерфакс-Россия, URL: <https://www.interfax.ru/world/645028> (дата обращения 05.06.2021).

Пелюх О. С.

доктор юридичних наук,
Національна академія СБ України

АКТУАЛЬНІ ПИТАННЯ ФОРМУВАННЯ СТРАТЕГІЇ КОНТРРОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ В УМОВАХ «ГІБРИДНОЇ ВІЙНИ» РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

Аналіз тенденцій розвитку сучасного стану протидії розвідувальній діяльності спеціальних служб Російської Федерації (далі – РФ)

дає підстави констатувати, що контррозвідувальні підрозділи СБ України не можуть обмежуватися реалізацією заходів виключно на тактичному рівні. Асиметричні загрози державній безпеці України спричинені використанням спецслужбами РФ «гібридних» методів діяльності, зумовлюють необхідність застосування національною контррозвідкою стратегічних підходів до їх виявлення та нейтралізації. Зазначене має забезпечити контррозвідці можливість оптимального визначення, оцінки, моніторингу та контролю ризиків державній безпеці, що продукуються зазначеними спецслужбами. Нам видається аксіоматичною теза щодо неможливості ефективно тактично протидіяти реалізації стратегічних планів та намірів спеціальних служб іноземних держав, особливо в разі застосування ними відверто диверсійних, терористичних та інших суспільно-небезпечних методів, спрямованих на реалізацію стратегічної мети щодо позбавлення України незалежності та нейтралізації її проєвропейського курсу.

Це можливо лише шляхом розробленням та реалізації Стратегії контррозвідувальної діяльності України (далі – Стратегія). Це поняття за походженням має військове підґрунтя, тобто, це мистецтво підготовки і ведення війни та великих воєнних операцій. Етимологічно стратегія також тлумачиться як мистецтво суспільного і політичного керівництва масами, яке має визначити головний напрям їх дій або вчинків та як спосіб дій, лінія поведінки кого-небудь.

Наукова думка стосовно досліджуваного поняття досить різниться в залежності від обраних у його дослідженні підходів. Зокрема, стратегія може розглядатись через призму концепції, плану, процесу, програми, моделі, принципу тощо. На нашу думку, кінцева мета Стратегії повинна сформувати контекст протидії розвідувальній діяльності спеціальних служб іноземних держав, та комплекс контррозвідувальних заходів, в процесі реалізації яких виконуються завдання контррозвідувальної діяльності із своєчасного виявлення та запобігання реальним та потенційним загрозам державній безпеці України, що формує бажаний стан забезпечення державної безпеки. Таким чином, Стратегія є завчасно спланованим засобом досягнення кінцевої мети, яка передбачає виконання пріоритетних функціональних завдань контррозвідувальної діяльності щодо своєчасного виявлення та запобігання загрозам державній безпеці України, розв'язання яких є критично важливою і складною проблемою для держави. Передбачений в Стратегії комплекс контррозвідувальних заходів програмує модель діяльності підрозділів контррозвідки з її реалізації по досягненню основної мети.

Цілком логічним в даному контексті є запровадження в тому числі і в рамках Стратегії контррозвідувальної діяльності України національної системи стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, в тому числі «гібридного» характеру, що повинна передбачати:

- оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей;
- ефективне стратегічне планування і кризовий менеджмент, зокрема впровадження універсальних протоколів реагування на кризові ситуації та відновлення з урахуванням рекомендацій НАТО;
- дієву координацію та чітку взаємодію органів сектору безпеки і оборони, інших державних органів, територіальних громад, бізнесу, громадянського суспільства і населення у запобіганні й реагуванні на загрози та подоланні наслідків надзвичайних ситуацій;
- поширення необхідних знань і навичок у цій сфері;
- налагодження та підтримання надійних каналів комунікації державних органів із населенням на всій території України.

Національна система стійкості повинна враховувати той факт, що одна з основних екзистенціальних загроз державній безпеці України – це діяльність спецслужб РФ, які проводять розвідувальну діяльність у тісній взаємодії з російським зовнішньополітичним відомством, державними корпораціями та фінансово-промисловими групами, залучають ресурси підконтрольних засобів масової інформації і громадських організацій, а також використовують підтримку російських аналітичних центрів, фондів з метою створення політико-ідеологічного підґрунтя «гібридної війни» проти України, деструктивної пропаганди та реалізації сценаріїв «керованого хаосу» на шкоду державній безпеці нашої держави.

Однак, реалізацію окреслених планів варто починати за результатами реформування Служби безпеки України як спеціально уповноваженого державного органу у сфері контррозвідувальної діяльності, суб'єкта забезпечення кібербезпеки і кібероборони та захисту критичної інфраструктури, що надасть нові можливості своєчасно виявляти зовнішні та внутрішні загрози безпеці України у протидії агресивним методам розвідувальної діяльності спецслужб РФ і ефективно запобігати їм, усувати умови, що сприяють їм у проведенні розвідувальної і підривної діяльності проти України, та причини їх виникнення.

В контексті зазначеного сутність Стратегії повинна полягати не у впливі на розвідувальну діяльність спеціальних служб іноземних держав, в тому числі і спецслужб РФ, а у виявленні загроз, які ними

продукуються, на якомога ранній стадії проведення ними розвідувальної діяльності, не очікуючи конкретних проявів розвідувального або підривного характеру. При цьому виявлення як одне з функціональних завдань контррозвідувальної діяльності знаходиться в діалектичному взаємозв'язку з іншим її функціональним завданням – запобіганням. Тому, ефективність реалізації Стратегії полягає у створенні необхідної інформаційної основи для вироблення тактики запобігання загрозам державній безпеці, своєчасного відвернення наслідків існуючих та потенційних загроз безпеці держави.

В межах визначеного змісту Стратегії необхідно створювати нові підходи до своєчасного виявлення загроз державній безпеці, в межах яких започаткувати функціонування моделі забезпечення державної безпеки та прогнозування реальних та потенційних загроз з метою вибору ефективних шляхів їх протидії. Одним із таких інструментів є забезпечення функціонування безперервного моніторингу та аналізу загроз державній безпеці із застосуванням нових інформаційних технологій, що дасть змогу своєчасно обрати найбільш оптимальні підходи до запобігання загрозам державній безпеці для вирішення окреслених в національному законодавстві завдань контррозвідувальної діяльності.

Враховуючи окреслений зміст Стратегії та стан протидії «гібридним» впливам спецслужб РФ на шкоду державній безпеці України можна констатувати, що в найближчій перспективі ситуація залишатиметься складною із тенденціями до загострення, що обумовлено продовженням збройного конфлікту на території Донецької і Луганської областей, та підтримкою РФ терористичних організацій «ДНР»/«ЛНР», завданнями спецслужб РФ з протидії євроатлантичній інтеграції нашої країни тощо. Зазначене підтверджує парадигму державної безпеки, яка не може бути визначена за відсутності загроз та забезпечена шляхом їх повної ліквідації, оскільки негативні для об'єктів державної безпеки чинники існуватимуть завжди, і забезпечення її розвитку потребує передусім створення умов, за яких загрози не будуть обмежувати її розвиток.

Саме тому необхідно не тільки мінімізувати вплив таких чинників на уразливі об'єкти, а й створювати певний «іміунітет» щодо їх впливу, тобто здатність системи державної безпеки ефективно функціонувати всупереч негативному впливу. Отже, підтримання здатності функціонувати в умовах існування загроз є найбільш важливим напрямом практичної діяльності щодо захисту об'єктів державної безпеки, а також забезпечення реалізації законних інтересів держави.

Печериця С. В.
кандидат юридичних наук,
старший науковий співробітник,
Національна академія СБ України

ТЕРОРИСТИЧНІ ЗАГРОЗИ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В КОНТЕКСТІ ГІБРИДНИХ ВОЄН СУЧАСНОСТІ. ВИКОРИСТАННЯ МІЖНАРОДНОГО ДОСВІДУ

Історія розвитку людства насичена безперервними конфліктами. Крайньою формою їх розв'язання завжди виступали війни (збройні конфлікти). Незважаючи на тривалі пошуки справедливості та виваженості у змісті й шляхах урегулювання існуючих суперечностей, глибоку історичну традицію пацифістських теоретичних концепцій, практика міжнародного життя свідчить: *наси́льницький спосіб вирішення проблем у минулому, сьогодні й осяжному майбутньому у багатьох відношеннях залишається безальтернативним*. Уроки воєн, незважаючи на моральні та фізичні жертви і страждання людей, витрачені фінансово-економічні ресурси, шкоду довкіллю, занепад багатьох держав, поки що не виступають стримуючим фактором в ескалації наси́льницьких конфліктів.

Держави, інші суб'єкти боротьби за поширення впливу або домінування на глобальному чи регіональному рівнях у тій чи іншій сфері людського буття, завжди переймалися досягненням власних егоїстичних інтересів, не завжди раціонально обґрунтованих. Спливали історичні епохи, утворювалися та зазнавали краху світові імперії, змінювалися інструменти, способи, засоби й методи розв'язання суперечностей, залишаючи постійною, незмінною орієнтацію на експансію влади, зміцнення фінансово-економічної, політичної, воєнної могутності.

Практики реально вивчають інформаційну революцію, однак вони не можуть і не мають ресурсів цікавитися довготривалими закономірностями, причинами і наслідками і впливом економічних і технологічних процесів на інші сфери людського життя.

Проте сильні складові колоніальних й революційних воєн були творчо узагальнені і ефективно використані спецслужбами, зокрема при організації боротьби з обмеженим контингентом радянських військ в Афганістані. Як свідчить З. Бжезинський, з липня 1979 р. президент США Дж. Картер підписав першу директиву щодо надання допомоги противникам прорадянського режиму в Кабулі. Після вводу

радянських сил в Афганістан багато хто з західних фахівців передбачав негативний для СРСР розвиток подій і виснаження й деморалізацію його воєнної структури.

За допомогою спецслужб США і Пакистану протягом 1982-1992 рр. близько 35 тис. радикально налаштованих мусульман з понад 40 країн світу брали участь у бойових діях в Афганістані; значна кількість з них пройшла ідеологічний вишкіл у Пакистані. У березні 1985 р. президент Р.Рейган підписав таємну директиву № 166 щодо операцій проти СРСР а Афганістані. Постачання озброєння і бойової техніки зросло до 65 тис. т. щорічно. При цьому ЦРУ діяло через спецслужби Пакистану, активно використовувалось, як один із засобів послаблення СРСР, виробництво наркотиків в цьому регіоні [1].

Вся ця детально спланована система заходів мала відчутний вплив на динаміку й зміст збройної боротьби. Радянські війська почали бойові дії у традиційному руслі: масований вогонь авіації, артилерії, танків і т.ін., обережне просування вперед, масштабні чистки районів, що вимагало величезних витрат у снарядах, ракетах, бомбах тощо. Афганці дуже швидко навчилися блискавично відходити, вислизати і повертатись назад через години, дні, а іноді й тижні, уражати противника там, де він незахищений і не чекає удару. Оперативна і тактична концепція радянських військ була розрахована для високоінтенсивних бойових дій в Європі, і тому спочатку вони були слабо адаптовані до нової тактики. Не витримувала критики гігієна та санітарія у бойових умовах. Західні джерела свідчать, що серед 642 тис. радянських військовослужбовців, які пройшли Афганістан, 415932 чоловік хворіли, у тому числі 115300 - гепатитом і 31080 - черевним тифом. Військовослужбовці не мали навичок та бажання відходити від панцерних машин далі, ніж на 200 м. Їх обмундирування та спорядження також не було розраховане на це. Приміром, панцерожилет важив більше 15 кг, що не дозволяло пройти по складній місцевості більше 1 км. Польова форма солдат незручна, обмежувала дії та була камуфльована для ведення бойових дій у Північній Європі, вже не кажучи про жахливі рюкзаки, спальні мішки, чоботи тощо, вироблені за технологією 50-х років.

Все це дуже нагадує використання сучасними терористими слабкостей та вразливостей сучасного світу. Інформаційно-технологічні інновації, як і певні соціально-політичні, економічні тенденції, що зараз спостерігаються, створили для цього чудові умови.

Проте радянські війська в Афганістані швидко вчилися. Військові школи і тренувальні центри почали втілювати бойовий досвід у жит-

тя. Було знайдено нову воєнну методологію у боях з партизанами, яка включала концепцію нелінійної збройної боротьби з використанням можливостей високоточної зброї, реорганізацію військ з метою підвищення бойової гнучкості та виживання.

На початку і до середини 80-х років радянські війська змінили концепцію стратегічного наступу, ввели більш дрібне ешелонування на всіх рівнях, розвивали концепцію повітряного ешелонування, експериментували з новими структурами такими, як корпус, бригада, угруповання батальйонів тощо, відпрацьовували стратегію гнучкого тилу і т.ін. Сухопутні війська розвинули інноваційну тактику бронегруп, що посилює можливості маневру в тил та у фланг противнику. Більш ефективно почали використовуватися панівні на місцевості точки для прикриття та підтримки вогнем своїх військ. Значно поліпшилось використання повітряно-десантних військ, гелікоптерів тощо. Афганці високо цінували виучку радянських військ, особливо спеціального призначення та повітряно-десантних [2].

Сьогодні таліби повернулись до влади в Афганістані, не виключено, що за підтримки приватних військових компаній Російської Федерації. Саме ПВК «Вагнера» спеціалізуються на підтримці тоталітарних режимів в так званих «гарячих точках», вигідних керівництву РФ.

Все це, разом з досвідом інших військових операцій («Буря в пустелі» і т.ін.), свідчить про загальну тенденцію у формах і методах збройної боротьби - перехід від лінійного до осередкового характеру. При цьому підвищується автономність та самостійність військових частин і підрозділів, скороминучість бойових дій, ефективність вогневих уражень. Непересічного значення набувають переваги у швидкості збору, обробки інформації, прийнятті рішень. Генерал Норман Шварцкоф, починаючи 17 січня 1991 р. операцію «Буря в пустелі» вимагав від своїх підлеглих планувати і проводити її у такому швидкому агресивному темпі, щоб прийняття рішень командуванням противника, вже не кажучи про фізичну реакцію, було занадто запізним для того, щоб бути ефективним.

Потужно розвивається концепція повітряно-наземної операції, відбувається еволюція воєнних доктрин, все тіснішою стає взаємодія видів та родів військ. Величезними темпами зростає значення захисту військ, у тому числі проти непередбачених технологічних, стратегічних та оперативних раптовостей. Підвищується необхідність забезпечення потайності, мобільності, розосередження сил, посилення темпів проведення операції серед усіх елементів, що беруть участь у бою. У свою чергу мобільність та підвищена розосередженість військ потребуватимуть нових можливостей в засобах зв'язку, координації та си-

нхронізації дій. Нижчі за рівнем військові організації зможуть контролювати більші площі, підвищуватиметься роль професіоналізму, ініціативи та ін. окремих військовослужбовців, маленьких підрозділів.

Особливого значення набуде інформаційна перевага над противником. Вона буде включати традиційні методи - знищення командних пунктів противника та його спроможностей контролю, і нетрадиційні - електронне проникнення в інформаційну мережу противника, захист власних інформаційних комунікацій, антивірусний захист нових способів передачі інформації тощо.

Зазначені вище підходи стосуються не тільки збройних сил, але й інших силових структур. Нагальною вимогою сучасності постає необхідність досягнення якісно нового рівня співробітництва та кооперації не тільки між оборонними відомствами союзників і друзів, але й міжнародного співтовариства в цілому. Великі потенційні можливості має співпраця силових структур, зони відповідальності яких ще до недавня чітко визначені, зараз, в умовах загроз, що постали чи постають, розмиваються.

Сьогодні можна констатувати, що час класичних антиколоніальних й революційних (з огляду їх класового змісту) воєн практично закінчився, почався період внутрішніх воєн, збройних конфліктів, терористичної діяльності екстремістських угруповань, які ставлять перед собою далекосяжні цілі. Однак багато що у способах, засобах, методах, формах, інструментах тощо боротьби збереглося і набуло ще більшої актуальності. Головним при цьому виступає боротьба на виснаження противника у довготривалій боротьбі, відхід від прямого воєнного протистояння в бік асиметричних відповідей, з урахуванням слабких та уразливих місць ворога, переваг швидкості, раптовості, секретності тощо.

Значні можливості для терористів відкриваються із розвитком інформаційних технологій. Поки що позитивні аспекти експлуатації інформаційних технологій значно перевищують можливий негативний вплив, який нестиме боротьба з ними. Отже екстремісти ще не зацікавлені у тотальному руйнуванні інформаційних мереж, оскільки, приміром Інтернет слугує для них дієвим інструментом комунікації. Сьогодні терористи зосереджуються, швидкіше, на систематичному виведенні із ладу комунікацій. Крім цього інформаційні технології дозволяють значно розширити спектр цілей та сприяють ефективному поширенню новин та ідей, що, зрештою, дозволяє маніпулювати свідомістю людей [3].

Отже людство зустрілося з новими небезпеками, які владно диктують необхідність об'єднання зусиль всіх державних і неурядових

організацій, міжнародного співтовариства в цілому. Особливою проблемою при цьому постає не тільки повний та всебічний контроль над зброєю масового ураження (ядерною, хімічною, бактеріологічною), напрацювання механізмів попередження можливості використання новітніх технологій подвійного призначення.

Література

1. Інтерв'ю З.Бжезинського *Le Nouvel Observateur* 15-21.1 1998. – Р. 78.
2. Gran, Lester W., Mohammad Yahia Nawroz. The Soviet Experience in Afganistan. *Military review*, Sept.-Oct., 1995. – Р. 17-27.
3. Pillar P. Terrorism Goes Global: Extremist Groups Extend their Reach Worldwide // *The Brookings Review*. – Fall 2001. – № 19. – Р. 34-37.

Присяжнюк М. М.

кандидат технічних наук,
старший науковий співробітник,
Національна академія СБ України

Карпович О. М.

Національна академія СБ України

ІНФОРМАЦІЙНА ЗБРОЯ ЯК НОВИЙ ЗАСІБ МІЖДЕРЖАВНОГО ПРОТИБОРСТВА

Актуальність теми полягає в тому, що процес протиборства на міжнародній арені відбувається без безпосереднього застосування збройної сили. Значне місце серед тенденцій сучасного силового протистояння належить геополітичному інформаційному протиборству. Це одна із сучасних форм боротьби між державами, яка здійснюється однією державою з метою порушення інформаційної безпеки іншої держави, при одночасному захисті від аналогічних дій з боку супротивної держави.

Інформаційну боротьбу поділяють на інформаційно-технічну та інформаційно-психологічну. При інформаційно-технічній боротьбі головними об'єктами впливу і захисту є інформаційно-технічні системи. У процесі інформаційно-психологічної боротьби головними об'єктами впливу і захисту є психіка політичної еліти та населення протиборчих сторін; система формування суспільної свідомості, державно-управлінські рішення у сфері національної безпеки.

З поняттями «інформаційна війна» та «інформаційна боротьба» тісно пов'язане поняття «інформаційна зброя». Це різновид зброї, го-

ловними елементами якої є інформаційні технології та інформаційні процеси. Характерними рисами її є надзвичайна небезпечність та різноманітність її видів і каналів впливу – від засобів масової інформації та засобів масової комунікації до методів і технічних засобів впливу на свідомість і підсвідомість людей.

Потужність інформаційної зброї зумовлена такими її перевагами:

- універсальністю (не залежить від кліматичних чи географічних особливостей об'єкта інформаційної атаки);

- прихованістю;
- економічною ефективністю;
- масштабністю застосування;
- ефектом «ланцюгової реакції».

Загроза інформаційної зброї полягає в її невловимості. Якщо вона проникла в інформаційний простір держави, то зупинити її вплив надто складно. Враховуючи той факт, що інформаційна зброя часто орієнтована і на свідомість, і на емоції людини, наслідки її використання можуть бути непередбачуваними.

Основними особливостями інформаційної зброї можна вважати:

- масштабність – можливість завдання значних збитків економіці та воєнному потенціалу держави;

- універсальність – можливість багатоваріантного застосування як військовими, так і цивільними структурами проти об'єктів державного та військового управління;

- економічність – низька собівартість та вигідне співвідношення витрат порівняно з наслідками її застосування.

Але найбільш важливою відмінністю інформаційної зброї від традиційних засобів ураження є знеособлений характер та прихованість її застосування.

Формування єдиного глобального інформаційного простору, що є природним результатом науково-технічного прогресу і розвитку комп'ютерних та інформаційних технологій, створює передумови для розробки різних видів інформаційної зброї.

В сучасних умовах володіння ефективною інформаційною зброєю та засобами захисту від неї стає одним з головних завдань забезпечення національної безпеки держав. Саме тому захист національних інтересів у інформаційній сфері має передбачати реалізацію низки програм гуманітарного, економічного, військово-технічного та наукового характеру.

