ISSN 2227-5525. Мова і суспільство. 2017. Випуск 8. С. 47–55
Language and society. 2017. Issue 8. P. 47–55

УДК 321.01:323

КОМУНІКАЦІЙНО-КОНТЕНТНА БЕЗПЕКА ЯК ГЛОБАЛЬНИЙ НАПРЯМ РОЗВИТКУ КРЕАТИВНИХ ІНДУСТРІЙ У БЕЗПЕКОВІЙ СФЕРІ

Григорій Любовець

Військовий інститут
Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81, Київ, 03680, Україна
bmv0662@i.ua

Валерій Король

Військовий інститут
Київського національного університету імені Тараса Шевченка,
вул. Ломоносова, 81, Київ, 03680, Україна
valkor2005@ukr.net

Стаття присвячена дослідженню актуальних загроз національної безпеки в інформаційній сфері. Об'єктом аналізу є сучасні технології комунікаційно-контентних експансій з боку російських технологів проти демократичного світу. Розкрито можливості відповідей на такі загрози шляхом застосування креативних індустрій в безпековій сфері України та світу. Зроблено висновок про невідповідність управлінських стандартів державних органів влади сучасним публічним динамікам та необхідність використання соціолінгвістичних потенціалів креативних індустрій в безпековій сфері держави і суспільства. Обґрунтовано сутність поняття "комунікаційно-контентна безпека".

Ключові слова: інформаційна безпека, комунікаційно-контентна безпека, безпековий сектор, гібридно-месіанські агресії, інформаційні потоки, соціолінгвістика.

З початком окупації Криму та захоплення окремих районів Донецької та Луганської областей в 2014 р. Україна постала перед абсолютно новими викликами, відповіді на які вона шукає в партнерстві з міжнародними інституціями вже четвертий рік. Світ зрозумів, що необхідно наполегливіше добиватися виконання Кремлем Мінських домовленостей, що було підтверджено під час зустрічі лідерів країн "Великої сімки" на Сицилії [1].

Боротьбу з путінським режимом як гібридно-месіанським агресором потрібно вести (і певною мірою це вже здійснюється) і в сфері комунікаційно-контентної безпеки. Зростає потреба формування світового соціолінгвістичного дискурсу для активізації функціоналу дипломатично-інституційного рівня в царині глобальної безпеки та, водночас, системної різноформатної комунікаційно-контентної роботи з різними середовищами громад в країнах об'єднаної Європи. У зв'язку з цим потрібно відреагувати на відсутність цілісної технологічно-координаційної організації як креативно-ситуативної інфраструктури, яка б опікувалася системами адекватної діагностики та палітри аудитів (включаючи й лінгвістичний), координацією комунікаційно-контентної протидії в

загальнодержавному масштабі і яка б базувалася на технологічних рішеннях інноваційних сервісів безпекового сектору країни.

У такому формулюванні науковці не розглядали окреслені проблеми, хоча окремі аспекти висвітлюють праці В. Горбуліна, Д. Дубова, О. Власюка, У. Ільницької, М. Ожевана, Г. Почепцова тощо.

Мета статті – обґрунтувати потребу формування комунікаційно-контентної безпеки як самостійного напряму національної безпеки.

Завдання: 1) обґрунтувати потребу наукового аналізу поняття "комунікаційно-контентна агресія"; 2) розкрити комунікаційно-контентну агресію проти України; 3) розробити концепцію комунікаційно-контентної безпеки України.

У статті багатовимірні аспекти динамічних комунікаційно-контентних агресій проти української держави та суспільства, передусім нелінійні недетерміновані динамічні процеси і явища, досліджено за допомогою усталених індуктивно-дедуктивних методів та шляхом методики контекстного аналізу інформаційних резонансів.