Необхідно зазначити, що важливими засобами протидії інформаційним загрозам є розвиток та оптимізація системи освіти й вихован-

ня населення, проведення активної інформаційної політики держави, економічна підтримка наукових досліджень у сфері інформаційних технологій тощо.

Радовецька Л. В.

кандидат юридичних наук,
Національна академія СБ України

Гасанов М. А.

доктор філософії з політичних наук, доцент,
Академія Державного управління
при Президентові Республіки Азербайджан

НОВЕ СПРИЙНЯТТЯ БЕЗПЕКИ В КОНТЕКСТІ ГЛОБАЛІЗАЦІЇ ТА ГІБРИДНОЇ ВІЙНИ З РОСІЙСЬКОЮ ФЕДЕРАЦІЄЮ: ГІБРИДНІ ЗАГРОЗИ

Ще задовго до початку відкритої фази «гібридної війни» (а фахові юристи наполягають на доречності застосування терміну «неконвенційна війна» [1, с. 254; 2, с. 47-48]) з боку одного із гарантів безпеки України за Будапештським меморандумом – Російської Федерації у 2014 році, мудро і далекоглядно зазначав один із відомих у минулому політиків України, колишній голова комітету ВРУ з питань національної безпеки і оборони в одному із періодичних видань, те, що «проблема забезпечення безпеки у сучасному світі все більше набуває глобального характеру і більшою мірою залежить від геополітичного протистояння провідних суб'єктів світової політики» [3]. Україна є об'єктом геополітичних інтересів різних країн, чому сприяє її вдале в цьому відношенні геостратегічне розташування, а також великою мірою та внутрішня і зовнішня політика, яку вона вибудовувала впродовж років своєї незалежності.

В умовах глобалізації, транскордонної природи організованої злочинності та тероризму, інтеграції України у європейський та міжнародний правовий та безпековий простори суттєвого значення набувають можливості та здатності протистояти зовнішнім загрозам, вираженим на сьогодні насамперед у веденні гібридної війни Російською Федерацією проти України та деяких інших країн. Ці обставини особливо актуалізують проведення наукових досліджень у царині протидії гібридним загрозам не лише в Україні, а й в зарубіжних країнах, оскільки дозволять розробити оптимальні та ефективні шляхи їх попередження та протидії.

Процеси глобалізації та інформатизації, останні досягнення в сучасних технологіях та бурхливий розвиток інформаційного простору безпосередньо вплинули на те, що сучасне середовище безпеки стає все більш складним. Загрози стабільності та безпеці все частіше трапляються у т.зв. «сірій зоні», в якій дезінформація або кібератака є інструментами гібридних тактик державних та недержавних суб'єктів. Тож часи, коли мир, криза та конфлікт були трьома окремими фазами, конфлікти велися переважно військовими засобами, а противники були добре відомі, минули. Кібератаки наносять удари по країнах нижче порога військової атаки. Кампанії в соціальних мережах створюють альтернативні реалії, які прагнуть дестабілізувати політичні спільноти без жодного солдата, який би перетнув єдиний кордон. А «гібридна» комбінація військових та невійськових інструментів створює неоднозначність, яка ускладнює обізнаність про ситуацію, а отже, і швидкість ухвалення консенсусних рішень [4].

На сьогодні в політико-правовому та безпековому, науковому міжнародному та внутрішньодержавному просторах небезпідставно з'явилася низка термінів і понять, які так чи інакше пов'язуються з гібридними загрозами, і формують понятійно-категоріальний апарат новітнього безпекового концепту протистояння гібридним загрозам. Це, зокрема: «гібридна війна» («hybrid warfare»), «суб'єкти гібридних загроз» (англ. «hybrid threat actors», тобто суб'єкти ведення гібридних війн), «гібридна діяльність», «гібридні супротивники», «гібридна атака», «гібридні комбінації», «регіони гібридної війни/конфліктів», «гібридний ландшафт гібридних загроз» тощо, які потребують свого подальшого наукового осмислення та переосмислення у зв'язку з новітніми подіями як в Україні, так і за кордоном (зазначимо, що останнім часом західні демократії – країни Європи та США все частіше стають об'єктами всебічних гібридних дій, що створюють безпосередню загрозу безпеці низки країн.

Термін «гібридна загроза» прийнято застосовувати відносно дій державних чи недержавних суб'єктів, здійснюваних з метою підірвати або завдати шкоди певній цілі, вплинути на прийняття нею рішень на місцевому, регіональному, державному чи інституційному рівні. Дії таких суб'єктів скоординовані, синхронізовані та безпосередньо спрямовані з метою нанесення уражень демократичним державам, її інституціям, а їх діяльність може відбуватися, у політичній, економічній, військовій, цивільній чи інформаційній сферах і проводиться із використанням широкого спектру різноманітних засобів і способів. Діяльність же розробляється і здійснюється в такий спосіб, щоб залишатися нижче порога свого виявлення та атрибуції [5].

Характерною ознакою (властивістю) гібридних загроз є вчинювані суб'єктами гібридних загроз гібридні дії (діяння), здійснювані в межах гібридної діяльності, характеризуються так званою *дуальністю*, тобто мають *подвійну природу*. Ця подвійна природа проявляється у тому, що суб'єкти ведення гібридних війн стирають звичні кордони міжнародної політики та діють на межі, перетині між зовнішнім та внутрішнім, правовим та протиправним, миром та війною. Дуалізм стає можливим і створюється, переважно, шляхом поєднання традиційних та нетрадиційних засобів, зокрема з використанням дезінформації та шляхом втручання у політичні дебати чи вибори, завдаючи шкоди критичним інфраструктурним порушенням, проводячи різноманітні атаки, кібер-операції, використовуючи різні форми злочинної діяльності, зокрема й шляхом асиметричного використання військових засобів та веденням гібридних воєн.

Іншими іманентними *змістовими* ознаками гібридних загроз є такі:

- злагоджені синхронізовані дії, вчинювані свідомо з використанням різноманітних засобів, спрямованих на системну вразливість демократичних держав та її інституцій;
- діяльність, у якій використовуються різні пороги виявлення та атрибуції, а також поділу, як-от: війна-мир, внутрішня-зовнішня безпека, внутрішньодержавний та міжнародний аспекти, тощо;
- діяльність, здійснювана у різних формах, що спрямована на прийняття рішень на місцевому (регіональному), державному чи інституційному рівнях та на подальше виконання стратегічних цілей суб'єкта гібридних загроз, і яка підриває або завдає шкоди цілі.

У наукових дослідженнях, присвячених гібридним загрозам доводять *економічну* доцільність та ефективність використання вищезазначених нетрадиційних засобів, оскільки суб'єкт ведення гібридних війн використовує вразливі місця свого супротивника, перетворюючи це на свою пряму силу, що ускладнює не лише атрибуцію суб'єкта гібридних загроз, але й запобігання та реагування на гібридні дії.

Окремим вельми актуальним дискусійним і малодослідженим питанням в контексті гібридних загроз залишається питання т.зв. *правової стійкості*. Робота в правовому полі показала, що існують сірі зони як на міжнародному, так і на національному рівнях, які можуть бути використані супротивниками. Метою наукових досліджень було встановити спроможності національних правових систем оперативно реагувати на події, які не проявляються як явна збройна агресія, однак які, фактично, становлять військову загрозу. Результати цих досліджень дозволяють стверджувати, що в деяких країнах діють норми,

які дозволяють оперативно реагувати, однак в деяких випадках своєчасне прийняття рішень, очевидно буде важким [6].

Вищезазначене свідчить про міждисциплінарну природу гібридних загроз та актуальність й доцільність проведення подальших наукових розвідок та міждисциплінарному рівні із використанням широкого спектру методологічних підходів та використанням відповідної методології за активної співпраці урядових та неурядових організацій та експертів.

Література

1. Світова гібридна війна: український фронт. Монографія. За заг. ред. В.П. Горбуліна. К.: НІСД, 2017. 496 с.
2. Лещенко О.Я. Трансформація системи цивільного захисту України в умовах сучасних воєнно-політичних конфліктів гібридного типу: дис. на здобуття наук. ступеня канд. політ. наук: спец. 21.01.01 «Основи національної безпеки держави (політичні науки)» / О.Я. Лещенко. – К., 2020. – 293 с.
3. Крючков Г. Безопасность Украины в контексте геополитического противостояния / Г. Крючков // Киевский весник. – №58 (6469).
4. Електронний ресурс:
<https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html>.
5. Електронний ресурс: https://www.hybridcoe.fi/hybrid-threats/?fbclid=IwAR0Cyf0-Bxb2LmWt9OkDZTSxdrsJlXhcEMh6K8ONYX4z-sQcA8vi_sQNnX4.
6. Електронний ресурс: <https://www.hybridcoe.fi/publications/hybrid-coe-trend-report-3-hybrid-threats-and-the-law-concepts-trends-and-implications/>.

Юдін О. К.

доктор технічних наук, професор,
Національна академія СБ України

Четверяков І. О.

кандидат технічних наук, доцент,
Національна академія СБ України

Петренко А. Б.

кандидат технічних наук, доцент,
Національний авіаційний університет

ТЕХНОЛОГІЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ІОТ

Сучасне представлення цифрового простору та визначень понять Інтернет речей Internet of Things (IoT), вказує на поєднання інформаційної інфраструктури з фізичним світом в рамках глобального циф-

рового мережевого простору з використанням різного класу інформаційних ресурсів. В даному випадку, можна казати про цифрову інформаційну інфраструктуру або кіберпростір, що включає в себе засоби інформаційних технологій (ІТ), такі як зберігання даних, хмарні послуги, операційні системи, програми, різні мережеві технології, служби резервного копіювання, моніторинг і механізми безпеки, а також процеси автентифікації, авторизації та аудиту. Фізична інфраструктура включає пристрої та датчики всіх форм, а також системи управління, які забезпечують належне функціонування цих елементів [1]. Безпека ІТ-інфраструктури IoT є необхідною, але недостатньою умовою, оскільки навіть якщо вона буде захищена передовими методами безпеки ІТ, будь-яке порушення фізичних пристроїв і датчиків може призвести до порушення всієї системи. Отже, якщо буде порушена робота пристроїв, то і дані, створені за допомогою цих пристроїв, скоріш за все будуть ненадійними. Безпека інфраструктури IoT вимагає комплексного підходу, починаючи від фізичних пристроїв і датчиків до послуг і даних у хмарі. Таке формулювання вимоги безпеки для технології IoT залишається проблемою, оскільки інфраструктура IoT зазвичай розробляється, розгортається і експлуатується не тільки ІТ-фахівцями, а й дизайнерами, розробниками та операторами фізичних пристроїв і машин. Для розробників ІТ-інфраструктури, безпека та конфіденційність персональних даних, паролів та пріоритетів доступу повинні бути однією з найбільш важливих функцій системи, разом з функціональністю, зручністю використання та вартістю. Проте, розробники фізичних машин можуть вважати більш важливими доступність і надійність машини, ніж безпека та безпосередньо конфіденційність даних.

Дослідження, даної галузі, дало чітке розуміння того, що найслабшим місцем технології IoT є передача та зберігання критичних даних. В роботі представлено дослідження, щодо розробки власної моделі архітектури IoT та визначення, процесів і процедур захисту пристроїв IoT на основі протокольних рівнів моделі ISO\OSI. Також надано рекомендації, щодо впровадження таких систем на основі сучасного програмно-апаратного забезпечення провідних компаній світу.

Глобальна Інтернет мережа складається з мільйонів локальних і глобальних приватних, публічних, академічних, ділових і урядових мереж, пов'язаних між собою з використанням різноманітних дротових, оптичних і бездротових технологій. Інтернет становить фізичну основу для розміщення величезної кількості інформаційних ресурсів і послуг.

IoT складається з пристроїв, які обладнані вбудованими датчиками, за допомогою яких збирається та оброблюється інформація з навколишнього середовища, та передається для її подальшого аналізу. Одним з базових принципів захисту інформаційних ресурсів класу IoT, це забезпечення підключення пристроїв до хмари, а також впровадження процедур забезпечення конфіденційності даних в хмарі під час обробки і зберігання [1]. Цьому перешкоджає наявність пристроїв з обмеженими ресурсами, географічний розподіл розгортання і велика кількість використовуваних в рішенні пристроїв. Але в першу чергу безпека Інтернету речей це цілісність коду, що виконується на пристроях, перевірка справжності користувачів і пристроїв, визначення чітких прав володіння для пристроїв (в тому числі даних, створених цими пристроями), а також стійкість до віртуальних і фізичних атак [2].

Велика кількість IP адрес та інтеграція взаємозв'язків між елементами інфраструктури накладає відбиток на всю інфраструктуру та децентралізує саму мережу з точки зору використання великої кількості точок доступу (входів управління) до ресурсів IoT. Це дозволяє збільшити кількість точок доступу в мережу, що вводить більшу кількість уразливостей, в т.ч. з бездротовими функціями. Значна кількість пристроїв, що зв'язуються через IP тип протоколів моделі ISO\OSI, буде передавати дані і ідентифікатори доступу, але ці передавачі повинні бути безпечними та захищені на тлі сучасних програмно-апаратних засобів, моделей та методів.

В дослідженнях представлено розробку моделі захисту інформаційних ресурсів класу IoT, що впроваджується з метою створення системи управління безпекою мережі, для зменшення часу обробки даних з урахуванням невеликих потужностей забезпечення відповідних механізмів захисту, достатніх для кожного з рівнів безпеки IoT [3; 4]. Запропонована модель допомагає дослідникам і розробникам вибирати зручні протоколи і механізми безпеки кожного рівня безпеки для захисту даних і інтелектуальних об'єктів. Така модель використовується для максимального запобігання або зменшення атак, загроз і проблем.

У дослідженнях представлено розроблену структуру моделі захисту інформаційних ресурсів класу IoT на основі відповідних механізмів безпеки з урахуванням передачі даних на необхідних рівнях моделі ISO\OSI. Модель забезпечує вимоги безпеки, такі як контроль доступу, управління маршрутизацією, автентифікація, конфіденційність і цілісність для кожного рівня безпеки, а також гарантує безпеку базових додатків.

Література

1. Кібербезпека сучасної повсякденності – європейський досвід [електронний ресурс]. – 2016.
2. Управление безопасностью и доступом [електронний ресурс] / naresh persaud. – 2020.
3. Информационная безопасность интернета вещей (internet of things) [електронний ресурс]. – 2021.
4. IoT architecture: building blocks and how they work [електронний ресурс].

Бараннік В. В.

доктор технічних наук, професор,
Харківський національний університет імені В.Н. Каразіна

Сідченко С. О.

кандидат технічних наук, старший науковий співробітник,
Харківський національний університет Повітряних Сил

Супрун О. М.

кандидат фізико-математичних наук, доцент,
Національна академія СБ України

Бараннік Н. В.

Харківський національний університет надзвичайних ситуацій

ПРОБЛЕМНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ВІДЕОІНФОРМАЦІЙНИХ РЕСУРСІВ В УМОВАХ ІНФОРМАЦІЙНИХ ТА КІБЕРНЕТИЧНИХ ВІЙН

З початку ХХ сторіччя спостерігається значна напруженість в інформаційному просторі, яка постійно набирає оберти та призводить до відкритих звинувачень та відкритих дій відносно планування та здійснення інформаційних та кібернетичних атак між різними державами. При цьому поле інформаційного протиборства не має меж. Сьогодні навіть США становляться ареною інформаційних війн. Інформаційні атаки здійснюються, як в політичній площині, так й на інформаційно-технічні системи. Так, наприкінці 2020 року на державні та корпоративні системи США було здійснено масовану кібернетичну атаку. Адміністрація США напряду звинувачує уряди Росії та Китаю в цьому втручанні та зазначає, що зловмисники отримували доступ до важливої державної інформації щонайменше 8 місяців. Державний департамент обіцяє зробити хід у відповідь та провести кібернетичні атаки на інформаційно-технічні системи зазначених держав [1]. Все це говорить про те, що велика кількість держав, які розробляють та

мають доступ до високих технологій, не тільки розробляють інформаційну зброю, а й активно використовують її.

В Україні, починаючи з 2014 року рівень напруженості в інформаційному просторі знаходиться на високому рівні, а тому критично-важлива інформаційна структура та інформаційні ресурси знаходяться під загрозою втручання та потребують забезпечення інформаційної та кібернетичної безпеки. Але просто купити на ринку високоефективні засоби захисту інформації не можливо. Це в першу чергу пов'язано з тим, що високорозвинені в технічному плані держави обмежують доступ до цих засобів, відносячи їх до високоефективних зразків озброєння та забороняючи їх розповсюдження. Тому для відсічі агресії в інформаційно-технічному просторі Україна змушена розробляти власні ефективні засоби захисту від інформаційних та кібернетичних атак. Це крім сфери забезпечення обороноздатності держави пов'язано й з тим, що курс спрямований на діджиталізацію усіх сфер держави потребує безперебійної роботи усіх інформаційно-технічних систем та забезпечення захисту інформації, яка циркулює в них. Адже збій цих систем або втручання до них може призвести до значних втрат, аж до втрати державного суверенітету. Бурхливе зростання відеосервісів призвело до того, що відеоінформація стала важливим державним ресурсом. Вона впливає на національну безпеку, безпеку комерційних структур і дотримання прав особистості, та визначає рівень економічного розвитку держави, оборонний потенціал держави, формує суспільну думку. Її незаконне розголошення може привести до великої кількості загроз безпеки особи, об'єкту, підприємства, структури, системи, держави тощо. Тому, критично важливий відеоінформацій ресурс потребує забезпечення конфіденційності. Необхідність створення комплексної системи захисту інформації закріплена на законодавчому рівні [2; 3]. Однак, способи і методи захисту відео- і фотоматеріалів на законодавчому рівні не визначені, хоча необхідність забезпечення належного зберігання закріплена в ряді нормативно-правових актів, в яких порушуються питання застосування систем відеоспостереження. При цьому, резолюція Парламентської Асамблеї Ради Європи (яку підписала Україна) щодо здійснення відеоспостереження в громадських місцях рекомендує на законодавчому рівні закріпити практику кодування (шифрування) даних відеоспостереження для захисту їх від несанкціонованого доступу і модифікації, що може допомогти гарантувати достовірність інформації для кримінальних розслідувань [4]. Існуючи методи захисту інформації не орієнтовані на джерело, а тому не завжди можуть бути використані

для забезпечення конфіденційності відеоданих. Розробка нових методів потребує вирішення наступної проблеми в технічному плані. З одного боку збільшення конфіденційності відеоінформації призводить до збільшення витрат часу на її обробку і доставку, тобто відбувається зниження доступності. З іншого боку при збільшенні конфіденційності для підтримки заданої оперативності необхідно знизити обсяг корисної інформації, що призводить до зменшення вірогідності, тобто втрати цілісності. При цьому необхідно переходити до розробки нових технологічних рішень, які зможуть застосовувати недетерміновані властивості при обробці відеоданих [5; 6].

Література

1. Biden Is Tested in How to React to Cyberattacks From Russia and China / The New York Times. – March 8, 2021. – Section A, p. 11 [Електронний ресурс]. – Режим доступу: <https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html>.
2. Закон України “Про захист інформації в інформаційно-комунікаційних системах” від 5 липня 1994 року № 80/94-ВР зі змінами.
3. Указ Президента України “Про рішення Ради національної безпеки і оборони України від 20.05.2016 року “Про Стратегічний оборонний бюлетень України” від 06.06.2016 року № 240/2016.
4. Resolution of PACE 1604 (2008) “Video surveillance of public areas” [Електронний ресурс]. – Режим доступу: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17633&lang=en>.
5. Alimpiev A.N., Barannik V.V., Sidchenko S.A. The method of cryptocompression presentation of videoinformation resources in a generalized structurally positioned space // Telecommunications and Radio Engineering. – 2017. – Vol. 76, No 6. – pp. 521-534. – DOI: 10.1615/TelecomRadEng.v76.i6.60.
6. Barannik, V. and Belikova, T. and Gurzhii, P.: The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 656 – 661 (2019), DOI: 10.1109/ATIT49449.2019.9030432.

Бараннік В. В.
доктор технічних наук, професор
Юдін О. К.
Національна академія СБ України
Красноруцький А. О.
кандидат технічних наук,
старший науковий співробітник
Шульгін С. С.
кандидат технічних наук
Харківський національний університет радіоелектроніки

ТЕХНОЛОГІЯ КОДУВАННЯ ДЛЯ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СПЕЦІАЛЬНИХ ВІДЕОРЕСУРСІВ

Особливості цифрового зображення і сучасних технологій кодування відеоінформації в бортових системах безпілотних літальних апаратів не дозволяють в водночас отримувати достовірну і цілісну інформацію. Пов'язано це з існуючим дисбалансом: забезпечується необхідний рівень цілісності доставки відеоінформації, але з сумнівною достовірністю інформації і навпаки: забезпечивши необхідний рівень достовірності зображення, втрачається його цілісність та оперативність доставки, що веде до старіння інформації і ставить під сумнів інформаційну безпеку спеціальних відеоресурсів. Одним з напрямків збереження інформаційної безпеки спеціальних відеоресурсів є зниження інформаційної надмірності відеоінформації, отриманого з борта безпілотного апарату, шляхом методики виділення значущих і не значущих семантичних областей зображення [1-2].