1. Про потребу наукового аналізу змісту поняття "комунікаційно-контентна агресія"

За період 2015−2016 років Рада національної безпеки і оборони України на своїх засіданнях неодноразово розглядала питання "якісно нової державної політики, спрямованої на ефективний захист національних інтересів в економічній, соціальній, гуманітарній та інших сферах, комплексне реформування системи забезпечення національної безпеки та створення ефективного сектору безпеки і оборони України" [2]. Результатом цієї роботи стало схвалення (з наступним затвердженням Президентом України) таких визначальних для безпеки держави документів як Стратегія національної безпеки України (травень 2015 р.), Воєнна доктрина України (нова редакція, вересень 2016 р.), Концепція розвитку сектору безпеки і оборони України (березень 2016 р.), Стратегія кібербезпеки України (березень 2016 р.), Стратегічний оборонний бюлетень України (червень 2016 р.), Доктрина інформаційної безпеки України (лютий 2017 р.).

У перелік актуальних загроз національній безпеці країни в Стратегії національної безпеки України потрапили "інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу, комунікаційно-контентна агресія".

Розглядаючи актуальні загрози національній безпеці України, розробники перелічених документів не задавалися метою їхнього змістовно-креативного та інноваційного наповнення й обмежилися лише лінійним (традиційним) баченням за усталеними безпековими шаблонами НАТО, які залишаються в минулих реальностях і враховують віртуальні мережі, зазвичай, в парадигмі загроз з боку втручання в кібермережеві або кіберінфраструктурні ресурси. Такий спрощений підхід до кардинально важливих основ діяльності держави у безпековій сфері дезорієнтує українське суспільство і, власне, наших партнерів.

2. Комунікаційно-контентна агресія проти України

На заході кібернетична та інформаційна безпека виокремлені в окремі напрями дослідження та практичного застосування. Але у нас ці напрями традиційно поєднуються в одне ціле (можливо, за управлінського домінування в стратегічних інституціях мережевих технологів), що призводить до примітивізації процесу забезпечення саме інформаційної, тобто комунікаційно-контентної, складової. Підхід до цієї проблематики через призму нішевого бачення спеціалістів інформаційно-психологічних операцій, де

в основі лежить традиційне оперування інформаційно-психологічними операціями (війнами), набув ознак корпоративної лінійності і формального застосування технологічних рішень. Вони бувають ефективними на локальних аренах комунікаційно-контентного протистояння, але майже неефективні в сучасних динаміках та масштабних процесах геостратегічного домінування [3].

Усі ці традиційні (і законодавчо-нормативні) підходи, можливо, не були б вадами чи індикаторами провалів, якщо б ми в сучасних умовах четвертої промислової революції, що знищує кордони між країнами, державою і суспільством, державою і конфесіями, військовими і цивільними спеціалізаціями і навіть між сферами знань та електоральними нішами, не потерпали від масової і навіть експертно-управлінської неадекватності розуміння безпекового стану, в якому знаходиться сучасна Україна як арена геостратегічних процесів.

Автори статті вже звертали увагу громадськості на те, що сучасні "процеси геополітики переросли в геостратегічні моделі (з різними швидкостями розвитку міждержавної комунікації залежно від статусно-ресурсних можливостей учасників та важливості інтересів гравців з обох боків чи групової зацікавленості), оскільки глобалізація наблизила країни одну до одної за багатьма характеристиками, прямими й опосередкованими. А геостратегія, як модель співставлення різних векторів розвитку людства (якому, зазвичай, вже мало ділитися на сфери і воно більшою мірою визначається середовищами уваги), кличе в реальне життя – примушує стверджувати необхідність економіки сенсу (знань) для людства, а не просто відпрацьовані до автоматизму механізми монополізованих сфер [4].

Комунікаційно-контентна агресія Кремля є небезпечнішою за фізичну агресію, особливо, якщо дивитись на коротку і середньострокову перспективу України і її геосусідів. Процеси комунікаційно-контентних впливів та тотального домінування штучних соціолінгвістичних міфів, які потужно демонструють путінські креативно-технологічні центри на Донбасі та в АРК, довели факт реального творення віртуального світу, що навіть має свою назву "рускій мір". Ці технології перетворились у руках кремлівських пропагандистів в універсальний інструмент лінгвістично-мілітарного вторгнення у глобальних масштабах. Вони роблять це, поєднуючи в симбіозні конфігурації жорсткі пропагандистські методи та реалії відкритого медійного ринку, конкурентного контентно-комунікаційного дизайну з динамічними комунікаційно-контентними сервісами, де соціолінгвістичні сервіси та аудити стають ланкою комплексних динамічних моделей комунікаційно-контентного домінування. Так виникає єдиний енергетично-смисловий стиль корпоративних ідей як стиль державно-корпоратизованого режиму в симбіозі із мобілізованим суспільством й утворюється тотальна державна корпорація, реальну дієвість якої нам демонструє сучасний путінізм. На цей аспект неодноразово звертав увагу (з відповідними обґрунтуваннями) російський історик та публіцист Д. Шушарін [5]. Методи пропаганди та сучасні технології комунікаційно-контентних експансій стали надзвичайно ефективними в межах замкнутого віртуального середовища, в яке російські креативно-технологічні центри занурюють не лише власне суспільство, а й суспільства високої геостратегічної мотивації (як це відбулося в Нідерландах під час дискредитації референдуму щодо асоціації України з ЄС у квітні 2016 р.).

Однак у статті виокремлюємо ще один аспект – ефективний вплив сучасного путінського пропагандистсько-ситуативного моделювання та технологічного комунікаційно-контентного оперування публічною правдою як зброєю недовіри та етичного дисонансу проти становлення нових демократій – таких, як Україна. Це підтвердив на засіданні підкомітету з питань безпеки та оборони Європейського парламенту під час обговорення проблем інформаційної війни з боку Росії очільник підрозділу швидкого

реагування у сфері медіа Зовнішньої служби Європейського Союзу Гіл Портман (Giles Portman) 18 лютого 2016 р. Він заявив, що в країнах ЄС зростає кількість тих, хто підтримує політику Кремля, а це свідчить про те, що інформаційні зусилля путінських технологів поступово досягають мети: "Ми бачимо, наприклад, що половина населення Франції у недавньому опитуванні звинуватила Київ у війні в Україні, одна третина німців також це зробила, ми бачимо ріст кількості людей, які більше симпатизують Росії, ніж ЄС" [6].

Тут слід зазначити, що подібний розвиток ситуації вітчизняні аналітики прогнозували, звертаючи увагу державних інституцій, відповідальних за цей напрям роботи, на необхідність кардинального переформатування зусиль щодо активізації спротиву російській інформаційній агресії на міжнародному рівні [7].

Такого ефекту кремлівські технологи досягають за рахунок технологічно-креативного використання (дискредитації) форм і методів класичної публічної демократії. Західний масовий споживач звик на суспільно-ментальному рівні довіряти засобам масової інформації, які у свідомості пересічного західного громадянина ототожнюються зі сталим інститутом влади. Тому вміло подана в західних ЗМІ брутально-креативна брехня (інсинуації, занурені в місцевий соціолінгвістичний ландшафт суспільної перцепції та елітарної аперцепції) сприймається західним суспільством як достовірна і надійна інформація.

Продукуючи в промислових масштабах потоки інфікованих неправдою змістів та образів з агресивним підгрунтям, які на короткому часовому відрізку технологічно перемагають демократії з їхньою свободою вибору та довірою до офіційної публічної інформації з відомих глобальних медіаінституцій, кремлівські технологи за допомогою креативно-сценарних мистецьких конкурентних глобальних потоків не лише фокусують увагу на заданих тематиках, але й досягають у відкритих середовищах інтернет-спільноти впливу, близького до абсолюту. При цьому ефективно задіюються всі рівні контентних вимірів, сенсів і змістів – від актуальної публічної теми аж до аргументаційних ритмік і змістовних енергетик, що вимірюють ефективність креативних індустрій сучасності.