З точки зору цифрової обробки зображень, області ландшафту характеризуються невеликими значеннями динамічного діапазону елементів уявлення сегментів початкового зображення [3-4]. З точки зору семантичної насиченості, ландшафтні ділянки є незначними. Для розробки методу ефективного синтаксичного представлення відеозображення на борту літального апарату пропонується використовувати особливості сегментів зображення, які несуть інформацію про ландшафт. Одним з напрямків зниження інформаційної інтенсивності сегментів вихідного зображення зі збереженням його семантичної цілісності, є використання підходів заснованих на локалізації структурно-комбінаторної надмірності [5-6]. Однак такі підходи зниження інформаційної інтенсивності мають ряд недоліків. Так, з одного боку, здійснюється усунення структурно-комбінаторної надмірності, обу-

мовленої обмеженням в динамічному діапазоні, з іншого - цей підхід вимагає великих обсягів двійкових розрядів, що витрачаються на уявлення службових даних [7-8].

Можливий напрямок зменшення впливу обсягу службових даних на величину ступеня зменшення інформаційної інтенсивності передбачає збільшення розмірів сегмента [9]. В цьому випадку, перший прохід виконується для формування єдиної системи основ, а другий - для обчислення коду; зниження ступеня інформаційної інтенсивності пов'язано зі збільшенням динамічного діапазону елементів в сегментах зображення. Наслідком наведених недоліків є, як необхідність збільшення обсягу жорсткого диску, так і підвищення часу на обробку сегментів відеозображення.

Для усунення виявлених недоліків при розробці технології кодування передбачений метод формування ефективного синтаксичного представлення сегментів, які несуть інформацію про ландшафт. Тут необхідно забезпечити виконання наступних умов: підвищення ступеню усунення інформаційної інтенсивності за рахунок зниження питомих витрат на подання службових даних; зменшення обсягу проміжних даних обчислювального процесу і як наслідок зниження необхідних обчислювальних ресурсів; зниження часу на обробку сегментів зображення, шляхом побудови кодограми сегмента за один прохід. Напрямок вдосконалення технології кодування для підвищення інформаційної безпеки спеціальних відеоресурсів, з метою збереження водночас інформаційної цілісності і достовірності стоїть на платформі розробки методу формування ефективного синтаксичного представлення сегментів, які несуть інформацію про ландшафт.

Такий метод передбачає виділення значущих і не значущих семантичних областей зображення. Тут необхідно враховувати, що зростання розміру сегменту веде до зниження питомих витрат службових даних одночасно з обмеженням розміру інформаційної щільності.

Література

1. Chen, Ch.-Ch. and Wu, W.-J.: A secure Boolean-based multi-secret image sharing scheme. *Journal of Systems and Software*, Vol. 92, pp. 107-114 (2014) DOI: 10.1016/j.jss.2014.01.001.
2. Chen, T.-H. and Wu, Ch.-S.: Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*, Vol. 91, Iss. 1, pp. 90-97 (2011) DOI: 10.1016/j.sigpro.2010.06.012.
3. Deshmukh, M. and Nain, N. and Ahmed, M.: An (n, n) -Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic. In: *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, pp. 690-697 (2016) DOI: 10.1109/aina.2016.56.

4. DSTU 7624:2014: Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm. Order of the Ministry of Economic Development of Ukraine № 1484 (29.12.2014).
5. 4.Auer, S. and Bliem, A. and Engel, D. and Uhl, A. and Unterweger, A.: Bitstream-based JPEG Encryption in Real-time. In.: International Journal of Digital Crime and Forensics (2013) DOI: 10.4018/jdcf.2013070101.
6. Barannik, V. and Barannik, N. and Ryabukha, Yu. and Barannik, D.: Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System. In.: 15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020), pp. 699-702 (2020) DOI: 10.1109/TCSET49122.2020.235522.
7. Barannik, V. and Barannik, V.: Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones. In.: 15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020), pp. 775-780 (2020) DOI: 10.1109/TCSET49122.2020.235540.
8. Barannik, V. and Belikova, T. and Gurzhii, P.: The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), pp. 656 – 661 (2019), DOI: 10.1109/ATIT49449.2019.9030432.
9. Barannik, V., and Krasnoruckiy, A. and Hahanova, A.: The positional structural-weight coding of the binary view of transformants. In: East-West Design & Test Symposium (EWDTS), pp. 1-4. Rostov-on-Don (2013) doi: 10.1109/EWDTS.2013.6673178.

Жевелєва І. С.

кандидат юридичних наук,
Національна академія СБ України

ВИКОРИСТАННЯ МЕТОДІВ ПРОПАГАНДИ У ГІБРИДНІЙ ВІЙНІ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

Гібридна війна відбувається, як мінімум, у чотирьох зонах – зоні прямого збройного протистояння, зоні ворожого тилового населення, зоні власного населення, зоні міжнародної спільноти.

Пропаганда є важливою складовою методів гібридної війни. Уперше в ХХ ст. погляди на важливу роль пропаганди у війні були чітко викладені в книзі Гарольда Д. Лассуелла (Harold D. Lasswell) «Техніка пропаганди у світовій війні», виданій в 1927 році. Автор одним із перших у світі окреслив інформаційно-психологічну сферу війни, визначив пропаганду як особливий вид зброї, що впливає на моральний

(тобто психічний) стан ворога [1, с. 102]. Ще однією людиною, причетною до створення багатьох ідеологічних кліше і пропагандистських прийомів, що використовуються дотепер російськими ЗМІ, є Віллі Мюнценберг – агент Комінтерну, пропагандист і агітатор сталінського режиму. Усі головні прийоми сучасної масової пропаганди Російської Федерації, такі як: представлення злочинця жертвою, приписування своїм ворогам власних злочинів, тотальне ігнорування фактів, таврування всіх, хто не поділяє «затверджених» поглядів, практика створення великої кількості комісій і комітетів для надання відвертій брехні статусу громадської думки – були створені ще в 1920-х роках Віллі Мюнценбергом [1, с. 103].

Незважаючи на достатньо тривалу історію існування пропаганди, використання її активізувалося у ХХІ ст., коли відшліфовані у ХХ ст. практики доповнилися можливостями нових інформаційних технологій, що використовуються у інформаційному протистоянні в межах сучасних військових кампаній.

Пропаганда – це ідеологічно спрямована діяльність партії, громадського об'єднання чи іншої організації для формування у конкретних верств населення певних позицій і уявлень (світогляду). Пропаганда зазвичай поширюється через різні засоби масової інформації, щоб досягнути бажаного результату. На відміну від об'єктивної подачі інформації, пропаганда подає інформацію, насамперед, для впливу на аудиторію [2]. Для пропаганди дуже важливою є масова комунікація, оскільки вона дозволяє пропагандистам максимально ефективно досягати своєї мети. Для цього вони використовують майже всі форми масового спілкування, насамперед, телебачення та Інтернет.

Пропаганду можна класифікувати за двома принципами: джерелом повідомлення та природою повідомлення.

Дослідник В. Березін залежно від джерела повідомлення визначає білу, чорну та сіру пропаганду. Інформація білої пропаганди подається з відкритого і загальнодоступного джерела, використовує м'які, стандартні методи переконання, наприклад односторонній виклад аргументів. Сіра пропаганда публікується без визначеного джерела повідомлення чи автора. Чорна пропаганда використовує метод маскування правдивого джерела, коли інформація подається під виглядом одного джерела, а насправді походить з іншого.

Е. Аронсон визначив, що залежно від природи повідомлення пропаганда може бути позитивною або негативною. Позитивна (конструктивна) подає інформацію в доступній, зрозумілій формі.

Головним її завданням є сприяння гармонії та спокою в суспільстві. Вона не переслідує маніпулятивної мети. На противагу їй, мета негативної (деструктивної) пропаганди – розпалювання ворожнечі та конфліктів у суспільстві. Це роз'єднує соціум, завдяки чому він підпорядковуються волі пропагандистів, які з легкістю можуть маніпулювати масами в своїх інтересах [3].

«Енциклопедія методів пропаганди» В. Сороченка допомагає визначити низку найпопулярніших методів, що використовують журналісти з метою пропаганди:

- анонімний авторитет – використання у матеріалі слів шанованого та авторитетного джерела, ім'я якого при цьому не повідомляється;
- буденна розповідь – метод, що використовується для адаптації людини до негативної інформації. Якщо, наприклад, необхідно привчити людей до насильства, убивств та злодіянь, телеведучий зі спокійним обличчям, щоденно повідомляє публіці про найважчі злочини. Через деякий час спрацьовує психологічний ефект звикання, коли глядач припиняє реагувати навіть на найжахливіші злочини чи масові вбивства;
- ефект присутності – містить низку трюків, які імітують реальність. Їх постійно використовують у репортажах з місця боїв і в кримінальній хроніці, фабрикуючи «заднім числом» зйомку воєнних дій, погоні за бандитами, автокатастрофи. Створюється ефект присутності, глядач немов бере участь у показаних подіях, не підозрюючи, що це всього лиш фарс;
- інформаційна блокада – створюється інформаційний вакуум якої-небудь проблеми з подальшим поширенням тенденційної інформації про неї. Оскільки цікавість до цього питання в суспільстві досить сильна, відомості, вигідні для пропагандистів, отримують максимальне розповсюдження. Це дає змогу забезпечити єдину інтерпретацію подій;
- використання медіаторів – розповсюдження правдоподібних чуток, які транслюються на рівні міжособистісних комунікацій;
- констатація факту – бажаний розвиток подій подається ЗМІ як такий факт, що вже відбувся;
- навішування ярликів – надання явищу, проти якого виступає пропаганда, яскравої агресивної назви для створення у публіки негативних асоціацій. Також цей метод пропаганди добре працює і у зворотному напрямку;
- затуманення свідомості, неясність, плутанина – публікування з умисно неконкретних, нечітких повідомлень для збентеження та дезорієнтації аудиторії в інформаційному просторі [3].

Основні інструменти, що активно використовуються РФ для пропаганди, є такими.

1. Російська система медійного впливу:

- всеросійська державна телевізійна і радіомовна компанія (телеканали «Россия-1», «Россия-2», «Россия-24», «РТР-планета», EuroNews; інтернет-проекти «Россия», «Вести.ru», «Страна друзей», Digitalrussia.tv, «Страна.ru» та інші);

- міжнародне інформаційне агентство «Россия сегодня» (телеканал Russia Today, новинне відеоагентство Ruptly, міжнародна інтернет-студія Sputnik, РІА «Новости», сайт Ria.ru та інші);

- перший канал Росії («Первый канал. Всемирная Сеть»), на базі якого запущений «Первый Балтийский канал», мовлення якого поширене на Латвію («ПБК Латвия»), Естонію («ПБК Эстония»), Литву («ПБК Литва»).

- медіа «Газпрому» (телеканали «НТВ», «ТНТ»; супутникова телекомпанія «НТВПЛЮС»; радіостанції СІТІ-FM, «Эхо Москвы», «Авторадіо», «101.ru»; видавництво «Семь дней»; кіностудії «НТВкино», «Централ Партнершип»; інтернет-портали Rutube і Now.ru та інші);

- Національна Медіа Група (НМГ), яка позиціонує себе як приватний медіахолдинг (телеканали «Пятый канал», «РЕН ТБ», LifeNews TV; газета «Вести», сайт LifeNews.ru; студія «Российская служба новостей»);

- Russia Beyond the Headlines – міжнародний видавничий проект «Российской газеты», який періодично виходить безкоштовним друкованим і електронним додатком до найвідоміших видань світу 16 мовами (The Washington Post (США), The New York Times (США), The Daily Telegraph (Велика Британія), Le Figaro (Франція), Zuddeutsche Zeitung (Німеччина), The Economic Times (Індія), Folha de Sao Paulo (Бразилія), La Repubblica (Італія), JoongAng Ilbo (Південна Корея), China Business News (Китай) та інші).

2. Російські засоби мережевої комунікації:

- соціальні мережі «Одноклассники», «ВКонтакте» і «Мой Мир»,
- інстант-месенджер «Агент Mail.Ru» з поштовим сервісом ICQ, які з 2014 року повністю зосереджені в руках російської інтернет-компанії Mail.Ru Group.

3. Програмно-комп'ютерні і мережеві елементи впливу:

- «Лаборатория Касперского»;
- проект «Киберберкут»;

- спеціальні підрозділи кібербезпеки ФСБ, МВС, МО РФ та інших структур;

- організації інтернет-тролів (селище Ольгіно (Санкт-Петербург), селище Яблоновське (Республіка Адігея), селище Пережат (Республіка Адігея), селище Зелений Город (Нижегородська обл.), м. Белгород, м. Рязань, м. Хабаровськ, м. Калінінград та інші. Найвідомішою з-поміж цих організацій є ТОВ «Интернет-исследования» (м. СанктПетербург).

4. Російська система соціального формування громадської думки:

- Всеросійський центр вивчення громадської думки (ВЦИОМ),
- дослідне агентство «Евразийский монитор»,
- соціологічна служба Фонд «Общественное мнение»,
- аналітичний центр «Левада-центр» та ін.

5. Федеральне агентство у справах СНД і співвітчизників, які проживають за кордоном, – «Россотрудничество», у складі якого функціонують представництва в 80 країнах світу, у т.ч. в Україні.

6. Інститути громадянського суспільства – урядові та неурядові фонди, які виступають як громадські організації:

- громадська організація «Фонд «Русский мир» ;
- неурядова організація «Фонд поддержки публичной дипломатии имени А. М. Горчакова»;
- некомерційна організація «Российский совет международных дел в сфере внешней политики и международных отношений», заснована Міністерством закордонних справ РФ і Міністерством освіти і науки РФ, Російською академією наук, Російським союзом промисловців і підприємців та інформаційним агентством «Интерфакс»;
- неурядова організація «Фонд исторической перспективы», створена для фінансування європейської (Париж) і американської (Нью-Йорк) філій Інституту демократії і співпраці.

7. Окремі європейські суспільно-політичні організації націоналістичного і ультрарадикального штибу, що фінансуються керівництвом Кремля:

- Front National (Франція), UKIP (Велика Британія),
- BNP (Велика Британія),
- AfD (Німеччина),
- Jobbik (Угорщина),
- Latvijas Krievu savienība (Латвія),
- Атака (Болгарія),
- Forza Italia (Італія) та інші.

8. Російська православна церква, духовенство якої відіграє особливу роль в інформаційній підтримці дій РФ щодо України, пропаганді теорії «Русского мира» під прикриттям ідей православної єдності.

9. Проросійські партії, рухи та суспільні організації, фінансовані та керовані з Москви, які відіграли значну роль на підготовчому етапі гібридної війни («Русский мир», «Русская община Крыма», «Русское единство», «Русский блок», «Славянская партия», «Авангард», «Оплот», «Юго-Восток», «Великая Русь» та ін.) [1, с. 105-106].

Служба безпеки України веде активну діяльність по протидії пропагандистським впливам Російської Федерації. У 2020 році, за матеріалами Служби безпеки України вдалося притягнути до кримінальної відповідальності 40 осіб, які поширювали деструктивну антиукраїнську пропаганду та здійснювали підривну діяльність в інформаційній сфері, 32 особи засуджено, 158 іноземцям, причетним до пропаганди сепаратизму в інтернеті, заборонено в'їзд в Україну. Загалом порушено понад 50 кримінальних проваджень за різними статтями Кримінального кодексу України (109, 110, 111, 161 ККУ) [4].

На сьогодні значна частина антиукраїнської пропаганди фінансується та курується спецслужбами країни-агресора. В Україні російські наративи просуваються в маси через лідерів суспільної думки та відомих «експертів», які інтерпретують факти і події у вигідному для противника світлі. Ворожа пропаганда маскується під «свободу слова», «альтернативну точку зору» або «політичну агітацію» під час виборів.

У 2020 році СБУ заблокувала понад 2,5 тисячі спільнот у соцмережах з мільйонною аудиторією та понад 20 бот-мереж потужністю більше ніж 60 тисяч акаунтів; нейтралізувала понад 600 кіберінцидентів та кібератак на інформаційні ресурси органів державної влади; припинила діяльність 20 хакерських угруповань, причетних до таких атак [4].

Інтенсивність і використання пропаганди з боку Російської Федерації на телебаченні, інтернет-ЗМІ, у соціальних мережах зумовлено зумисним дезінформаційним впливом на аудиторію для розпалу і загострення гібридної війни. Завдання сучасної антиукраїнської пропаганди – підірвати довіру, дискредитувати українську владу, політику, економіку, культуру та інше через навмисне та масове поширення неправдивих, упереджених новин з ворожою політичною метою. Крім цього, внести хаос у суспільну свідомість закликами до порушення державного суверенітету, територіальної цілісності України.

Для сучасної пропаганди в засобах масової інформації властиві такі ознаки: зумисне свідоме поширення викривленої інформації з де-

структивними намірами, спрямованими на дестабілізацію ситуації в Україні та дискредитацію її міжнародного авторитету.

Для захисту від дезінформації та боротьби із російською пропагандою в важливо забезпечити обізнаність населення з цього питання. Перевірка отриманої інформації, уточнення відомостей через інші джерела, обізнаність у сфері методів пропагандистського впливу дають змогу виявити маніпулятивні прийоми та технології.

Література

1. Ткач В.Ф. Спецпропаганда як інформаційний складник гібридної війни Росії проти України. *Стратегічні пріоритети*. Серія: «Політика». № 1 (38). 2016 р. С. 99-109.
2. Шевців М. Б., Гончарук К. А. Пропаганда як соціально-політичне явище: проблеми розуміння. *Південноукраїнський правничий часопис*. 2019. № 1. URL: <http://www.sulj.oduvs.od.ua/archive/2019/1/31.pdf> (дата звернення: 06.07.2021).
3. Іваницька Божена, Гусєва Софія. Основні методи пропаганди в російському інтернет-змі pravda.ru. *Вісник Національного університету «Львівська політехніка»*. Серія: «Журналістські науки». 2018. Вип. 896, № 2. С. 59-64. DOI:<https://doi.org/10.23939/sjs2018.01.059> (дата звернення: 06.07.2021).
4. Сайт Служби безпеки України. URL: <https://ssu.gov.ua/novyny/pokarannia-za-poshyrennia-antyukrainskoi-propahandy-u-2020-rotsi-sbu-prytlahnula-do-kryminalnoi-vidpovidalnosti-40-osib> (дата звернення: 06.07.2021).

Лисенко О. В.

кандидат філософських наук,
Національна академія СБ України

ОСОБЛИВОСТІ ГІБРИДНОЇ ВІЙНИ: УКРАЇНСЬКИЙ КОНТЕКСТ

Суть гібридної війни у порівнянні з класичною мілітарною моделлю (ведення бойових дій, знищення фізичної сили та техніки супротивника, систем управління та комунікації, змушення військовою силою до капітуляції, виконання власної політичної волі чи повернення у зону геополітичного впливу та контролю), полягає у поєднанні військово-терористичної, кримінально-злочинної, інформаційно-пропагандистської та соціально-політичної агресії. Така агресія

ретельно приховує дійсні цілі, наміри, методи, ресурси, засоби та факти безпосереднього чи опосередкованого втручання у справи суверенної країни; 2) реалізується завдяки створенню, розвитку, нагнітання внутрішніх протиріч, конфліктів, протистоянь у яких сторона – агресор позиціонує себе як справедливий захисник «зкривдженої» сторони, а відтак забезпечує собі підтримку з боку маргінальної частини населення країни – суверену, прагне виглядати як «миротворець» в очах міжнародної спільноти і міжнародних організацій та бути «месією» для власного народу; 3) симуляція участі у перемовних процесах, що спрямовані на врегулювання конфліктної ситуації, натомість відверте нехтування результатами домовленостей, міжнародних правових норм (зокрема правил ведення війни та поводження з військовополоненими), моральних цінностей тощо.

Переважно гібридні війни плануються на довгострокову перспективу з гнучкою стратегією та тактикою, що залежить від результативності тих чи інших акцій, довіри та підтримки курсу такої зовнішньої політики у власних громадян, внутрішньої соціально-політичної динаміки країни – суверена, реакції міжнародної спільноти та світових організацій тощо. Також оновлюються і засоби прихованої агресії: від кібернетичних атак і меметичної зброї соціальних мереж до створення квазі державно-політичних утворень. Разом з тим, надзвичайно важливими полями протистояння, окрім військово-технічного, лишаються ідеологія, дипломатія, економіка, релігія.

Відомий американський дослідник тероризму Брюс Хофман у праці «Тероризм. Погляд з середини» зазначає, що уже на початку 1990-х років застосування і значення слова «тероризм» були доповнені новими ознаками та коннотаціями, пов'язаними з виникненням таких явищ як «наркотероризм» і так званий «феномен перехідної зони» [2, с. 12].

Останній термін став використовуватися для позначення загрози територіальній цілісності, суверенності та стабільності національних держав, що виходить від недержавних виконавців, не підконтрольних державі рухів і організацій, або прихованої агресії з боку іншої країни, а також для визначення насильства, що здійснює вплив на населення великих територій або міської зони, де влада перейшла від законного уряду до нових напіврадикальних напівкримінальних структур. Нарешті, цей термін об'єднав в одну категорію військові конфлікти, які більш не вписувалися в рамки традиційних уявлень про ведення війни як про битву збройних сил двох або більше країн, що воювали, але замість цього здійснювалися іррегулярними силами в особі одного і більше осіб.

З 2014 р. об'єктом гібридної агресії з боку Російської Федерації стала Україна, яка, захищаючи свій цивілізаційний вибір, шостий рік боронить не лише власний суверенітет, а й усталений регіональний та світовий порядок і безпеку.

Прогнозованого Ф. Фукуямою «кінця світу» не відбулось – стала трансформація дуального протистояння США – СРСР у формат Захід – Росія, у якому Україна вимушено виконує свою споконвічну місію форпосту, щодо агресії зі Сходу. Росія ж «...у свідомість обивателя наполегливо впроваджує ідея саме світової війни «руського світу» проти безбожного англосаксонського світу, проти Заходу на чолі з США.» [1, с. 52]. – пише аналітик Андрій Піонтковський.

Насправді у процесі цього протистояння відбулося пробудження етно-культурної самосвідомості, актуалізувалися ключові аспекти української екзистенційності та національної ідентичності: військово-патріотичний, національно-культурний та духовно-релігійний – «Мова, Армія, Віра».

Усвідомлюючи життєво-практичну значимість і стратегічну важливість цих факторів, ворог по цим позиціям веде комплексний і безперервний наступ, що вимагає від влади, громадськості, науковців, силових структур та відомств негайної рішучої та адекватної відповіді.

Література

1. Піонтковський А. Четверта світова гібридна війна. Злет і падіння “Руського світу”. URL: https://razumkov.org.ua/images/Material_Conference/2016_12_14/GIBRID-WAR-FINAL-1-1.pdf.
2. Хофман Б. Тероризм взгляд изнутри. URL: https://royallib.com/read/hoffman_bryus/terrorizm___vzglyad_iznutri.html#0.

Титаренко Я. А.
Національна академія СБ України

ПРАВОВІ ОСНОВИ РОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ СПЕЦІАЛЬНИХ СЛУЖБ ІНОЗЕМНИХ ДЕРЖАВ ЩОДО УКРАЇНИ

Вивчення правових основ здійснення розвідувальної діяльності спеціальними службами іноземних держав щодо України є актуальним у зв'язку з тим, що протягом останніх десятиліть розвідувальна

діяльність все частіше стає вирішальним інструментом (хоча і протиправним у більшості випадків) в системі визначення і реалізації зовнішньої політики учасників міжнародних відносин і є, на нашу думку, основним інструментом втручання у внутрішні справи України. Крім того, дослідження правових основ регламентації розвідувальної діяльності провідних зарубіжних країн дозволить краще зрозуміти, які саме нормативно-правові механізми дозволяють ефективно проводити розвідувальну діяльність щодо України і регламентувати втручання у внутрішні справи нашої держави.

Наразі розвідувальна діяльність безпосередньо впливає на формування зовнішньополітичного курсу будь-якої іноземної держави, розробку її геополітичної стратегії та оборонної доктрини. Так, володіючи потужним апаратом отримання первинної інформації, виконання владних замовлень на моніторинг, оцінку, аналіз, прогнозування та моделювання можливих сценаріїв глобальних світових чи регіонального значення подій і процесів, спеціальні служби беруть активну участь у перспективному й поточному плануванні, у формуванні інформаційної основи для прийняття високими посадовими особами владних структур важливих політичних рішень.

До того ж, у сучасних умовах високої динамічності розвитку міжнародних відносин і геополітичних процесів саме розвідувальна діяльність відіграє важливу роль в оперативному інформаційному забезпеченні дипломатії, в прийнятті її структурними підрозділами поточних політичних рішень найбільш вигідних для певної держави. На розвідувальну діяльність покладаються також функції здійснення прихованого спостереження за виконанням іншими партнерами умов підписаних міжнародних договорів та угод.

На нашу думку, з цієї причини розвідувальну діяльність доцільно вважати цілісним самостійним соціально-політичним і правовим явищем міжнародних відносин, специфічною формою організації і практики реалізації зовнішньої політики їх учасниками, котре в сучасних умовах здійснюється як у правових, так і неправових формах.

Спеціальні служби іноземних держав намагаються проводити розвідувальну діяльність в Україні у рамках власного правового поля, що забезпечує її легітимність та безпечне застосування задіяних сил і засобів. З цією метою вони використовують такі прикриття для своїх розвідників та агентів, які дозволяють з легальних позицій збирати інформацію та здійснювати вигідний вплив в інтересах іноземних держав.

У зв'язку з цим, правові форми організації розвідувальної діяльності спеціальних служб у зовнішньополітичній сфері є тісно пов'язаними із публічною політико-дипломатичною діяльністю і здійснюються шляхом прийняття нормативно-правових актів, котрі спрямовуються на розв'язання таких питань організації повсякденної діяльності спеціальних служб іноземних держав, як:

- створення відповідних органів, посад-прикриття або навіть спеціальних зовнішньополітичних та внутрішньополітичних структур;
- визначення їхньої компетенції, порядку і джерел фінансування;
- співробітництво з іншими аналогічними органами;
- регулювання взаємовідносин з дипломатичними, недипломатичними державними органами (міністерствами, відомствами, місцевою владою, поліцією, судом тощо) та неурядовими організаціями, призначення на посади тощо.

Доцільно підкреслити, що нині розвідувальна діяльність із відомчого, насамперед військового інструменту реалізації політики набула специфічних тільки цій діяльності організаційних якостей і переросла у винятковий вид організації зовнішньополітичної практики. Функції реалізації найбільш делікатних таємних заходів зі сфери «таємної дипломатії» у зовнішньополітичній діяльності іноземних держав покладаються на розвідувальні органи. Сучасна розвідувальна діяльність проводиться у політичній, фінансово-економічній, науково-технічній, воєнній і сфері безпеки. У даному випадку дипломатія використовується лише як засіб легалізації результатів розвідувальної діяльності або як прикриття для таємної діяльності учасників міжнародних відносин.

У зв'язку із цим, у всіх державах поряд із системою органів, котрі займаються публічною зовнішньополітичною діяльністю, сформувалася паралельна система спеціальних служб і відпрацьований механізм реалізації таємних зовнішньополітичних заходів у вигляді розвідувального співтовариства, до якого входять усі державні структури (зокрема, представники Міністерства закордонних справ), відповідальні за забезпечення оборони, національної безпеки, практичну реалізацію зовнішньополітичних заходів і захист життєво важливих інтересів держави, суспільства, нації, громадян.

Аналіз матеріалів, які висвітлюють рівень правового забезпечення публічної зовнішньополітичної діяльності політико-дипломатичних відомств та оперативної діяльності спеціальних служб, свідчить про те, що у міжнародно-правовому аспекті як змістовна сторона, так і рі-

вень легітимності розвідувальної і контррозвідувальної діяльності учасників міжнародних відносин не є достатньо визначеними.

Річ у тім, що у межах національного законодавства переважна більшість сучасних держав опосередковано визначили у нормативних актах агентурно-оперативну діяльність власних спеціальних служб як правомірну, а іноземних партнерів – визначають як таку, що підпадає під кримінальну відповідальність.

Наприклад США, Велика Британія, Франція, Німеччина, Російська Федерація та інші держави мають цілу систему внутрішнього законодавства, котре регулює діяльність у сфері інформаційного забезпечення спеціальними службами, державними нерозвідувальними органами та неурядовими структурами у сфері зовнішньої діяльності власних урядів.

У даному випадку спостерігається певна подвійність у ставленні до такого соціального явища, як розвідувальна діяльність. Зокрема, це стосується одного із напрямів оперативної діяльності спеціальних служб – розвідувально-інформаційного й конкретних дій агентів і кадрових співробітників спеціальних служб, які виконують оперативні заходи щодо завдання безпосереднього підриву, котрі визначаються як шпигунство.

Одночасно їхня діяльність щодо реалізації вигідного впливу на політичні чи економічні процеси певної держави, яка проводиться, залишаються поза увагою контррозвідувальних та інших спеціальних служб, у зв'язку із тим, що існує велика проблема юридичного визначення поняття «втручання у внутрішні справи держави», а також певні складності у документуванні цієї протиправної діяльності іноземців і пов'язаних із ними впливових громадян власної держави.

На сьогодні демократичні суспільства вимагають, щоб розвідувальні служби діяли у відповідності з національним законодавством. Правові основи розвідувальної діяльності спеціальних служб іноземних держав дозволяють виокремити чотири основні елементи.

По-перше, законодавство чітко визначає призначення, роль і завдання розвідувальних служб та їх представників. Законами також визначається діяльність, яку їм дозволяється проводити. Уряди контролюють розвідувальні служби у відповідності до положень закону.

По-друге, правові основи діяльності всіх урядових структур мають принципове значення для забезпечення належної прозорості. Закони дають громадськості важливу інформацію для ознайомлення з функціями і повноваженнями урядових структур. Розвідувальним службам потрібні правові основи для застосування спеціальних пов-

новажень з метою збору інформації, яка загалом недоступна іншим урядовим структурам та приватним особам. Наприклад, закони можуть їм дозволяти застосування заходів оперативного характеру стосовно певних осіб. Ці особи мають знати – яким чином розвідувальні служби можуть впливати на їхнє приватне життя, а також чи поважають співробітники розвідки права особи як це визначено законом.

По-третє, правові основи забезпечують розвідувальним службам легітимність в очах громадськості. Доступне для ознайомлення законодавство сприяє кращому розумінню ролі розвідувальних служб, а також пояснює, чому їм потрібні державні кошти для виконання своїх завдань. Це допомагає забезпечити підтримку населенням діяльності розвідувальних служб.

По-четверте, публічні закони про розвідку потрібні для того, щоб забезпечити підзвітність уряду. Органи контролю за діяльністю розвідки та громадськість загалом слідкують за забезпеченням відповідальності урядових структур і розвідувальних служб та за дотриманням цих законів. Публічні закони також дозволяють окремим особам добиватися справедливості у випадках, коли вони вважають що розвідувальні служби вдавалися до незаконних дій проти них.

Утім, аналіз матеріалів, які висвітлюють рівень правового забезпечення публічної зовнішньополітичної діяльності політико-дипломатичних відомств та оперативної діяльності спеціальних служб, свідчить про те, що у міжнародно-правовому аспекті як змістовна сторона, так і рівень легітимності розвідувальної діяльності учасників міжнародних відносин не є достатньо визначеними.

Гребенюк В. М.

доктор юридичних наук, старший дослідник,
Національна академія СБ України

СИЛОВИЙ СЦЕНАРІЙ ГІБРИДНОЇ ВІЙНИ В КРАЇНАХ БАЛТІЇ: ПРОЙДЕНИЙ ЕТАП ЧИ «ДАЛІ БУДЕ»?

Силові сценарії гібридної війни у країнах Балтії були застосовані Російською Федерацією задовго до сумнозвісного 2014 року: у форматі «бронзових ночей» в Естонії, «бунта булыжников» у Латвії, заворушень профспілок у Литві.

Цілком припустимо стверджувати, що саме з цих подій почалось удосконалення механізму поширення «керованого хаосу», вповні за-

діяного в Україні. Було створене агресивне середовище – провідник російських експансій них інтересів, т.зв. «русского мира». Чи не вперше були залучені «політичні туристи», зокрема активісти руху «Наши» - загальноросійського політичного руху, створеного адміністрацією Президента РФ. Їх куратором виступив глава федерального агентства у справах молоді, федеральний комісар цього руху В. Якеменко, а їх засновником – заступник глави адміністрації Президента РФ В. Сурков. Поряд з представниками зазначеного руху участь у заворушеннях брала неформальна бойова група «Ночной дозор».

В країнах Балтії відбулись тренування провокацій гуманітарної кризи шляхом розорення території противника й інфраструктури, а також розколу суспільства. Апробовані технології були успішно використані під час агресії в Україні, спецоперації «Русская весна-2014», лише тому, що незаслужено залишились поза увагою українських експертів з питань національної безпеки.

На цьому тлі ми констатуємо факт того, що зазначені вище події певною мірою потрясли країни Балтії, але все ж не призвели до втрати територіальної цілісності Естонії, Латвії та Литви, як це відбулось в Україні. Можна сказати, що балтійські держави гідно витримали іспит, продемонстрували свою міць та навіть стали сильнішими.

Та чи остаточно усунуто східну загрозу після того, як вказані країни утвердили свою монополію на владу?

Президентка Естонії Керсті Кальюланд з упевненістю заявила, що подібні сценарії у сфері охорони правопорядку більше не повторяться, але вона не врахувала можливостей військової кризи. Кремль теж врахував балтійські уроки, накопичив досвід в Грузії та Україні, скоректував свої експансивні плани. В РФ зрозуміли ефективність привнесених ззовні бойових дій, що ведуть до дестабілізації територій суміжних держав та створення зон «керованого хаосу».

Надихнувшись «перемогами» в Грузії і Україні, Російська Федерація активізувала військові навчання на кордонах з балтійськими країнами. Зазначені навчання супроводжувала кремлівська пропаганда. Зокрема, аналітики проросійського видання «The National Interest» поширювали прогнозні дані про спроможність російських військ захопити країни Балтії всього за декілька годин, змете оборону країн Балтії ракетним обстрілом та авіаударами, а потім розпочне введення сухопутних військ у Литву.

Президент Литви Даля Грібаускайте ще у 2018 році в інтерв'ю Spiegel Online дала оцінку російським військам на кордоні з Балти-

кою та Польщею, зазначивши, що вони в десять разів сильніше, ніж війська НАТО. Лідер країни акцентувала увагу на тому, що небезпека вторгнення Росії в Литву реально існує та до можливого нападу РФ потрібно бути готовими «політично та технологічно». При цьому вона стверджує, що західні держави досі, на жаль, є легковажними у своїй оцінці Росії.

Ще у 2016 році РФ сформувала додаткові дивізії та армії біля кордонів з Балтією, серед них: мотострілецька дивізія у м. Єльня Смоленської області та 1 гвардійська танкова армія. Якщо НАТО направила чотири батальйони в балтійські країни та до Польщі, кожен чисельністю по тисячі солдат, то РФ на своїх західних рубежах сформувала три нових дивізії загальною кількістю особового складу до 30 тисяч військовиків.

Експерти аналітичного центру RAND Corporation підрахували, що Росія може зібрати 22 батальйони у Західному військовому окрузі, які здатні досягнути околиць столиць Естонії чи Латвії максимум за 60 годин. На думку зазначених експертів, цих сил більше ніж достатньо, аби здолати будь-яку оборону балтійських армій. Російські частини мають моторизовані, механізовані чи танкові підрозділи. Їх вісім десантних батальйонів оснащені легкою бронетехнікою.

Водночас НАТО в країнах Балтії розташувало всього 12 батальйонів, погано оснащених для боротьби проти броньованого противника, сім з яких надзвичайно легкі та без належної тактичної мобільності. Щоб протистояти військовій агресії РФ проти балтійських країн потрібно біля семи бригад, у тому числі трьох танкових, які будуть підтримуватись авіацією, та збільшення фінансування на їх утримання до \$ 2,7 млрд.

У розпорядженні Кремля знаходиться також ексклав – Калінінградська область, яка може бути використана як плацдарм для можливого наступу та яку доцент кафедри політології та соціології Балтійського федерального університету імені Канта В. Абрамов назвав «пістолетом біля виска Європи» чи «бурштиновим пістолетом». У цьому регіоні Кремль розмістив сили Балтійського флоту РФ - оперативно-стратегічного об'єднання ВМФ РФ, 11-го армійського корпусу, у складі якого у 2020 році сформована мотострілецька дивізія з мотострілецькими, артилерійським та танковим полками. На території Калінінградської області розташовані: пускові установки оперативно-тактичних ракетних комплексів «Іскандер-М» (можуть вразити ціль на відстані до 500 км); протикорабельні комплекси «Бал-Э» та «Бастіон-П», здатні вражати ракетами цілі за сотні кілометрів; щільна ме-

режа протиповітряної оборони із системами С-300 та С-400 великої дальності, а також комплексом малої дальності «Панцирь», радіолокаційною станцією 29В6 «Контейнер», що відслідковує повітряну активність від Великобританії до США.

Не слід також забувати про союзню Росії Білорусь, у складі збройних сил якої два види військ – Сухопутні війська, Військово-повітряні сили та війська протиповітряної оборони, а генеральному штабу підпорядковані Сили спеціальних операцій, спеціальні війська (служби). Чисельність цих збройних сил, за різними даними, складає від 62 до 65 тис. осіб. В складі двох оперативно-тактичних командувань (Західного та Північно-Західного) знаходяться 3 механізовані, 2 мобільні (десантно-штурмові), 1 – спецназу, 2 ракетні, 5 артилерійських, 2 зенітно-ракетні бригади сухопутних військ, 3 авіабази, 5 зенітно-ракетних та 2 радіотехнічні бригади ВПС та ППО. Техніка ЗС Білорусі включає 1 600 танків, 2 500 броньованих машин, 1 490 артилерійських систем, що переважає польську й українську армії: по танках – в 1,8 и в 2,1 рази відповідно; по бронемашинах – в 1,6 та в 1,2 рази; по важких артсистемах – в 2 и 1,3 рази. Білоруські війська проходять бойове злагодження з російськими збройними силами під час щорічних навчань.

Озброєння та техніка ЗС РБ більшою мірою успадковані від СРСР, а їх оновлення є невід’ємною задачею для бюджету Білорусі. Відтак, уся надія у цій ситуації покладається на Російську Федерацію. Військово-технічна допомога РФ стає ефективним механізмом зміцнення її геополітичних позицій та встановлення важелів впливу на процеси оборони й безпеки у Білорусі. ЗС РБ залежать від донорства Кремля та можуть виступити слухняним інструментом в руках господарів Білокамінної.

Проте, якщо повномасштабна військова операція із залученням усіх цих сил не буде реалізована, що тоді? А тоді з арсеналу Кремля може бути використаний український сценарій, за яким російські триколори вперше були ввезені на територію України козаками. Озброєні представники групи козачого генерала М. Козіцина 3 травня 2014 року двома вантажівками перетнули кордон України та взяли під контроль місто Антрацит. На Луганщині угруповання донських козаків склало до 4 тисяч осіб. Їм вдалось закріпитися в містах Северодонецьк, Лисичанськ, Красний Луч, Свердловськ, Алчевськ. Використання козаків підпало під формулювання параграфу g) статті 3 «Визначення агресії» Резолюції № 3314 Генеральної Асамблеї ООН від 14 грудня 1974 року.

Військове козаچه товариство «Всевеликое Войско Донское», яке діє в Україні, включає більше 135 000 козаків, які знаходяться на державній службі відповідно до Федерального закону від 5 грудня 2005 р. № 154-ФЗ «Про государственную службу российского казачества». Статут товариства затверджений Указом Президента РФ від 17 червня 1997 р. № 612. Тобто, фактично козачі угруповання є підконтрольною Кремлю силою. Вони беруть активну участь у гібридних війнах РФ в усьому світі. Так, спеціально для повалення влади у Чорногорії та недопущення її вступу в НАТО, а також для встановлення контролю Кремля над виходами до Адріатичного моря був створений «Союз козаків Балкан», Балканське козаچه військо». Козаки фігурували в Придністров'ї, в Абхазії та Південній Осетії.

Практично на однаковому відділенні від кордонів України та країн Балтії, в м. Наро-Фомінськ РФ дислокується кантемирівська дивізія, у якій служать козаки. Вони регулярно проходять військову підготовку під керівництвом Головного управління Генерального штабу Збройних сил Російської Федерації, в т.ч. для бойових дій в умовах міста. Їх назвали таємною зброєю Росії, їх забезпечують сучасною зброєю та організовують для них навчання. Вони будуть першими у вторгненнях, попередньо проникнувши у суміжні раїни через культурологічні організації та релігійні громади.

У травні 2013 року у Балтії була заснована зарубіжна структура Окремого Північно-Західного козачого округу - Посольська станиця, яка входить у склад Санкт-Петербурзького міського козачого товариства «Императорский конвой». Її отаманом став «родовий» кубанський козак Юрій Канишев. Фактично розпочалось укорінення козачих сил в країнах Балтії за аналогією з подіями, що відбулись на Балканах.