Саме тому в динамічному геостратегічному сьогоденні можливо сформувати так звану альтернативну Європу, про що говорив на щорічній Мюнхенській конференції з безпеки (лютий 2016 р.) Президент України П. Порошенко: "Ця альтернативна Європа має свого власного лідера. Його звуть пан Путін. Ця альтернативна Європа має своїх піхотинців. Це проросійські і антиєвропейські партії, які є в кожній європейській країні" [8]. Для створення цієї альтернативної Європи кремлівські технологи використовують потужні інноваційні арсенали креативних індустрій Заходу, технологічно добиваючись об'єднання радикального крила лівих та правих сил, до яких за створення відповідних геополітичних умов (наприклад, направлення в Європу цілеспрямованого потоку біженців) доєднуються націоналістичні, соціалістичні, соціал-демократичні ідеологічні табори.

Саме тому необхідність **"**технологічно-іноваційного стримування потенційного агресора" стає не просто нагальною потребою, а вимагає об'єднання зусиль провідних фахівців світу в галузі інформаційної (комунікаційно-контентної) безпеки та постійної уваги міжнародної спільноти як на рівні окремих країн, так і міжнародних інституцій (ООН, ОБСЄ, ПАРЄ тощо) [9: 117].

3. Концепція комунікаційно-контентної безпеки України

Зусилля українського уряду щодо інформаційного прориву (тобто, кібер-технологічного та комунікаційно-контентного) на Донбасі та в АРК наразі залишаються

недостатніми за динамікою скоординованих соціолінгвістичних векторів дій, масштабами та структурою охоплення, глибиною технологічних інфраструктур та креативно-сценарних рішень в різних сегментах інформпросторів України та світу. Це призводить до суттєвих втрат (і навіть провалів) публічних впливів, не кажучи вже про комунікаційно-контентні домінування на окупованих і прифронтових територіях – від населеного пункту до блок-посту чи переходу.

Україна четвертий рік поспіль відновлює інфраструктуру ефірного покриття на окупованих територіях і за ці три роки не застосовано технологічні та креативні системні рішення в середовищах життя громад, хоча вже заявили – організаційно і законодавчо – про достатній потенціал військово-цивільних адміністрацій. Український споживач інформаційної (комунікаційно-контентної) продукції (про західного мова не йде, це окрема тема) не має цілісної уяви про потокові процеси, які відбуваються в прифронтовій зоні та на окупованих територіях. Українські громадяни за лінією розмежування майже повністю віддані на поталу інформаційно-пропагандистським і креативним сервісним агресіям Кремля.

Особливо небезпечним в цьому плані є створення окупантами на Донбасі і в Криму нових місцевих ЗМІ та ЗМК, які покликані заповнити нестачу інформації на територіальному рівні. Вона є значно потужнішою, ніж була за мирного часу, та має перевагу в швидкості доходження до кінцевого споживача, оскільки будується на базі сучасних оптоволоконних мереж (за оперативними даними, в АРК ці проекти завершені повністю ще наприкінці 2015 р.).

У Верховній Раді є активний профільний комітет з питань свободи слова та інформаційної політики, який фіксує проблему протиріч між кібербезпекою і власне інформаційною (комунікаційно-контентною), але не знаходить позитивного нормативно-законодавчого вирішення. Створено Мінінформполітики, яке один із дипломатів, посол США в Україні пан Д. Паєтт в лютому 2016 року розкритикував: “У психології існує явище, яке називається дзеркальним відображенням, під час якого ви наслідуєте звичку відображати поведінку вашого опонента. І це, на мою думку, є одним із ризиків для України. Це величезна помилка для української влади, для українського народу, створити “фабрику тролів” як у Санкт-Петербурзі, просуваючи контрпропаганду в соціальних медіа. Це величезна помилка, щоб створити “Міністерство правди”, яке намагається створити альтернативні історії. Це не спосіб перемогти цю інформаційну війну” [10]. Пан посол прямо вказує управлінцям, що не може партнер США, ЄС і цивілізованого світу використовувати технологічні прийоми і філософію гібридно-месіанського агресора для продукування стандартів глобального гібридного путінського тероризму у світі, оскільки, такі спроби, як підтверджує дослідницька практика, тільки підсилюють вплив на публічне домінування кремлівських комунікаційно-контентних центрів.

Фундаментальною науковою-практичною проблемою постає інше ключове питання для всього безпекового сектору українського державотворення: кібербезпека, ресурсний масштаб мереж доступу до інтернету (мають статус приватної інфраструктурної монополії) чи інноваційно-технологічний національно-безпековий інфраструктурний комплекс (глобальна фундаментальна функція держави, а саме безпеково-інноваційного сектору, щодо творення стандартів та середовищ реальної цифрової демократії в сучасному житті Майданної України)?

Ще одне питання в парадигмі змін управлінсько-функціональних практик сьогодення – безпековий сектор перейде в режим прямої функціонально-процедурної та регламентно-інноваційної відповідальності перед громадянами і громадами чи він залишиться (за давніми управлінськими традиціями) транзитним корпоративно-технологічним анклавом закритих функціональних зон державного впливу управлінсько-номенклатурних еліт, які поділили між собою ресурсно-перспективні потенціали держави?

Сьогодні йде технологічно-лобістська війна за домінування над процесами, що відбуватимуться на базі інноваційно-технологічних цифрових рішень в масштабах мультифункціональних платформ. Питання про те, чи це буде тотальний банківський сервіс, чи інфраструктура міждержавних технологічно-інфраструктурних трастових гарантів на рівні НАТО чи ООН (унеможливлювали б узурпації в межах національних держав та використання в особистих приватно-партійних цілях технологічних потенціалів майбутнього) в даному випадку є вторинним.

Україна і її (за наявними потенціалами**)** надсучасний мультифункціональний безпековий сектор мали б зважитися на відповідальність за цю технологічно-інфраструктурну місію. Такий підхід був би надзвичайно важливим прикладним індикатором переходу (модернізації) безпекового сектору від технологічної ресурсної неадекватності до масової функції цілодобового характеру (а не тільки на віддалені ситуації особливого часу, яким нині оперує безпековий сектор).

Важливим сьогодні є стан і структура інформаційного простору України та його складових: інформаційного поля країни, регіональних комунікаційно-контентних середовищ, регіональних інформаційних полів областей, міжрегіональних комунікаційно-контентних середовищ тощо. Наразі методологічне питання про організацію координаційно-регламентного супроводу залишається поза увагою влади як центру прийняття управлінських рішень, хоча воно є принциповим з погляду формування відповідних сил, засобів, механізмів тощо для організації процесу адекватної протидії агресіям. До цього слід додати нагальну потребу розробки інноваційних технологічних ліній, тобто інформаційно-технологічних баз даних, які були б адекватними для застосування в детермінованих і недетермінованих процесах в державі. Наприклад, відсутні дослідження про особливостей розмежування інформаційних масивів комунікаційно-контентного характеру з цифровими даними і водночас резонансної інформації технологічно-безпекового значення тощо.

Окремим блоком питань постає проблема сучасних управлінських стилістик, зокрема, оперування інформаційними високодинамічними потоковими масивами.

Проблематичним у безпековому секторі є те, що моніторингові технології домінують, хоча вони не є базою для прогнозного моделювання домінантів контентного впливу на суспільну думку громадян. А технології, що є базою для прогнозної діагностики всіх недетермінованих процесів в суспільстві та безпековому секторі, не формуються тільки тому, що держава не розвиває гуманітарно-комунікаційні (лінгвістично-когнітивні) сфери і не затрачає необхідні ресурси та потужності сучасних інноваційно-технологічних рішень для ефективної роботи із публічними кон'юнктурами різних складових інформаційного простору України. Відтак ми і не запроваджуємо практику функціонування інноваційних сервісів та потужних промислових інформаційно-технологічних баз потоків даних соціолінгвістичних потенціалів. Причина проста: на управлінських рівнях не усвідомили нагальність і перспективність публічної політики і функціонального управління як основи євроінтеграційної та євроатлантичної модернізації. Не усвідомили і те, що ми всі вже живемо в епоху ситуативних сервісів тотальної публічності, а не в традиціях закритих корпоративних ситуативних центрів з очевидними тільки для владних еліт стратегічними проблемами.