Козаки товариств Санкт-Петербурга та Ленобласті активізувались в прикордонні з балтійськими країнами. Для прикладу, 22 липня 2017 р., в 525-річчя м. Івангороду за інформаційного супроводження інтернет-порталу 47news.ru. «Зеленые человечки» козаки демонстрували зразки сучасної зброї та бойової техніки РФ, організовували тренування з розбирання та збирання автоматів Калашникова. Був розгорнутий мобілізаційний пункт для бажаючих вступити на службу у Збройні сили РФ. Козаки на тлі естонської фортеці Нарва організували акт групового фотографування, позуючи з шашками, автоматами, прапорами Росії та козачих товариств. Вони провели «Казачий круг», прийнявши рішення про заснування первинної козачої організації «Станица Принаровская», створивши на кордоні з Естонією воєнізо-

вану організацію, за умовами роботи якої передбачений набір як мешканців РФ, так і країн Балтії.

Зауважимо, що створення й підтримка парамілітарних груп, які регулярно проходять збори з ідеологічної, політичної й спеціальної підготовки на території суміжної держави вже є ознакою жовтого рівня гібридної війни. А саме в такому форматі діє Принаровська станиця в РФ та Посольська станиця в Естонії.

Наступний помаранчевий рівень позначає: посилення активності військової розвідки суміжної держави на території сусіда; концентрація збройних сил та засобів у ближній зоні, проведення військових навчань біля кордонів. Як ми розуміємо, ці ознаки теж фігурують на сучасному етапі гібридної війни проти країн Балтії. Після цього локалізується наступний, червоний рівень, сумісний з появою: загонів самооборони, козачих підрозділів (такі вже наявні, принаймні, в Естонії), приватних військових формувань, неідентифікованих мілітарних груп («зелених чоловічків»).

Виходячи з викладеного, країни Балтії знаходяться між помаранчевим та червоним рівнями гібридної війни Російської Федерації.

Значить, далі буде ...

Морозов О. М.

доктор медичних наук, професор,
почесний академік НАПН України,
заслужений діяч науки і техніки України,
Національна академія СБ України

ДЕМОГРАФІЧНА СКЛАДОВА СИСТЕМНОЇ (ГІБРИДНОЇ) ВІЙНИ

Війна завжди була, є і буде сполученням багатьох складових. Перед тим, як розпочинається збройний конфлікт противник намагається вплинути на ворога в інший спосіб: застосувати політичний тиск, ізолювати на міжнародній арені, ослабити економічно, розкласти його армію пропагандою, розхитати суспільство в середині держави. Особливість кожної з воєн полягає лише в питомій вазі застосування кожного з засобів впливу. В одному випадку активніше застосовувався економічний вплив, в другому – психологічний, в третьому – соціальний, у четвертому – зброя, а у п'ятому – демографічний фактор. Можливими є різноманітні сполучення названих складових, напри-

клад, одночасне їх застосування або розтягування в часі однієї з складових та багато інших варіантів. Центральний зміст поєднання різних засобів впливу на противника полягає не тільки в тому, що удари по різних вразливих точках швидше послаблюють його, а й перш за все у тому, що кожен із засобів впливу посилює ефективність іншого, а правильне їх поєднання (синергія) підвищує загальну ефективність впливу і руйнівний ефект в цілому, прискорює досягнення остаточного результату з меншими ризиками і втратами. Таку війну ми називаємо системною. Визначення може звучати наступним чином: системна війна – це форма протиборства, яка базується на сполученні декількох складових, зокрема, економічної, психологічної, соціальної, демографічної та фізичної, які побудовані за принципом взаємодії між собою (синергії), посилюють одна одну і дозволяють досягнути більшого результату в коротший термін і з меншими втратами (принцип « $1+1=3$ »).

Розглянемо сутність демографічної складової системної війни. Демографічна складова є п'ятою складовою системної війни та полягає в біологічному протиборстві різних рас, народів, національностей на кшталт боротьби за виживання в тваринному світі. Головною її умовою є наявність у агресора значних людських ресурсів, а технологія передбачає повільну інфільтрацію території противника населенням агресора, а у подальшому винищення непокірної частини корінного люду. Населення, яке агресор використовує для інфільтрації чужої території як правило є етнічно, культурно та ментально однорідним і відрізняється від корінного народу. Аналіз показує, що формування «п'ятої колонії» чисельністю в 20% від чисельності корінного населення, згуртування «п'ятої колонії» за релігійною ознакою, в різноманітні земляцтва, громадські, культурні та спортивні організації, дитячі гуртки за етнічним та мовним принципом, а також належна підтримка з метрополії дозволяє «поставити на коліна» атаковану країну, примусити її підкорятися інтересам агресора. Протистояння активній, організованій «п'ятій колонії» потребує жорстких, тривалих заходів на які здатен не кожний народ, не кожний уряд і не кожен лідер країни.

Єдиним недоліком з точки зору агресора такої повзучої інфільтрації (окупації) є її тривалість, яка може розтягнутися на роки. Водночас абсолютною перевагою демографічної перемоги є її стійкий результат. Якщо агресору вдалося суттєво змінити демографічний ландшафт на території противника то він стає повним володарем цих територій на сторіччя.

У середині великих імперій демографічна боротьба має дещо інший характер. Населення титульної імперської національності, кероване вождями імперії, всіляко укріплює свій статус панівного народу. Проводиться жорстока денационалізація загарбаних народів, руйнується їх культура, мова, спосіб життя, спотворюється історія, а разом з цим зникають національна гордість та людська гідність, виникають меншовартість, підкорюваність, легіони холопів (рабів) та холуїв (хитрих рабів). Зокрема на українських землях починають зростати хохли, малороси, «русские казаки» – які вірно служать окупанту і стають та жорстокими карателями власного народу.

Безперервно відбувається «перемішування» народів – масові насильницькі переселення цілих етносів у віддалені пустельні райони імперії, на великі будівництва, до концентраційних таборів, які перетворюються в окремі країноподібні утворення (ГУЛАГ) на кшталт Мордовії де в різні часи панування московської влади кількість репресованого та переселеного люду перевищувала кількість корінного населення країни. Той хто чинить опір просто винищується (голодомори, тотальний терор, масове винищення).

Прикладом демографічної боротьби можуть слугувати дії СРСР проти Литви, Латвії та Естонії де російська діаспора, яка не піддається інтеграції та активно протидіє прагненню цивілізованого корінного народу до незалежності і добробуту, складає від 20 до 30 відсотків населення.

Яскравим прикладом слугує і Україна куди замість винищеного голодоморами, війнами, масовими депортаціями українців завозилися представники «русского мира» – напівдикі чужорідне населення з північних глибин імперії взуте у березові лапті з дерев'яними дощечками замість підошви, вбране у тулупи, підперезані мотузками та з малахаями на голові, не здатне до сприйняття прогресивного вільного способу життя. Незважаючи на те, що сьогодні представники цієї діаспори зовні скидаються на розвинутих людей насправді вони в середині незмінно залишаються представниками примітивної ментальності. Таки діаспори стають непримиренними ворогами титульного народу, тягарем і нездоланною греблею перед динамічним культурним та економічним розвитком країн. Таким є результат етнічних зачисток цілих регіонів країни.

Ще одним прикладом може бути інтенсивна інфільтрація мешканцями Китаю східних регіонів РФ, західних регіонів Канади, окремих територій Австралії та Нової Зеландії. Як подібне явище можна розглядати інфільтрацію представниками мусульманського світу Західної

Європи де народжується вже третє покоління емігрантів, яке не знає і знати не хоче мови країни, яка їх прихистила і годує. Вони намагаються силою насаджувати таку культуру, релігію і спосіб життя від якого колись тікали їх діди і батьки. Інфільтрація сходу РФ сягнуло такого рівня, що уряд РФ був змушений віддати в «оренду» Китаю територію, яка у двічі більше території окупованого РФ Криму. На Далекому Сході РФ збільшується кількість шкіл та вишів з викладанням китайською мовою. Поки РФ намагається інфільтрувати Україну її терени успішно інфільтрує Китай.

Одним з актуальних сьогодні прикладів демографічної інфільтрації є контрольований білоруською владою багатотисячний приплив утікачів з Африки та арабського світу до прибалтійських країн. Литовці, латвійці та естонці, які і так знаходяться в небезпечній зоні національного переродження, можуть опинитися в ще більш скрутному становищі. Б'ють на сполох політики та науковці деяких країн у зв'язку з можливим масовим нашествям утікачів з Афганістану.

Слід зауважити, що масові переселення людей, втечу від тиранічних режимів, голоду та воєн деякі країни почали свідомо використовувати як зброю проти інших країн.

Протидіяти демографічній інфільтрації в сучасних умовах вкрай складно. Засобів протидії натовпам голодних, хворих, виснажених людей з малими ослабленими дітьми на руках практично не існує. Їх не зупиняють а ні високі паркани, а ні колючий дріт, а ні злі собаки прикордонників, а ні постріли у повітря. На ураження ніхто стріляти не буде. Пропагандистські кампанії, розгорнуті у ЗМІ щодо «фашистів», котрі не хочуть допомагати нещасним дітям ще більш обмежують засоби припинення потоку переселенців. Де-факто, цих нещасних агресори використовують як худобу.

Викладене дозволяє зробити наступний висновок:

1. Сутність демографічної складової системної війни полягає в інфільтрації території противника населенням агресора та його організації в монолітну «п'яту колону», здатну ефективно та всебічно впливати на внутрішнє життя атакованої країни на користь агресора.

2. Демографічна агресія відбувається протягом тривалого часу але дає агресору стійкий бажаний результат.

3. Протидіяти демографічній інфільтрації в сучасних умовах панування «демократії» та ЗМІ вкрай складно.

Паливода О. О.
кандидат психологічних наук,
Національна академія СБ України

ВИКОРИСТАННЯ МАНІПУЛЯТИВНИХ МОЖЛИВОСТЕЙ ІНТЕРНЕТУ ТА НОВИХ МЕДІА В ПРОВЕДЕННІ СУЧАСНИХ ГІБРИДНИХ ВОЄН

В умовах надзвичайного збільшення ваги мережевих та медіа технологій у формуванні суспільної думки, неможливо оминати важливість аналізу інформації, що розповсюджується засобами масової комунікації. Адже, такий канал інформування суспільства, окремих груп населення наразі може бути як фактором дестабілізації ситуації в певних верствах населення, регіонах, країнах тощо, так і забезпечувати консолідацію громади на вирішення важливих суспільних проблем. Варто згадати лише деякі факти із недавнього минулого, коли завдяки використанню соціальних мереж організовувались масові протести (у тому числі проти злочинних дій окремих владних структур або представників політичного істеблішменту). Так у січні поточного року навіть російський сегмент соціальної мережи TikTok, яка до того була досить аполітичною, був використаний для агітації до участі у мітингах на захист російського політика Олексія Навального проти корупції Путіна (після публікації інформації про «таємний палац вождя з золотими йоршиками»). Або згадати активні закриття сторінок Трампа та його прихильників на платформах великих соціальних мереж (Twitter, Facebook, YouTube та ін.) після штурму останніми Капітолію США, який сколихнув не тільки Америку, але й весь світ.

На сьогодні, маніпулятивні впливи на певні групи людей (цільові аудиторії, окремі верстви населення тощо) здебільшого здійснюються через засоби масової інформації (мас-медіа), які наповнені великою часткою саме деструктивних інформаційно-психологічних впливів. Є і відкрито пропагандистські телерадіоканали, серед яких і російські, які зокрема підпали під запроваджені у 2015 році українські санкції і продовжені у 2018-2021 роках («Перший канал. Всесвітня мережа», Телекомпанія «НТВ», телеканали «РТР-Планета», інформаційний канал «Росія-24», які входять до структури Федерального державного унітарного підприємства «Всеросійська державна телевізійна і радіомовна компанія» тощо [1]), а також українські із так званої «трійки Медведчука» (телеканали 112, NewsOne та ZIK) [2]. Шляхом розпов-

сюдження пропагандистських ЗМІ на сьогодні активно стають і соцмережі та месенджери. Сучасна людина за допомогою гаджетів переглядає стрічки новин, статті, слідкує за життям людей, знаменитостей, громадських та політичних діячів у соцмережах, веде власні блоги, ділиться актуальними посиланнями, спілкується в чатах, залишає відгуки та коментарі про оприлюднені факти, події тощо. Усе це відповідно відкриває широкі можливості для формування, аналізу, прогнозування громадської позиції, думок і переконань. І відповідно, маніпулювання інформацією за допомогою створення підґрунтя для змін світогляду та поведінки.

Так, директор служби безпеки Facebook Алекс Стамос у повідомленні щодо можливого втручання Росії у вибори у США 2016 року наголосив, що Росія могла впливати на користувачів через рекламу у соцмережі. Він стверджував, що у компанії було знайдено приблизно 470 фейкових акаунтів та сторінок з Росії, які розміщували провокаційні оголошення [3]. А у жовтні 2020 року засновник компанії Facebook Марк Цукерберг, коментуючи американські президентські вибори 2020 року, заявив: «Ми не можемо зупинити такі країни, як Росія, від спроб втрутитись у вибори... Але ми створили системи, які забезпечують можливість набагато швидшого виявлення випадків, коли вони роблять спроби (втручання у вибори)... і це має вселити в жителів країни «високий ступінь довіри» [4].

Загалом, в сучасних умовах надзвичайного поширення маніпулятивних і пропагандистських впливів керівництво різних країн та представники медіа- та інтернет компаній активно об'єднуються у боротьбі із поширенням фейків й організованих спрямованих дезінформаційних компаній, що реалізуються у різних засобах комунікації. Приймається чимало юридичних та методичних документів, що спрямовані на упорядкування верифікації інформації, яка циркулює в медіапросторі, перевірки інформаційних повідомлень, організації системи моніторингу та протидії з урахуванням дотримання принципів демократії та свободи слова.

Так, у 2016 році Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу», а депутати Європарламенту ухвалили Резолюцію «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін», у якій містяться положення про співпрацю з НАТО у протидії ворожій Євросоюзу пропаганді [5]. На офіційному сайті НАТО також йдеться про співпрацю Альянсу з Європейським союзом, ООН, Великою сімкою (G7) і громадянським суспільством у боротьбі із дезінформацією. Надаються там і поради пе-

ресічним громадянам щодо основних правил фактчекінгу, які дозволяють убезпечити себе від маніпуляцій. Варто зазначити, що скільки б не було запропоновано правил перевірки достовірності інформації (серед різних публікацій їх налічують від 5 до 9 [6-9]), всі вони фактично налаштовують споживача на обов'язковість критичного ставлення до будь-якої інформації, що потрапляє у його поле зору. Адже, будучи активним користувачем віртуальної реальності – соціальних мереж, різноманітних блогів, форумів, груп за кругом інтересів тощо, людина отримує з неї актуальну їй інформацію або ж таку, що визначили актуальною. І частка отримувачів інформації через мережеві канали з кожним днем стає все більшою. Як показало опитування, проведене у 2017 році, велика частина респондентів в Україні (41 %) читає новини лише в Інтернеті, і тільки 28 % опитуваних дивляться новини по телевізору, 12 % – слухають по радіо, 9 % – читають газети (найстарша категорія опитуваних загалом), а 10 % опитуваних вибрали свій варіант відповіді, – зазвичай це була комбінація Інтернету з іншим видом ЗМІ [10]. Ця тенденція активно використовується при поширенні не тільки комерційної чи політичної інформації, але й повідомлень терористичного, деструктивного, дестабілізуючого спрямування.

Отже, підсумовуючи вищевикладене, зазначимо: на сьогодні зростання значення у повсякденному житті віртуальної культури, активне застосування мережевих технологій, завдяки чому реальність тісно переплітається із подіями віртуального світу, знищуються кордони між державами, соціальними верствами, нівелюється ментальні, демографічні, психологічні відмінності конкретних особистостей, поряд із позитивними змінами несуть і небезпеку. Інтернет знищує особистісний простір людини, призводить до зростання уразливості особи щодо маніпулятивних впливів, сприяє трансформації свідомості та формуванню специфічного світобачення. Саме тому, на сьогодні надзвичайна популярність Інтернету як засобу комунікації та спілкування людей з різних частин не лише однієї країни, а й світу актуалізує питання виявлення та протидії розповсюдження фейкової чи екстремістської інформації, попередження негативних змін та зростання соціального напруження. Це зумовлюється й тим фактом, що комунікація в Інтернеті ґрунтується на кардинально нових принципах. Налаштованість користувачів мережі на довіру, симпатію, співчуття й розуміння знижує рівень критичності в сприйнятті інформації. Саме тому нагальною постає проблема формування вміння аналізувати значний обсяг інформації з метою вчасного виявлення ознак дестабі-

лізації обстановки, виокремлення осіб, причетних до розповсюдження негативної інформації, ініціаторів та об'єктів впливу.

Література

1. Указ Президента України № 126/2018 «Про рішення Ради національної безпеки і оборони України від 2 травня 2018 року «Про застосування та скасування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».
2. Указ Президента України № 43/2021 «Про рішення Ради національної безпеки і оборони України від 2 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».
3. У Facebook заявили про можливий вплив Росії на користувачів через рекламу у соцмережі – ТСН, 7 вересня 2017 року URL: https://tsn.ua/nauka_it/u-facebook-zayavili-pro-mozhliivy-vplyv-rosiyi-na-koristuvachiv-cherez-reklamu-u-socmerezhi-9987353.htm. (дата звернення 12.05.2021).
4. Facebook не може припинити спроби втручання РФ у вибори в США – Цукерберг / Інститут масової інформації. – URL: <https://imi.org.ua/news/facebook-ne-mozhe-prypynyty-sproby-vtruchannya-rf-u-vybory-v-ssha-tsukerberg-i35921> (Дата звернення 24.05.2021).
5. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України URL: <http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf> (дата звернення 20.05.2021).
6. Поради НАТО: як виявляти дезінформацію та протидіяти фейкам. – 2020. – URL: <https://armyinform.com.ua/2020/10/porady-nato-yak-vyyavlyaty-dezinformacziyu-ta-protydiyaty-fejkam/> (дата звернення 14.04.2021).
7. Пропаганда. Виявлення та Протидія. – 2019. – URL: <https://www.nato.int/cps/uk/natohq/177273.htm> (дата звернення 14.05.2021).
8. Довіряй, але перевіряй. Медіаграмотність в українському суспільстві. – К. : Pictoric, 2017. – 136 с., іл., С. 98, 99
9. Як розпізнати фейкову новину в соцмережах – рекомендації The Huffington Post [Електронний ресурс] // Media Sapiens. – 2016. – 23.11. – URL: http://osvita.mediasapiens.ua/web/online_media/yak_rozpiznati_feykovu_novinu_v_sotsmerezkhakh_rekomendatsii_the_huffington_post. (дата звернення 16.02.2021).
10. Кіца М. Особливості та методи виявлення фейкової інформації в українських ЗМІ / Мар'яна Кіца // Вісник Національного університету «Львівська політехніка». Серія: Журналістські науки. – Львів : Видавництво Львівської політехніки, 2017. – № 883. – С. 28–32.

ОКРЕМІ АСПЕКТИ ІМПЛЕМЕНТАЦІЇ МІЖНАРОДНОГО ЗАКОНОДАВСТВА ПРО КІБЕРБЕЗПЕКУ У НАЦІОНАЛЬНИЙ ПРАВОВИЙ ПРОСТІР

До числа фундаментальних міжнародно-правових документів, котрий регулює, зокрема, і питання кібернетичної безпеки, належить прийнятий у 1992 році засадничий документ спеціалізованої установи ООН – Статут Міжнародного союзу електрозв'язку (МСЕ) [1], до якого приєдналися всі держави-члени ООН, в тому числі й Україна. Статут регулює комплекс питань міжнародної співпраці у сфері використання телекомунікацій, розвитку засобів та підвищення ефективності відповідних послуг, визначає чинники, котрі заважають функціонуванню існуючих телекомунікаційних мереж, тощо.

З метою оцінювання участі держав у галузі кібербезпеки на світовому рівні, підвищення поінформованості про важливість цих проблем та їх різні виміри МСЕ щороку оприлюднює так званий глобальний індекс кібербезпеки, котрий базується таких критеріях глобального прогресу у цій сфері: законодавчі заходи; технічні заходи; організаційні заходи; розбудова потенціалу; кооперація. Зазначимо, що обґрунтовані висновки МСЕ користуються широкою довірою.

Перша частина спільного законодавства ЄС про кібербезпеку – Директива щодо мережевої та інформаційної безпеки (Директива NIS) була ухвалена Європарламентом у 2016 році [2]. Правові заходи, передбачені Директивою, спрямовані на радикальне підвищення в Європейському Союзі загального рівня кібербезпеки (шляхом проведення відповідних операцій Групою реагування на інциденти, пов'язані з комп'ютерною безпекою, – CSIRT або CERT – та компетентним органом у галузі мереж та інформаційних систем), а також активізацію міжнародної співпраці й розвитку безпекової культури стосовно інформування відповідно до директивних вимог. Задля допомоги якнайшвидшій узгодженій реалізації державами-членами ЄС Директиви вона має додаток, де наведено найефективніший практичний досвід, пояснення та тлумачення, – так званий Інструментарій NIS (NIS Toolkit).

Ця Директива не є обов'язковою для України, котра поки що не входить до Євросоюзу, проте окремі її положення беруться до уваги у

правозастосовній практиці, а деякі були частково впроваджені у вітчизняне законодавство. Вбачається, що імплементацію Директиви NIS можна провести в рамках механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом. У теперішній час у Верховній Раді України зареєстровано законопроект, спрямований на приведення законодавства України у відповідність до Європейського. Це стосується і Директиви NIS (аналіз законопроекту наводиться у розділі Законодавчий рівень. Закон про кібербезпеку). Крім того, деякі вимоги Директиви вводять до розроблюваних законопроектів Державна служба спеціального зв'язку та захисту інформації України. Водночас її фахівці вважають, що при розробці загальних законів у сфері кібербезпеки відповідно до положень Директиви NIS буде вельми потрібною міжнародна допомога.

У виробленні єдиних підходів у сфері забезпечення кібернетичної безпеки як складової національної безпеки держав-учасниць значну роль відіграє Організація Північноатлантичного договору (НАТО). Цей напрям став одним із пріоритетних напрямів діяльності Альянсу з огляду на вразливість вказаної сфери, численність і різноманітність відповідних викликів і загроз [3, с. 42].

Нагальне завдання розбудови національної системи кібернетичної безпеки, спроможної ефективно протидіяти загрозам національній безпеці у кібернетичній сфері, стоїть сьогодні й перед нашою державою. Дедалі частіше на кібернетичні атаки й злочини наражаються державні, фінансові установи, підприємства енергозабезпечення і транспорту та інших об'єктів критичної інфраструктури. І, як засвідчив аналіз стану кібербезпеки в Україні, ця складова національної безпеки має високий ступінь уразливості від кіберзагроз і залишається вельми слабкою.

Відповідно до укладених міжнародних угод у сфері кібербезпеки Україна співпрацює з іноземними державами, їхніми збройними силами, правоохоронними органами і спецслужбами, а також із багатьма міжнародними організаціями. У цьому контексті одним із пріоритетних напрямів міжнародного співробітництва у цій сфері вбачається активна діяльність України у структурах ООН, стратегічне партнерство з Організацією Північноатлантичного договору та Європейським Союзом.

Література

1. Статут Міжнародного союзу електров'язку. URL: <https://www.itu.int/council/pd/constitution.html>.

2. Директива щодо мережевої та інформаційної безпеки (Директива NIS). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

3. Войціховський А.В. Кібербезпека як напрям євроатлантичної інтеграції України. Право і безпека у контексті європейської та євроатлантичної інтеграції : зб. статей та тез наук. повідомл. за матеріалами дискус. панелі

4. ІІ Харків. міжнар. юрид. форуму, м. Харків, 28 верес. 2018 р. / редкол.: Ю.Г. Барабаш, Т.М. Анакіна, Д.В. Аббакумова. Харків : Право, 2018. 190 с.

**Ткаченко О. П.
Сидоренко С. М.**

Національна академія СБ України

ПРАВОВІ МЕХАНІЗМИ СПІВРОБІТНИЦТВА СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ІЗ СПЕЦІАЛЬНИМИ ТА ПРАВООХОРОННИМИ ОРГАНАМИ КРАЇН ЄВРОСОЮЗУ У СФЕРІ ПРОТИДІЇ МІЖНАРОДНІЙ КІБЕРЗЛОЧИННОСТІ

Однією із загроз національній безпеці, яка використовується спецслужбами Російської Федерації в якості складової «гібридної війни» проти України є транснаціональна кіберзлочинність.

До заходів міжнародного співробітництва у сфері протидії транснаціональній кіберзлочинності Служба безпеки України почала залучатися у 2009-2011 роках.

Починаючи з 2011 року, після прийняття Верховною Радою України Закону України «Про Конвенцію Ради Європи з кіберзлочинності», активізувалося співробітництво СБ України з Комітетом Конвенції Ради Європи з кіберзлочинності.

У 2012 році СБ України, за активної участі європейських партнерів, підготувала перший проект «Стратегії кібербезпеки України», який був погоджений ЄС та НАТО і направлений на розгляд РНБО України.

Революція Гідності надала додатковий імпульс правовому регулюванню співробітництва Служби безпеки України із спецслужбами та правоохоронними органами країн-членів ЄС.

Зокрема, в рамках Європейської політики сусідства у форматі проектів, Кабінет Міністрів України розпорядженням № 847 від 17 вересня 2014 року затвердив План заходів з імплементації Угоди про асоціацію між Україною та Європейським Союзом.

Головним правовим інструментом ЄС у сфері протидії міжнародній кіберзлочинності на сьогоднішній день є Конвенція Ради Європи з кіберзлочинності, прийнята у 2001 році. Конвенція вступила в дію 2004 року. Станом на липень 2020 року до Конвенції приєдналося 65 країн. Учасниками Конвенції є країни не тільки країни – члени Євросоюзу, а й Азії (Японія, Шрі-Ланка), Америки (США, Аргентина, Чилі), Африки (Сенегал), Австралії тощо. Наразі це єдиний міжнародний, реально діючий механізм протидії кіберзагрозам.

Іншими законодавчими актами, прийнятими ЄС для протидії транснаціональній кіберзлочинності є: Директива ЄС щодо протидії кібератаками на інформаційні системи (2013 р.), Директива ЄС стосовно боротьби з сексуальною експлуатацією дітей он-лайн та дитячою порнографією, (2011р.), Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет (2017 р.).

Питання протидії міжнародній кіберзлочинності в форматі ЄС викладені у Стратегії кібербезпеки ЄС, ухваленій у 2013 році.

Виконавчим органом Конвенції – Комітетом Конвенції в червні 2017 року прийнято рішення щодо доцільності укладання додаткового протоколу до Конвенції. Результатами ухвалення вказаного протоколу стануть поглиблена взаємодія із світовими провайдерами Інтернет послуг, створення спільних слідчих робочих груп з розслідування кіберзлочинів, протидія кібербулінгу тощо.

З метою адаптації національного законодавства до європейських стандартів, Служба безпеки України у 2018 році спільно з Національною поліцією України, Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, іншими зацікавленими міністерствами та відомствами України, взяла участь у розробці проекту Закону України «Про внесення змін до деяких законодавчих актів щодо імплементації положень Конвенції про кіберзлочинність».

Враховуючи практичний досвід, розвинену інфраструктуру, ефективні правові механізми спецслужб та правоохоронних органів країн-членів ЄС, співпраця Служби безпеки України із зазначеними структурами є не тільки можливою і доцільною, а корисною і необхідною.

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО АСПЕКТУ ГІБРИДНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [1].

Одним із проявів інформаційної складової гібридної війни сьогодні є здійснення масових “вкидів” у вітчизняний інфопростір, що мають на меті викривлення реалій українського життя, підриг довіри до управлінських структур, а також переконання у безперспективності української державності тощо.

Специфіка цієї складової гібридної війни РФ проти України полягає в:

- інтенсивності та широті охоплення аудиторії інформаційних впливів, яка набула глобального масштабу;
- систематичному й комплексному застосуванні медійних та новомедійних засобів;
- створенні нового дискурсу війни, спрямованого на руйнування існуючих і формування нових інтерпретаційних та смислових механізмів сприйняття дійсності [2].

Слід зауважити, що інновацією сучасної інформаційної складової гібридної війни є дедалі ефективніше і всеохоплююче проникнення в інфопростір об'єкта агресії за допомогою сучасних технологій і, як результат – підвищення ефективності інформаційного впливу на його населення.

Очевидно, що в умовах триваючого гібридного протистояння забезпечення інформаційної безпеки України має включати не лише захист вітчизняного інформаційного простору від негативних впливів, а й створення та використання власних інформаційно-аналітичних продуктів, які виявлятимуть недоліки та прорахунки у суспільному житті противника.

На сьогодні українські інформаційно-аналітичні матеріали, які протиставляються російській пропаганді, зводяться здебільшого до засудження агресії РФ на сході нашої країни, а також до вимог щодо повернення територій Донбасу та Криму, проте майже не приділяється увага реаліям сьогодення Російської Федерації.

Проте в Росії існує чимало проблем, які не мають широкого розголосу серед населення, проте які могли б висвітлювати українські джерела інформації, сприяючи таким чином об'єктивному відображенню реалій російської дійсності і в глобальному інформаційному просторі, і серед населення РФ. До її істотних проблем можна віднести відсутність чіткої перспективи розвитку та орієнтирів у майбутньому, а також фактичне обмеження розвитку економіки Росії інтересами її олігархічних монополій, зацікавлених здебільшого у використанні багатих сировинних ресурсів країни тощо.

Розглядаючи РФ як об'єкт інформаційних впливів в рамках гібридної війни останньої проти України, також варто мати на увазі ще одну її особливість – сучасна Росія є однією з найбільших мультинаціональних держав, на території якої проживає понад 190 народів. Крім росіян до їх числа входять не лише малочисельні корінні народи, а й представники багатьох інших національностей, які раніше входили до складу СРСР, і чи не найбільша кількість – вихідці з України. Хоча їх вважають росіянами вже не одне покоління, проте в їхній самосвідомості все ще може зберігатися український етнічний елемент. Цю обставину слід враховувати при підготовці інформаційних продуктів, що орієнтовані на регіони, населені, ментально близькими нам мешканцями РФ, а також при підготовці інформаційно-аналітичних матеріалів, спрямованих на нейтралізацію зарубіжних інформаційних впливів на населення України.

Таким чином, варто правильно зосередити зусилля на здійсненні інформаційного впливу на найбільш податливу частину аудиторії противника. Крім того, доцільно висвітлювати проблеми та слабкі сторони РФ з метою створення об'єктивної “картини світу” в свідомості її населення.

Література

1. Доктрина інформаційної безпеки України, затверджена Указом Президента України № 47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 02.07.2021).

2. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. К.: НІСД, 2017.

ВИКОРИСТАННЯ МЕСЕНДЖЕРУ VIBER З МЕТОЮ ПОШИРЕННЯ ДЕСТРУКТИВНОГО ТА «ФЕЙКОВОГО» КОНТЕНТУ

За результатами аналізу початку та перебігу т.зв «Кольорових революцій», протестних акцій, які систематично відбуваються на території Європейського Союзу, подій в районі проведення операцій об'єднаних сил (далі ООС; фактично «гібридної війни») свідчить, що поширення фейкового контенту (аналіз вказаного поняття нами було наведено у попередніх роботах [10; 9; 1] в ході проведення спеціальними та розвідувальними службами Російської Федерації інформаційних операцій, призводить до вчинення громадянами антидержавних дій [4]. При цьому, в контексті забезпечення інформаційної безпеки України, потрібно враховувати, що наша держава відноситься до переліку країн, які найбільш піддаються інформаційними маніпуляціями з боку країни-агресора [8].

Вказані негативні наративи досить часто поширюються за допомогою месенджерів. Вказане обумовлено можливістю оперативного донесення до широкого кола громадян деструктивного контенту.

За результатами відповідних досліджень було встановлено, що станом на квітень 2021 року найбільш поширеним серед населення додатком для обміну інформацією став Viber, яким користуються майже 66% респондентів. Він лідирує серед усіх вікових груп. На вказаній позиції перебуває з 2018 року [6].

Друге місце посідає Facebook Messenger, який використовують майже 35% опитаних. Проте лідирує додаток не скрізь. У віковій категорії «18-29 років» друге місце займає Telegram, який використовують 45% користувачів. Також у віковій групі «70 років і старші» опитані більше користуються WhatsApp, ніж Facebook Messenger.

Третє місце за кількістю користувачів займає Telegram – йому довіряють 24,2% користувачів.

Четверте та п'яте місце займають WhatsApp та Twitter відповідно [7].

Зважаючи на об'єм доповіді та поширеність серед користувачів, вважаємо за доцільне більш детально зупинитися на характеристиці саме месенджеру Viber.

Отже, Viber є додатком для дзвінків і обміну повідомленнями, який дозволяє створювати чат-боти та спільноти тощо [3].

Незважаючи на те, що вказаний додаток є для значного відсотку українців джерелом новинної інформації, за своїми ознаками він є аналогом SMS-повідомлень (більш «прогресивна» версія).

Його поширеність та популярність обумовлена тим, що він став одним із перших каналів комунікації, який почали масово використовувати українці після стандартних текстових SMS. Зважаючи на те, що першочергово ми писали рідним, близьким людям, друзям у Viber, на підсвідомому рівні, сформувалося коло людей, яким ми довіряємо (т.зв. «коло довіри»). Разом з тим, в умовах сьогодення, месенджер перестав використовуватися виключно як «інструмент для спілкування», а став платформою для «викривлення інформаційного поля».

Наразі, вказане «коло» значно розширилося. У більшості користувачів в додатку є значна кількість чатів (спільнот) з тисячами учасників. Зважаючи на вказане, фізично відсутня можливість ідентифікувати осіб, які розміщують відповідні дописи. При цьому, психологічно, ми продовжуємо сприймати Viber як «зону безпеки». Вказана підсвідома реакція людського мозку активно використовувалася з метою оперативного поширення тенденційної інформації задля впливу на вільне волевиявлення громадян.

Яскравим прикладом деструктивного впливу через додаток може слугувати ситуація з підбуренням 20 лютого 2020 року місцевого населення в смт Нові Санжари (Новосанжарський район Полтавської області) до антигромадських виступів внаслідок незадоволення рішенням керівництва держави щодо поселення для обсервації на території вказаного населеного пункту евакуйованих українців з міста Ухань (Китайська Народна Республіка), яке стало епіцентром поширення коронавірусу [5].

Доведено, що з метою швидкого розповсюдження вказаної інформації та штучного підняття інтересу до неї активно застосовувалися технічні можливості ботоферм, в тому числі й тих, які розміщувалися на території РФ. Вказане обумовлено тим, що, наразі, в месенджері, існує значна кількість груп (спільнот), з великою кількістю учасників. При цьому, відсутні ефективні інструменти, які були б доступними користувачам та дозволили ділити аудиторію на ботів і не ботів [2].

Проаналізувавши психологічні та технічні прийоми, які використовуються зловмисниками при підготовці та поширенні у додатку фейкового чи деструктивного контенту, можна зробити висновок, що вони, в першу чергу, використовують властивість людської психіки обумовлену бажанням вберегти від небезпеки своїх близьких та рідних (як вже зазначалося: на підсвідомому рівні Viber = «коло довіри»).

Модель формування «фейкового повідомлення» для вказаного месенджеру, на нашу думку, є наступною:

1) є особа, яку неможливо ідентифікувати («чиновник, який має доступ до інформації з обмеженим доступом», «людиною з народу, яка працює на режимному об'єкті» тощо);

2) їй стає відома інформація «не для усіх» (ексклюзивні дані);

3) їх повідомляють, на умовах таємності, конкретному абоненту, або ж, навпаки, усім для того, щоб «врятувати людство»;

4) використовуються боти для створення штучного ажіотажу навколо новини, збільшення кількості вподобань, поширень тощо;

5) з метою провокування «стадного інстинкту» новина шириться у відповідних групах/спільнотах, в яких є значна кількість учасників (при цьому, неважливо боти вони чи реальні користувачі). На підсвідомому рівні спрацьовує уявлення: чим чисельніша аудиторія, тим об'єктивнішим є канал поширення новини.

Підсумовуючи викладене можемо дійти висновку, що зважаючи на розвиток інформаційних технологій та намагання представників спеціальних служб оперативно ширити деструктивну чи фейкову інформацію в протиправних цілях, в короткостроковій перспективі месенджери використовуватимуться все частіше.

Основні зусилля органів державної влади та місцевого самоврядування повинні бути спрямовані на формування у населення «критичного мислення», яке дозволить «фільтрувати» інформацію, завдяки якому інформація, що шириться не від імені суб'єктів владних повноважень, піддаватиметься сумніву та перевірятиметься усіма доступними засобами.

Вказане, в свою чергу унеможливить вплив сторонніх осіб (співробітників спеціальних іноспецслужб) на політичні, економічні, соціальні процеси, які відбуваються в середині України.

Література

1. Olena V. Sviatun, Olga V. Goncharuk, Chernysh Roman, Olena Kuzmenko, Ihor V. Kozych. Combating cybercrime: economic and legal aspects. WSEAS Transactions on Business and Economics, ISSN / E-ISSN: 1109-9526 / 2224-2899, Volume 18, 2021, Art. #72, pp. 751-762. DOI: 10.37394/23207.2021.18.72.

2. Roman F. Chernysh, Viktoriya L. Pogrebnaya, Iryna I. Montrin, Tetiana V. Koval and Olha S. Paramonova. Formation and application of communication strategies through social networks: legal and organizational aspects. International Journal of Management. Volume 11. Issue 06. June 2020. pp. 476-488. Article ID: IJM_11_06_041 Available online at

<http://www.iaeme.com/ijm/issues.asp?JType=IJM&VType=11&IType=6> DOI: 10.34218/IJM.11.6.2020.041.

3. Viber. URL: <https://uk.wikipedia.org/wiki/Viber>.

4. Грищук Р. В. Основи кібернетичної безпеки : моногр; за заг. ред. проф. Ю. Г. Даника. Житомир : ЖНАЕУ, 2016. 636 с.

5. Майстри паніки. Як проросійська мережа в Україні організувала бунт в Нових Санжарах. URL: <https://texty.org.ua/articles/100356/specoperaciya-imeni-portnova-ta-shariya-yak-rozhanyaly-paniku-v-novyh-sanzharah-i-hto-za-cym-stoyit/>

6. Месенджери в Україні: Viber знову перший, Telegram зростає. URL: <https://www.epravda.com.ua/news/2019/11/14/653717/>.

7. Названо найпопулярніші месенджери в Україні. URL: <https://glavcom.ua/techno/telecom/nazvano-naupopulyarnishi-mesendzheri-v-ukrajini-750989.html>.

8. Україна серйозно вражена інформаційним маніпуляціям РФ - дослідження Facebook. URL: https://petrimazepa.com/ukraina_serezno_porazhena_informmanipulyaciyami_rf_issledovanie_facebook?utm_source=gravitec&utm_medium=push&utm_campaign=News&fbclid=IwAR1mVNSEKe1K8kTWQsqdQbYUCB67ceOUt3GAjVAtrHcFDD2T3xGcpEMRQZY.

9. Черниш Р. Ф. Фейк, як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни. Часопис київського університету права. № 2. 2019. С. 109-114. URL: http://kul.kiev.ua/doc/chasopys2019/CHAS19_2.pdf.

10. Черниш Р. Ф. Юридична відповідальність за поширення фейкової інформації. Електронне наукове фахове видання «Юридичний науковий електронний журнал». №1. 2020. С. 191-194. URL: http://lsey.org.ua/1_2020/47.pdf.

Чіпуріна Г. М.

Національна академія СБ України

НАПРЯМИ ПРОТИСТОЯННЯ ІДЕОЛОГІЇ «РУСЬКОГО МІРУ» У ГІБРИДНІЙ ВІЙНІ ПРОТИ УКРАЇНИ

Феномен гібридної війни сьогодні активно вивчається науковцями та практиками з метою вироблення чіткого розуміння його сутності, складових та особливостей, а також розробки методів протидії, що особливо актуально сьогодні для України, яка змушена мобілізувати всі ресурси в боротьбі у гібридній війні проти нашої країни.

Термін гібридна війна з'явився вперше в 2006 році, і визначав стратегію, до якої вдалася «Хезболла» у Лівані. Виникнення та генезу феномену «гібридної війни» досліджували відомі зарубіжні вчені такі як Ф. Хоффман, Б. Флемінг, Г. Грант, А. Діп та ін., серед українських

науковців проблема досліджувалася Ю. І. Міхєєвим, Ю. В. Турченком, Г. П. Чернявським та ін. Є. В. Магда визначив гібридну війну «як сукупність заздалегідь підготовлених та оперативно реалізованих дій військового, дипломатичного, економічного, інформаційного характеру, спрямованих на досягнення стратегічних цілей. До базових компонентів гібридної війни можна віднести традиційні та нестандартні загрози, тероризм, підривні дії, новітні і нешаблонні технології» [1, с. 27]. Слід звернути увагу на відсутність єдиного підходу до визначення терміну «гібридна війна» а також на несприйняття багатьма експертами використання терміну «гібридний». На думку О. Морозова термін «гібридна війна» не тільки не відображає справжньої суті війни з використанням різних способів її ведення, а й ускладнює розуміння сполучених форм ведення сучасної війни» [2, с. 30]. Тому вченим пропонується визначення «системна війна».

Незважаючи на різноманіття підходів до визначення сутності, більшість експертів називають одним із елементів гібридної війни – інформаційне протистояння. Особливо чітко це можна спостерігати на прикладі діяльності РФ проти України: інформаційний вплив спрямований в кількох напрямках: на суспільство України, при цьому особливо потужно - на жителів тимчасово окупованих територій, на російське суспільство та на світову громадськість.