Саме тому традиційні моніторингові технології як атрибут перехідного етапу від статичності і монопольності медіасередовищ до сучасних комунікаційно-контентних потокових сегментів різного масштабу інформаційних просторів національного та глобального виміру все частіше не відповідають сучасним публічним негативам (викликам, ризикам та загрозам) безпекового сектору держави.

Намагання політикуму та певної частини державних органів жити та діяти в стандартах традиційних управлінських систем корпоративно-галузевого характеру стосовно середовищ публічного життя громад “автоматично веде до затягування модернізації України як процесу синергетичного єднання потенціалів громад та державно-політичних інститутів України” [11: 65−69].

Для адекватного реагування на інформаційні (комунікаційно-контентні) виклики, ризики та загрози необхідно мати наукове обґрунтування можливостей новітніх технологічно-креативних сервісів фіксації, реакцій та сценарних моделей реагування для ефективної поточної функціональної діяльності. Безпековий сектор держави на всіх рівнях повинен отримати відповідний координаційно-регламентний функціонал із адекватним технологічним і ресурсним забезпеченням.

Комунікаційно-контентна безпека вимагає розвитку креативних індустрій в безпековій сфері держави і суспільства в глобальних масштабах**.**

Постає питання про Концепцію комунікаційно-контентної безпеки України як систему офіційних поглядів на мету, завдання, принципи й основні напрями забезпечення безпеки інформаційно-комунікаційної сфери державии.

Комунікаційно-контентна безпека – це створення правових умов на національному та міжнародному рівнях, фахово-технологічних мотивацій, інфраструктурних рішень для адекватного розвитку всіх сегментів комунікаційно-контентних процесів національного інформпростору, які б пришвидшували кристалізацію перспективних комунікаційних вимірів в громадах різних масштабів та забезпечували здатність використовувати сучасну (і майбутню) палітру інформаційних форматів потокового контенту.

Висновки

Випереджальний комплексний розвиток комунікаційно-контентної безпеки України убезпечить її від сучасних потокових публічних негативів (викликів, ризиків, загроз) та геостратегічних потокових публічних агресій з боку інших країн чи глобальних міжнародних гравців та “включить” модель публічних позитивів в суспільно-державне продукування сьогодення і майбутнього в національному та глобальному вимірах.

1. G7 Taormina Leaders’ Communiqué. [Електронний ресурс]. – Доступно з : http://www.g7italy.it/sites/default/files/documents/G7%20Taormina%20Leaders%27%20Communique_27052017_0.pdf
2. Стратегія національної безпеки України. [Електронний ресурс]. – Доступно з : http://www.rnbo.gov.ua/documents/396.html
3. *Моісеєва Т.* Тактика проти стратегії. Урядовий кур’єр, № 66, 07.04.2016.
4. *Любовець Г., Савчук Р.* Від геополітики територій до геостратегій публічності цифрової епохи. [Електронний ресурс]. – Доступно з : http://armyua.com.ua/vid-geopolitiki-teritorij-do-geostrategij-publichnosti-cifrovo%D1%97-epoxi/
5. *Шушарін Д.* Осягнення зла. [Електронний ресурс]. – Доступно з : http://day.kyiv.ua/uk/blog/polityka/osyagnennya-zla
6. Російська пропаганда у Європі дає плоди – посадовець ЄС. [Електронний ресурс]. – Доступно з : http://ua1.com.ua/world/rosiyska-propaganda-u-evropi-dae-plodi-posadovec-es-16890.html
7. *Любовець Г., Король В.* Ситуаційний сервіс МОУ як намагання держави протистояти новим загрозам геополітичного та техногенного характеру. [Електронний ресурс]. – Доступно з : http://armyua.com.ua/situacijnij-servis-mou-yak-namagannya-derzhavi-protistoyati-novim-zagrozam-geopolitichnogo-ta-texnogennogo-xarakteru/
8. Про що говорив Порошенко у Мюнхені: головні тези. [Електронний ресурс]. – Доступно з : http://www.slovoidilo.ua/2016 /02/13/novyna/polityka/pro-shho-hovoryv-poroshenko-u-myunxeni-holovni-tezy