РФ використовує проти нашої країни найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної та релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету та територіальної цілісності України. При чому інформаційна війна з Україною почалася задовго до збройного вторгнення у Крим. Однією з численних цілей інформаційної війни було формування громадської думки та світогляду населення, в основу якої лягла ідеологія «руського міру», який на думку його розробників охоплює населення по всій колишній царській та радянській імперіях, які пов'язані з РФ російською мовою, а також спільною релігією, історією та культурою.

В загальних рисах – «руський мір» – це російська неоімперська геополітична та ідеологічна доктрина, розроблена з метою орієнтації російського населення стосовно ідейних основ існування та розвитку російського суспільства, яка полягає в об'єднанні народу, навколо таких елементів як єдина культура, російська мова, православна віра, а також «спільна історична пам'ять», та використовується з метою впливу на масову свідомість російськомовного населення, вигідному

РФ. При цьому Україна бачиться невід’ємною складовою «руського міру», що зіграло вирішальну роль у рішенні уряду РФ про вторгнення в Україну та сприяло високому рівню підтримки серед проросійських громадян, які надавали допомогу в окупації Криму та Донбасу та їх консолідації навколо зазначеної ідеології. Використання ідеї «руського міру» також сприяла вербуванню громадян РФ, які в перші роки війни бажали «захистити російськомовних братів» на Донбасі.

При поширенні ідеології «руського міру» агресор використав неспроможність світоглядно-ціннісних орієнтацій українського суспільства та певний ідеологічний вакуум, який утворився у більшості громадян після розпаду СРСР. Концепція «руського міру» формувалася П.Щедровицьким, Г.Павловським, В. Тишковим, О.Дугінім. Президент РФ В.Путін у своїх виступах теж неодноразово використовував термін «руський мір», визнавши його елементом російської зовнішньої політики. В останні своїй статті «Про історичну єдність росіян та українців» В.Путін чітко викладає своє бачення, яке повністю збігається із зазначеною ідеологією і підтверджує, що сьогодні ідеологія «руського міру» введена на рівень державної політики РФ, що потребує врахування на загальнодержавному рівні.

Використовуючи ідеологію «Руського міра» представники спецслужб РФ намагались також імплементувати сценарії створення т.зв. «Запорізької Народної Республіки», «Херсонської Народної Республіки», «Харківської Народної Республіки» та ін. Таким чином зазначена ідеологія активно використовується російськими спецслужбами та російськими ЗМІ для виправдання російської агресії щодо України і спрямована на дестабілізацію соціально-політичної обстановки в Україні, розпалювання сепаратистських настроїв, провокування діяльності з метою посягання на територіальну цілісність, що вимагає розробки та реалізації комплексу заходів з протидії зазначеній ідеології.

Протидія поширенню зазначеної ідеології повинна здійснюватися на кількох рівнях: на міжнародному, загальнодержавному та спеціальному. На спеціальному рівні – протидія СБ України поширенню ідеології «руського міру» в ЗМІ та соціальних мережах, виявлення «бот-ферм», створених з метою поширення фейків та виправдання ідеології агресора. На загальнодержавному рівні повинні вживатися такі заходи як вдосконалення нормативно-правової бази в галузі інформаційної політики, розробка системи захисту від інформаційного домінування іноземних країн, особливо країни-агресора, розвиток національної інформаційної інфраструктури, що надасть можливості

України ефективно протидіяти інформаційній агресії та практично діяти в інформаційній сфері, підвищення рівня медіа-культури суспільства.

Відомий дослідник М. Головатий вважає, що впровадження державотворчої ідеології є одним із засобів подальшого гарантування державотворчої безпеки і покликане «сприяти цілісності держави та її зміцненню, подолання загроз сепаратизму, зміцнення консолідації суспільства та міжетнічного миру» [3, с.14]. Вона має бути заснована на цінностях, що поділяються більшістю українського суспільства. В Карлова також визнає необхідність створення і впровадження «загальнонаціональної ідеології в Україні, що має включати культурно-історичну, політичну, економічну і соціогуманітарну складові» [4, с. 24]. Водночас ст. 15 Конституції України стверджує, що «жодна ідеологія не може визнаватися державою як обов'язкова». На нашу думку, державою все ж повинні вживатися певні заходи заповнення ідеологічного вакууму, в якому опинилися українці після розпаду СРСР. Тому важливим є формування на державному рівні ціннісних орієнтирів розвитку сучасного українського суспільства, які зможуть об'єднати та мотивувати український народ успішно долати виклики, спровоковані в тому числі гібридною війною РФ та спробами поширення вигідної агресору ідеології.

На міжнародному рівні Україна повинна вживати усіх заходів з використанням інструментів міжнародного права, зарубіжних змі та інших засобів з метою протидії поширенню та розвінчання ідеології «руського міру» як серед світової громадськості, так і серед населення РФ.

Література

1. Магда Є. В. Гібридна війна: вижити і перемогти. Х.: «Віват», 2015. – 304 с.
2. Морозов О. М. Системна війна – український вимір. К. 2017. - 113 с.
3. Головатий М.Ф. Соціологія політики: навч. посіб. / М.Ф. Головатий – К.: МАУП, 2003. – 504 с.
4. Карлова В. Проблема формування загальнонаціональної ідеології в Україні / В. Карлова// Вісник національної академії державного управління пр Президентів України. – 2010 – № 42. – С. 17-24 – Режим доступу: http://nbuv.gov.ua/UJRN/Vnadu_2010_4_4.

Щербина А. В.
кандидат юридичних наук,
Національна академія СБ України

РЕЛІГІЙНИЙ ЕКСТРЕМІЗМ З БОКУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ В УМОВАХ «ГІБРИДНОЇ» ВІЙНИ ПРОТИ УКРАЇНИ

Для України проблема протидія екстремізму набула особливої актуальності з початком агресії з боку Російської Федерації, яка порушила територіальну цілісність нашої держави та загрожує її незалежності. Силами і засобами розвідувальних органів і спеціальних служб країна-агресор спровокувала численні екстремістські прояви на території Автономної Республіки Крим, Донецької і Луганської та інших областей України, а також збройні виступи сепаратистів. Незаконні збройні формування, що діють на тимчасово непідконтрольній території України, широко використовують релігійно-екстремістську тактику, яка мало чим відрізняється від організацій, визнаних терористичними на міжнародному рівні (як «Аль-Каїда» або «Ісламська держава») [1].

Етнічне, культурне, релігійне, мовне, ідеологічне та національне розмаїття людства є унікальним фактором його розвитку, що дає змогу індивідам об'єднуватися за певними ознаками в стійкі групи, виробляти спільні цінності та соціальні норми, розвиваючись і захищаючи себе та власні здобутки в різних сферах суспільного життя. Вхідження до певної соціальної групи є об'єктивним процесом самоідентифікації особи, наслідком еволюції соціуму. Групова приналежність формує в кожного індивіда почуття «ми», що надає впевненості у власній безпеці та здатності до колективного захисту прав і свобод за допомогою ресурсів групи. Водночас таке розмаїття є джерелом виникнення соціальних конфліктів, особливо міжгрупових, що, як свідчить історія, неодноразово призводили та призводять до численних людських жертв, знищення певних прошарків населення або навіть націй. Незважаючи на те, що ми живемо у ХХІ ст. – у час, коли загально визнаною є необхідність побудови держави на демократичних засадах урядування, усебічного й повного захисту та реалізації прав і свобод людини та громадянина, дотримання принципу верховенства права, у світі виникає дедалі більше міжгрупових конфліктів. Стрімкий розвиток інформаційних технологій, глобалізація значно ускладнили соціальну структуру суспільства, спричинивши зростання його диференціації. Різні соціальні групи дедалі частіше намагаються не-

правовим шляхом здобути домінантне становище, зберегти або примножити свої активи, розширити сферу впливу, побудувати власний «ідеальний» світ. З огляду на це, вони вдаються до ініціювання або загострення суперечностей у межах концептів «свій – чужий», «ми – вони», «товариш – ворог». За своєю природою екстремізм є складним соціально-політичним і правовим феноменом. Саме тому він став об'єктом вивчення фахівців у галузях філософії, психології, соціології, політології, юриспруденції. В Україні це явище розкрито в працях В. Боярова, Є. Васильчука, Д. Веденєєва, Л. Веденєєвої, М. Паламарчука, Б. Петренка, Е. Расюка, І. Рижова, М. Розумного, А. Франзуза [2].

Залежно від цільової спрямованості і суб'єктної діяльності екстремізм представляють у трьох традиційних формах: політичний, національний і релігійний. Політичний екстремізм трактується як насильницькі дії, спрямовані на зміну політичного устрою або державної політики. Національний екстремізм розглядається як намагання політичних суб'єктів, громадських організацій і окремих громадян утверджувати всілякими засобами домінування інтересів нації або етносу, до яких вони належать, на шкоду міжнаціональній єдності, аж до порушення прав та свобод людини і громадянина за ознакою приналежності до національної групи або етносу. Релігійний екстремізм інтерпретується як нетерпимість до інших конфесій або утвердження переваг представників однієї з конфесій. Тому серед конструктів радикалістських політико-ідеологічних доктрин особливе місце посідає релігійність, яка виконує функцію національної ідентифікації особи, має суттєвий вплив на свідомість населення, значні мобілізаційний і сугестивний потенціали. Визначальною характеристикою релігійного типу світогляду є його неплюралістичність, оскільки кожна релігійна доктрина претендує на виключність та абсолютну істинність своїх світоглядних позицій. Аналізуючи особливості маніфестації релігії у суспільному житті, властивий будь-яким релігійним доктринам ідеалізм є своєрідним бунтом проти логіки фактів, науки, розуму, проти перспектив пізнання таємниць всесвіту, свідомого управління суспільним розвитком на науковій основі. Відповідно, екстремістська ідеологія, підсилена релігійними домінантами, містить значний деструктивний потенціал, що визначає виняткову агресивність маніфестації його суб'єктів у суспільстві [3].

Задовго до анексії Криму та неоголошеної війни на Донбасі було відкрито релігійний фронт, що стало основою проявам екстремістського характеру. Як показали події в Україні, православний фундаменталізм не менш агресивний, ніж ісламський, а «російська весна» не

менш кривава, ніж арабська. Оскільки цей різновид православ'я має державну підтримку і претендує на політичну роль, його можна назвати «політичним православ'ям». Більше того, віднедавна «політичне православ'я» проявило себе в формі «православного екстремізму» на окупованих проросійськими сепаратистами українських територіях. Варто зазначити, що анексія Криму була виправдана сакральною значимістю стародавнього Херсонесу, а війна проти України - захистом православ'я.

Зокрема, зусиллями ідеологів «російської весни», конфлікт між Росією та Україною, між московським православ'ям та українськими «уніатами, розкольниками і сектантами» виводиться на глобальний рівень і подається як конфлікт «руського міра» і «загниваючого Заходу», «традиційних цінностей» і «гейропи», як рятівної духовності. Більш того, залишаючись головною об'єднуючою силою, Російська православна церква намагається створити альянс із тих протестантів, юдеїв, мусульман, які згодні з православним баченням історії Росії та беззаперечно визнають своє принизливо підлегле становище. У певному сенсі вже не сама Росія як держава, а російське православ'я як наддержавний рух стає фактором геополітики. Саме захистом «справжнього», традиційного, канонічного православ'я виправдовуються дії «православних армій» Донбасу, що становить загрозу для національної безпеки і створює небезпечний прецедент для інших країн регіону. «Гібридна війна», яку розв'язала Росія, є не так антиукраїнською, як антизахідною, і настільки явно релігійно мотивованою, що цілком може бути названа «*holy war*», де «православна армія» бореться проти «уніатів, розкольників і сектантів». У свідомості ідеологів «російської весни» російська інтервенція подається як «хрестовий похід» проти Заходу, відвоювання, збирання, возз'єднання земель «руського міра». Всі, хто пов'язаний із Заходом за своїм походженням («чужі») чи усвідомленим вибором («зрадники»), автоматично заносяться до списку ворогів «руського міра»: греко-католики - як зрадники православної віри, уніати, «бандерівці»; православні Київського Патріархату - як розкольники, відступники, «націоналісти»; протестанти - як сектанти, західники, американські шпигуни; кримські татари - як проукраїнські і неправославні. Бачимо явну дискримінацію за релігійною ознакою всіх конфесій, крім Московського Патріархату.

Поширення православної ідеології «руського міра» і релігійні переслідування інших конфесій вже призвели до істотної зміни релігійної карти регіону. Більшість релігійних організацій припинили свою діяльність, а їхні парафії були змушені переїхати в інші регіони.

При цьому переважна більшість біженців не має необхідних умов для проживання своїх родин, а також перспектив на отримання роботи в умовах економічної кризи в країні. Цілі громади опинилися в розсіянні, а служителі, які залишилися на окупованих територіях, знаходяться у постійній небезпеці. Можна говорити про розгромлені релігійні об'єднання в трьох регіонах України - Криму, Луганській і Донецькій областях. Віруючі цих конфесій можуть вважатися жертвами релігійних чисток [4].

Таким чином, релігійний екстремізм православного «руського міра» несе з собою загрозу релігійній своєрідності, державній безпеці України, захист її самобутності вимагає міжнародної допомоги - професійного моніторингу, експертного аналізу, адвокації релігійної свободи, розширення міжнародних зв'язків, інтеграції в глобальний простір. У свою чергу, у світової спільноти є тільки один спосіб протистояти поглинанню України Росією - зблизитися з Україною, зв'язати себе з нею міцними релігійними, культурними, політичними, економічними зв'язками; використовувати всі дипломатичні засоби для визнання сепаратистських «народних республік» терористичними організаціями, їхньої «політики» щодо релігійних організацій - політикою дискримінаційною, а їхні жертви - жертвами релігійно мотивованого екстремізму.

Література

1. Актуальні питання протидії тероризму у світі та в Україні [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/content/articles/files/aktualniPitannya_press-1c1ef.pdf.
2. Екстремізм як одна з головних загроз безпечному існуванню людини, суспільства та держави у ХХІ ст. / Є. Д. Скулиш, Ю. Б. Ірха // Науковий вісник Національної академії внутрішніх справ. - 2016. - № 1. - С. 19-35. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/Nvknuvs_2016_1_4.
3. Бояров В. І. Криміналістична класифікація кримінально-караних проявів екстремізму / В. І. Бояров // Вісник Академії адвокатури України. - 2015. - Т. 12. № 2. - С. 210-216. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/vaau_2015_12_2_28.
4. Черенков М. Виклик релігійній свободі та духовно-конфесійному плюралізму України: ідеологія та терор «руського міра» / М. Черенков // Схід. - 2015. - № 2. - С. 30-34. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/Skhid_2015_2_6.

ПРАВОВІ АСПЕКТИ ПРОТИДІЇ ПРОПАГАНДІ ВІЙНИ

Пропаганда (лат. *propaganda* дослівно – «яка підлягає поширенню (віра)», від лат. *propago* – «поширюю») – форма комунікації, спрямована на поширення в суспільстві – світогляду, теорії, твердження, фактів, аргументів, чуток та інших відомостей для впливу на суспільну думку на користь певної спільної справи чи громадської позиції [1].

Одним з типів пропаганди є негативна (деструктивна) пропаганда. Мета негативної пропаганди – розпалювання соціальної ворожнечі, нагнітання соціальних конфліктів, загострення суперечностей у суспільстві, пробудження низинних інстинктів у людей тощо [1]. Негативна пропаганда включає в свою чергу пропаганду війни.

Остання створює загрозу людині, суспільству, державі, безпеці людства та довкіллю, порушуючи підвалини мирного людського співіснування.

Відповідно до статті 34 Конституції України кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [2, ст. 34].

Таким чином, негативна пропаганда та насамперед пропаганда війни є протиправним діянням, що знайшло відображення як у Конституції України так і ст. 46 Закону України «Про інформацію», п. 2 ст. 6 Закону України «Про телебачення та радіомовлення» та у ряді інших нормативно-правових актах України [3; 4].

Відповідно до вимог Статуту ООН, національне кримінальне право фактично усіх держав світу забороняє агресивну воєнну пропаганду. Зазначене положення міжнародного права знайшло відображення у ст. 18 Конституції України, відповідно до якої зовнішньополітична діяльність України спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигід-

ного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права [2, ст. 18]. У 2000 році Україна підписала Римський статут Міжнародного кримінального суду (надалі – МКС). Зазначений суд уповноважений розглядати такі злочини як геноцид, злочини проти людяності, військові злочини та злочини агресії [5]. У розділі XX «Злочини проти миру, безпеки людства та міжнародного правопорядку» Кримінального кодексу України, законодавцем закріплена ст. 436 «Пропаганда війни», що гарантує виконання зазначеної вимоги Статуту ООН всередині нашої держави [6].

В диспозиції даної статті зазначено наступне: «Публічні заклики до агресивної війни або до розв’язування воєнного конфлікту, а також виготовлення матеріалів із закликами до вчинення таких дій з метою їх розповсюдження або розповсюдження таких матеріалів». Визначення агресії дається в резолюції XXIX сесії Генеральної Асамблеї ООН від 14 грудня 1974 р. Під агресією слід розуміти застосування збройної сили державою проти суверенітету, територіальної недоторканності чи політичної незалежності іншої держави або будь-яким іншим чином, що несумісний зі Статутом ООН. Свідченням агресії, як правило, є таке застосування збройних сил державою першою [7].

Актом агресії може визнаватися будь-яке із таких діянь: 1) вторгнення або напад збройних сил держави на територію іншої держави або будь-яка воєнна окупація, яка є результатом такого вторгнення чи нападу, або будь-яка анексія із застосуванням сили території іншої держави або частини її; 2) бомбардування збройними силами держави території іншої держави або застосування будь-якої зброї державою проти території іншої держави; 3) блокада портів або берегів держави збройними силами іншої держави; 4) напад збройними силами держави на сухопутні, морські або повітряні сили чи морські та повітряні флоти іншої держави; 5) застосування збройних сил однієї держави, що перебувають на території іншої держави за угодою з приймаючою державою, на порушення умов, передбачених угодою, або будь-яке продовження їх перебування на такій території після закінчення дії угоди; 6) дії держави, яка дозволяє, щоб її територія, яку вона надала в розпорядження іншої держави, використовувалась цією іншою державою для вчинення акту агресії проти третьої держави; 7) засилання державою або від імені держави озброєних банд, груп і регулярних сил або найманців, які здійснюють акти застосування збройної сили

проти іншої держави, які мають настільки серйозний характер, що це рівнозначно переліченим вище актам, або її значна участь у них [7].

Останнім часом фіксується збільшення кількості правопорушень, пов'язаних з негативною пропагандою. Так, у 2020 році, за матеріалами Служби безпеки України, притягнуто до кримінальної відповідальності 40 осіб, які поширювали деструктивну антиукраїнську пропаганду та здійснювали підривну діяльність в інформаційній сфері [8].

У зазначеному році СБ України:

- заблоковано понад 2,5 тис. спільнот у соцмережах з мільйонною аудиторією та понад 20 бот-мереж потужністю понад 60 тис. акаунтів;

- нейтралізовано понад 600 кіберінцидентів та кібератак на інформаційні ресурси органів державної влади;

- припинено діяльність 20 хакерських угруповань [8].

Пропаганда війни була криміналізована лише у деяких європейських країнах, наприклад, в статті 92 Кримінального кодексу Естонії, в статті 77 Кримінального кодексу Латвії та інших. Така ситуація обумовлена тим, що більшість європейських держав визнають юрисдикцію МКС.

В ст. 436 Кримінального кодексу України на відміну від відповідних нормативно-правових актів таких держав як Таджикистан, Казахстан, Молдова не передбачена така кваліфікуюча ознака пропаганди війни як вчинення таких дій службовими особами.

Враховуючи те, що відповідно до чинного законодавства саме ця категорія суб'єктів має виконувати завдання та функції держави, та, зважаючи на своє становище, має можливість ефективно контролювати або керувати політичними або військовими діями держави, на нашу думку, було б доцільним закріпити на законодавчому рівні спеціальний суб'єкт цього злочину та доповнити ст. 436 КК України частиною другою диспозицією статті наступного змісту: «Ті самі діяння, якщо вони вчинені службовою особою». Розробка санкції до ч. 2 ст. 436 може бути досліджено у подальших наукових розробках.

Література

1. Вільна енциклопедія вікіпедія. URL: <https://uk.wikipedia.org/wiki/пропаганда>.
2. Верховна рада України Конституція України від 28 червня 1996 року. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/paran4269#n4269>.
3. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

4. Закон України «Про телебачення і радіомовлення» від 21 грудня 1993 року № 3759-XII. URL: <https://zakon.rada.gov.ua/laws/show/3759-12#Text>.
5. Римський статут Міжнародного кримінального суду: Статут від 17.07.1998 р. № 995_588. URL: https://zakon.rada.gov.ua/laws/show/995_588 (дата звернення 12.11.2019).
6. Кримінальний кодекс України. Офіційний вісник України. 2001. № 21. Стор. 1. Ст. 920.
7. Определение агрессии : Резолюция от 14.12.1974 г. №995_001-74. URL: https://zakon.rada.gov.ua/laws/show/995_001-74#Text.
8. Армія inform. URL: <https://armyinform.com.ua/2021/03/40-osib-prytyagnuto-do-kryminalnoyi-vidpovidalnosti-za-poshyrennya-antyukrayinskoyi-propagandy-u-2020-roczni-%E2%88%92-sbu/>.

РЕКОМЕНДАЦІЇ КРУГЛОГО СТОЛУ

«Гібридна війна: сутність, виклики та загрози»

У науковому форумі взяли участь представники українського політикуму, Апарату Верховної Ради України, Інституту законодавства Верховної Ради України, Національної академії наук України та її наукових установ, Національного інституту стратегічних досліджень, Київського національного університету ім. Тараса Шевченка, Національного університету оборони України ім. Івана Черняховського, громадської професійної організації «Всеукраїнська асоціація політичних наук», співробітники підрозділів Центрального управління СБ України, від мас-медіа – шеф-редактор проєктів телеканалу ICTV «Громадская оборона» та «Антизомби» (всього понад 50 учасників).

Метою заходу стало вироблення узгоджених підходів до розуміння сутності та змісту феномену гібридної війни в контексті сучасного цивілізаційного протистояння між Російською Федерацією як країною-агресором й демократичною світовою спільнотою.

У ході фахових дискусій предметом найбільш зацікавленого та ґрунтовного обговорення стали наступні питання:

- політико-ідеологічного підґрунтя гібридної війни Російської Федерації проти міжнародного правопорядку;
- інформаційна складова гібридної війни Російської Федерації: викривлення реальності та деструктивної пропаганди в арсеналі політики Москви;
- економічні компоненти гібридної війни й експансійні механізми у досягненні військово-політичних цілей Російської Федерації;
- силовий розвиток гібридної війни Російської Федерації – «гаряча» фаза сценаріїв «керованого хаосу».

У виступах та при їх обговоренні було охарактеризовано основні операційні лінії гібридної війни Російської Федерації проти міжнародного правопорядку, вироблено спільне бачення щодо масштабів загроз, спричинених діями країни-агресора, досягнуто взаєморозуміння з основних принципів питань між науковцями та фахівцями-практиками, експертним середовищем й законотворцями.

Підводячи підсумки роботи круглого столу, учасники та гості підкреслили конструктивність проведеного обговорення проблемних питань, що стосуються стратегії й тактики протидії гібридним викликам та загрозам, а також застосування проактивного підходу у проти-

борстві з агресором. Загальним консенсусом ухвалено рекомендації щодо вибудовування сутнісно-змістової характеристики гібридної війни та вироблення адекватних кроків для локалізації її проявів на основі наступних базових положень, згрупованих за чотирма напрямками:

1) Політико-ідеологічне підґрунтя гібридної війни Російської Федерації проти міжнародного правопорядку

– Сучасне суспільство є вкрай залежним від безпеки інформаційної інфраструктури. Поширення інформаційних технологій практично на усі сфери функціонування соціуму створило передумови для позиціонування інформаційної зброї в парадигмі гібридної війни як зброї першого удару. В якості цілей інформаційних атак розглядаються не лише військові формування, населення та органи влади держави, а й господарські об'єкти, що складають національну критичну інфраструктуру.

– Російська гібридна агресія проти України реалізується одразу на кількох напрямках: воєнному, політичному, економічному, соціальному, гуманітарному та інформаційному. Але саме інформаційна агресія наразі продукує найбільше загроз, оскільки ворожа пропаганда, що базується на брехні, маніпуляціях та підміні понять, запереченні самого факту війни в Україні та участі у ній Російської Федерації; спроби останньої перекласти відповідальність за власні протиправні дії на нашу державу; цілеспрямоване свідоме спотворення української історії; кібератаки та дестабілізація критичної інфраструктури – все це, за відсутності належної протидії, може спровокувати поступову деградацію українського суспільства та руйнування самоідентичності української нації.

– Пропагандистські впливи агресора реалізуються за повномасштабної підтримки на рівні державної політики, передусім, через просування ідеологем зміцнення «братніх зв'язків між російським, білоруським та українським народами», укріплення позиції російської мови як «мови міжнародного спілкування», підтримки громадян Російської Федерації, які проживають в інших країнах, в їх прагненні до збереження «загальноросійської культурної ідентичності».

– Прогнозовані подальші деструктивні дії Російської Федерації в інформаційному просторі матимуть на меті, передусім, формування осередків лобіювання її інтересів у різних регіонах і на загальносвітовому рівні, пропагування та активне нав'язування власного спотвореного егоцентричного бачення світоустрою. Основним засобом при цьому виступатиме інформаційна агресія, яка втілюватиметься у

масштабному маніпулюванні людською свідомістю та громадською думкою в інтересах отримання бажаного для Російської Федерації ефекту.

2) Інформаційна складова гібридної війни Російської Федерації: викривлення реальності та деструктивна пропаганда в арсеналі політики Москви

Інформаційні війни руйнують суспільні організми (державні, політичні, соціальні інститути і організації), деформують цивілізаційно-культурний код нації і суспільну мораль, нівелюють почуття патріотизму, розхитують людську психіку, паралізують здатність народу до спротиву агресії ворога. Інструментами ж, за допомогою яких Російська Федерація здійснює свій деструктивний вплив на наш інформаційний простір, є інформаційні та психологічні операції, у ході яких здійснюється приховане впровадження підготовлених країною-агресором та вигідних їй наративів і меседжів з метою загальної дестабілізації ситуації, формування сприятливої для Російської Федерації громадської думки. З огляду на зазначене доцільно:

- в Конституції України, як в суспільному договорі, чітко врегулювати взаємовідносини народу, як замовника послуг, і держави, яка має надавати ці послуги, особливо в інформаційно-комунікаційній сфері, що в умовах гібридної війни стає головним театром воєнних дій.

- Забезпечувати ефективний захист вітчизняного інформаційного простору від поширення впливів на свідомість та самоідентичність українців. При цьому недостатньо діяти «у відповідь», руйнуючи та спростовуючи брехливі повідомлення. Необхідно вдаватися до дій на випередження, створюючи власний якісний контент та досягаючи його найширшого розповсюдження та сприйняття.

- Забезпечити ефективну координацію дії відповідних органів державної влади та місцевого самоврядування, громадянського суспільства й науково-експертного середовища в інтересах забезпечення інформаційної безпеки.

- Невідкладно актуалізувати та зорієнтувати на потреби протидії гібридній війні Російської Федерації перелік пріоритетних дослідницьких тем та проектів для наукових установ гуманітарного профілю, в тому числі в системі НАН України, а також для провідних вітчизняних вишів.

3) Визначення економічних компонентів гібридної війни й експансійних механізмів у досягненні військово-політичних цілей Російської Федерації

– Характерними особливостями застосування економічних заходів для досягнення цілей агресії є нанесення економічними інструментами державі-об'єкту агресії збитків, які можуть бути співставними із втратами у період активних бойових дій (депопуляція, падіння ВВП, катастрофічне зниження промислового та воєнно-економічного потенціалу, критичне зростання безробіття тощо) або нагромадження економічних залежностей, які згодом можуть використовуватись для тиску.

– Використання в ході агресії «вузьких» місць економіки України, насамперед, її високої залежності у низці сегментів енергетичного ринку, суттєво посилило негативні наслідки для економічного й соціального розвитку держави, а також зменшило спроможності щодо фінансування важливих для національної безпеки проєктів.

Починаючи з 2014 року, в Україні спостерігається суттєвий приріст витрат на оборонну функцію держави взамін видатків на розвиток економіки, соціальної інфраструктури, зростання оплати праці та інші заходи економічного розвитку країни. Спонукання країни до значного збільшення своїх оборонних витрат слід розглядати як один із інструментів гібридної війни. Тому пріоритетні напрями формування нашої економічної стратегії варто зосередити на:

– заходах щодо кардинального прискорення економічного зростання та зміцнення конкурентоспроможності національної економіки на інноваційній основі, що дозволить створити належну матеріальну базу для адекватної відповіді на гібридну агресію;

– посиленні інституціональної спроможності протидії деструктивному впливу в економічній, фінансовій, цифровій, технологічній, промисловій та інфраструктурній сферах на основі регламентації іноземної присутності у відповідних галузях економіки та застосування симетричних заходів у разі я деструктивного зовнішнього втручання;

– локалізації в Україні виробництва та/або диверсифікації джерел постачання товарів критичного імпорту;

– системному зміцненні наукової, дослідницької, технологічної та інноваційної бази національної економіки;

– захисті активів, які мають вирішальне значення для національної безпеки, від іноземного деструктивного втручання у процесі володіння, розпорядження та користування;

– забезпеченні національного контролю над морською, енергетичною та цифровою інфраструктурою за активної підтримки міжнародної спільноти;

– контролі над інвестиціями у таких чутливих для сучасної економіки сферах як: інфраструктура 5G, хмарні технології, бази даних, операційні системи, доступ до космосу тощо.

У ситуації, що склалася, Україна має здійснювати наступні заходи, спрямовані на забезпечення валютно-курсової та інфляційної стабільності як необхідної передумови успішного протистояння зовнішнім гібридним загрозам в економічній сфері:

– послаблення імпортозалежності національної економіки задля поліпшення стану торговельного балансу та посилення внутрішніх чинників реалізації національного економічного потенціалу;

– запобігання недобросовісній конкуренції імпортерів (у т. ч. протидія контрабанді) на внутрішньому ринку, сприяння доступу до внутрішніх ринків суб'єктів малого бізнесу, зниження енергоємності економіки (зважаючи на значну частку імпорту в енергетичному балансі), сприяння залученню вітчизняних компаній до участі у публічних закупівлях та інвестиційних проектах;

– поліпшення структури експорту, оскільки переважання товарів з низькою доданою вартістю в експорті та товарів з високим рівнем переробки в імпорті закладає підґрунтя перманентного дефіциту зовнішньої торгівлі;

– активізація підтримки експортної діяльності вітчизняних товаровиробників, сприяння виходу на зовнішні ринки нових учасників ЗЕД, освоєнню нових ринків та розширенню кола зовнішньоторговельних партнерів України;

– забезпечення відповідності обмінного курсу гривні параметрам, що закладені при формуванні Державного бюджету, шляхом недопущення неочікуваної ревальвації, що стимулює зростання імпорту, погіршує показники експорту, податкові та митні надходження;

– корекція режиму інфляційного таргетування через збільшення ваги немонетарних інструментів антиінфляційної політики та послаблення інфляційного потенціалу монетарних стимуляторів внаслідок удосконалення трансмісійних механізмів;

– посилення ролі облікової ставки як орієнтира для здешевлення кредитних ресурсів для реального сектору економіки, при збереженні її додатного рівня відносно прогнозованої базової інфляції, що має стимулювати депозитну активність вкладників та сприяти зниженню девальваційних й інфляційних очікувань;

– диференціація норми резервування залучених коштів у національній валюті залежно від строковості банківських пасивів: нульова або мінімальна ставка резервування має застосовуватись тільки для довгострокових пасивів;

– запобігання зниженню конкуренції на ринку банківських послуг внаслідок їх надмірної концентрації, що потребуватиме впровадження НБУ «антимонопольних» заходів, зокрема встановлення граничних значень процентів по кредитах і депозитах відносно облікової ставки;

– сприяння зниженню попиту на готівку через поширення безготівкових форм розрахунків, підвищення вартості отримання готівки, подальшого зниження граничної суми розрахунків готівкою;

– поетапне переведення всіх отримувачів пенсійних та інших соціальних виплат на безготівкову форму шляхом оформлення платіжних карток у державних банках, що сприятиме зростанню банківських пасивів, активізації безготівкових розрахунків та зниженню частки тіньової економіки в країні;

– забезпечення збалансованої валютної структури банківських кредитів і депозитів за рахунок зниження доларизації кредитного та депозитного портфелів банківської системи до рівня, нижчого за 35 % у середньостроковій перспективі.

4) Силовий розвиток гібридної війни Російської Федерації – «гаряча» фаза сценаріїв «керованого хаосу»

– У гібридній війні проти нашої держави, яка триває вже восьмий рік поспіль, збройна агресія – лише один з інструментів для спонукання України до повернення у сферу геополітичного впливу Російської Федерації. Окрім цього, здійснюються перманентні спроби добитися різними способами зміни влади в Україні на «проросійську», стримування її руху у напрямку євроатлантичної інтеграції, примусити відмовитись від намірів деокупації АР Крим тощо. Все це реалізується, передусім, в інформаційному просторі. Тому сьогодні інформаційна перевага значною мірою зумовлює результат, в тому числі, й збройного протистояння. Відповідно максимум уваги слід приділяти інформаційному протистоянню зі супротивником.

– Необхідно прискореними темпами розвивати сучасну інформаційну інфраструктуру, нарощуючи при цьому можливості держави у протидії використанню інформаційних технологій на шкоду національним інтересам.

– Слід забезпечити функціональну спроможність систем кібербезпеки та кібероборони не нижче гранично необхідного рівня для ефективної відсічі гібридним атакам країни-агресора.

– Необхідно активно продукувати та просувати якісні, змістовні наративи, націлені на руйнування російських міфологем та на гуманітарну деокупацію АР Крим, тимчасово окупованих територій Донецької й Луганської областей.

ЗМІСТ

Вступне слово	3
Єхануров Ю. І. Гібридна війна – треба атакувати	5
Томенко М. В. Історико-політологічні міфи та загрози «російського світу»	6
Зеленько Г. І. Економічні загрози та їх потенціал в російсько-українському протистоянні	8
Бебик В. М. Теоретичні та праксеологічні засади гібридних війн ...	10
Тітко Е. В. Роль та значення цивільно-військового співробітництва (СІМІС) у вибраних сучасних оборонних стратегіях країн світу	14
Горовий В. М. Науково-інформаційний аспект протистояння негативним інформаційним впливам в умовах російсько-української інформаційної війни.....	17
Новакова О. В. Пропагандистські наративи як зброя Російської Федерації в гібридній війні проти України.....	20
Шемаєва Л. Г. Вимушене збільшення оборонних витрат європейськими країнами як інструмент гібридної війни з боку РФ	24
Козьма В. В. Інформаційна зброя Російської Федерації як чинник сучасної геополітики	26
Мельніченко О. А. Основні напрями деструктивної діяльності російських спецслужб в інформаційній війні проти України.....	30
Гладких Д. М. Забезпечення валютно-курсової та інфляційної стабільності України в контексті протидії гібридним загрозам	33
Закіров М. Б. Використання глобальних інформаційних ресурсів у моніторингових матеріалах СІАЗ	36

Горовенко В. К. Деякі форми і способи забезпечення оборони держави в умовах гібридної війни.....	40
Горова С. В. Етнонаціональна проблематика інформаційної війни.....	44
Куровська І. А. Реалізація принципу верховенства права в умовах гібридної війни	48
Ковальчук І. М. Щодо питань протидії Службою безпеки України економічному тероризму як загрозі стабільному функціонуванню критичної інфраструктури держави в умовах гібридної війни	51
Шемаєв В. М., Толок П. О. Створення агенства з розвитку оборонних технологій – основа асиметричних можливостей України у гібридній війні	55
Желай О. П. Організація інформаційного обслуговування управлінських структур актуальною суспільно значимою інформацією	58
Мірошніченко О. П. Пріоритетні напрями протидії екологічним загрозам на тимчасово-окупованих територія України	61
Медведєва А. С. Особливості моніторингу регіональних електронних ресурсів в обслуговуванні управлінських структур	66
Базиліук Я. Б. Особливості сучасних економічних стратегій в умовах гібридної війни: висновки для України.....	68
Вдовенко С. Г., Ганенко С. О., Гульков М. О. Інформаційне підґрунтя гібридної війни РФ проти міжнародного порядку.....	73
Пермяков О. Ю., Королюк Н. О., Фараон С. І. Інформаційні та економічні аспекти й експансійних механізмів у досягненні військово-політичних цілей РФ у гібридній війні.....	75

Князєв С. О. Сучасні тенденції ведення інформаційних війн	78
Авдошин І. В., Коваленко С. М. Внутрішньо переміщені особи – дестабілізаційний чинник українсько-російської «гібридної» війни	81
Благодарний А. М. Особливості протидії інформаційній агресії як складовій гібридної війни.....	83
Вольвак О. М., Мокієнко О. С. Загальні засади формування зон керованого хаосу у соціальних системах за допомогою інструментів індустрії 4.0 та напрямки протидії таким діям	87
Герман Л. В. Тероризм як елемент гібридної війни	90
Звонарьов О. Ю. Концепція «гібридної війни» та роль спеціальних служб російської федерації у її реалізації щодо України	93
Кузьменко В. В., Сидоренко С. М. Антиукраїнські міфи в інформаційній війні Російської Федерації проти України	95
Куцій М. С. Феномен war weary як стан елементів гібридної війни	97
Липний С. І., Шепета О. В. Загрози національній безпеці в умовах гібридної війни РФ проти України: прикладні та наукові аспекти.....	99
Лісовська О. Л. Європейський вектор економічної експансії Російської Федерації в гібридній війні проти України.....	102
Мамченко С. М. Стійкість державної системи як чинник протидії гібридній війні	104
Окіпнюк В. Т. Спроби викривлення історико-правової реальності як елемент гібридної війни: витоки та шляхи протидії	107
Пальчик М. Л. Деструктивна пропаганда РФ щодо Польщі з використанням релігійного чинника	109

Пелюх О. С. Актуальні питання формування стратегії контррозвідувальної діяльності в умовах «гібридної війни» Російської Федерації	111
Печериця С. В. Терористичні загрози Російської Федерації в контексті гібридних воєн сучасності. Використання міжнародного досвіду	115
Присяжнюк М. М., Карпович О. М. Інформаційна зброя як новий засіб міждержавного протиборства	119
Радовецька Л. В., Гасанов М. А. Нове сприйняття безпеки в контексті глобалізації та гібридної війни з Російською Федерацією: гібридні загрози.....	121
Юдін О. К., Четверяков І. О., Петренко А. Б. Технологія безпеки інформаційних ресурсів IoT	124
Бараннік В. В., Сідченко С. О., Супрун О. М., Бараннік Н. В. Проблемні аспекти забезпечення конфіденційності відеоінформаційних ресурсів в умовах інформаційних та кібернетичних війн	127
Бараннік В. В., Юдін О. К., Красноручський А. О., Шульгін С. С. Технологія кодування для підвищення інформаційної безпеки спеціальних відеоресурсів	130
Жевелєва І. С. Використання методів пропаганди у гібридній війні Російської Федерації проти України.....	132
Лисенко О. В. Особливості гібридної війни: український контекст	138
Титаренко Я. А. Правові основи розвідувальної діяльності спеціальних служб іноземних держав щодо України	140
Гребенюк В. М. Силевий сценарій гібридної війни в країнах Балтії: пройдений етап чи «далі буде»?	144
Морозов О. М. Демографічна складова системної (гібридної) війни	149

Паливода О. О. Використання маніпулятивних можливостей інтернету та нових медіа в проведенні сучасних гібридних воєн	153
Ткачук Т. Ю. Окремі аспекти імплементації міжнародного законодавства про кібербезпеку у національний правовий простір.....	157
Ткаченко О. П., Сидоренко С. М. Правові механізми співробітництва Служби безпеки України із спеціальними та правоохоронними органами країн Євросоюзу у сфері протидії міжнародній кіберзлочинності.....	159
Уфимцева О. С. Особливості інформаційного аспекту гібридної війни РФ проти України.....	161
Черниш Р. Ф. Використання месенджеру Viber з метою поширення деструктивного та «фейкового» контенту	163
Чіпуріна Г. М. Напрями протистояння ідеології «руського міру» у гібридній війні проти України	166
Щербина А. В. Релігійний екстремізм з боку Російської Федерації в умовах «гібридної» війни проти України	170
Прозоров А. Ю. Правові аспекти протидії пропаганді війни	174
Рекомендації круглого столу «Гібридна війна: сутність, виклики та загрози»	178

Наукове видання

**ГІБРИДНА ВІЙНА:
СУТНІСТЬ, ВИКЛИКИ ТА ЗАГРОЗИ**

Збірник матеріалів круглого столу

(Київ, 8 липня 2021 року)

Електронне видання

Друкується в авторській редакції

Технічне редагування *Коркач Т. О., Волкова В. Є.*

Видавець і виготовлювач

Національна академія Служби безпеки України,
03066, Київ, вул. Михайла Максимовича, буд. 22.

факс: (044)257-30-35

E-mail: academy@ssu.gov.ua

Свідоцтво суб'єкта видавничої справи ДК № 6844 від 17.07.2019.