9. *Любовець Г., Король В.* Ситуаційний сервіс Міністерства оборони України як намагання держави протистояти новим загрозам геополітичного та техногенного характеру. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К. : ВІКНУ, 2015. − Вип. № 50. – 385 с.
10. Посол США назвав помилкою української влади створення "фабрики тролів" та "Міністерства правди". [Електронний ресурс]. – Доступно з : http://tsn.ua/politika/posol-ssha-nazvav-pomilkoyu-ukrayinskoyi-vladi-stvorennya-fabriki-troliv-ta-ministerstva-pravdi-581603.html
11. *Любовець Г., Король В.* Моніторінгові технології як відображення контентного інформаційно-інерційного публічного еха // Вісник Київського національного університету імені Тараса Шевченка (Військово-спеціальні науки). − №1 (34). − 2016.

COMMUNICATION-AND-CONTENT SECURITY – GLOBAL APPROACH FOR CREATIVE INDUSTRIES IN SECURITY MATTERS WORLDWIDE

Liubovets Hryhorii

Military Institute, T.Shevchenko Kyiv National University
03680 Ukraine, Kyiv, Lomonosova st. 81
bmv0662@i.ua

Korol Valerii

Military Institute, T.Shevchenko Kyiv National University
03680 Ukraine, Kyiv, Lomonosova st. 81
valkor2005@ukr.net

Russian military-civilizational aggression against Ukraine, which started in 2014, made our country and the whole world face entirely new challenges.

One of these challenges is the dynamic creative and mental communication-and-content attacks against the Ukrainian state and society, produced by Kremlin not only in Ukraine but also internationally. Such situational combinations of aggressions in cyberspace are one of the greatest threats for Ukraine on the international arena, as well as for procedures, rules, and principles of international democracy.

The topicality of research. The authors research the dynamic aspects of current threats to national security, particularly in the information sector.

The authors propose to research the possibilities of overcoming hybrid-messianic aggressions of Putin's Russia through the paradigm of communication-and-content security as a new branch of national security.

This requires innovation from our country in the current international sociolinguistic discourse as well as from national and global security authorities. Simultaneously, a set of communication-and-content multiformat activities with different groups, communities, and societies, especially in Europe, is required.

The object of research is the modern technologies of dynamizing Russian communication-and-content aggressions against the democratic world and the possibility of neutralization of such threats by using creative industries in the national and global security sector.

Today, we need an integrated technological and coordinating organization, which is analytical in its nature, a creative and situational structure that would provide systems of monitoring and evaluating by determined options (including linguistic), coordination of communication-and-content countermeasures at the national level, based on technological solutions and innovative services for the security sector.

In our days, functioning and structure of Ukraine's information space and its components: information field of the country, regional and cross-regional communication-and-content environments, regional information fields, etc. are important. Currently, the methodological question of adequate organization of coordinating and regulatory support is overlooked by authorities (centers of decision-making). However, it is fundamental for the creation of forces, means, mechanisms, etc. for organizing adequate countermeasures. In addition, we have the urgent need to develop innovative technological lines (information technology databases), which could potentially be used "online" and are appropriate for application with determined and non-determined processes in the state and society.

In order to research the multidimensional options of dynamic creative and mental communication-and-content aggressions against Ukraine, especially non-determined and non-linear dynamic processes and phenomena, the authors have applied the method of contextual analysis of information resonances in addition to traditional methods (e.g. inductive-deductive).

Based on the analysis, the authors have arrived at the conclusion that current management standards of state authorities do not meet modern public dynamics. In addition, the sociolinguistic potential of creative industries need to be used in the field of state and society security.

The article provides a definition for "communication-and-content security" that allows scientific and practical application of the multifaceted aspects of national security and, in particular, security information.

As a result, the authors have developed approaches for creating advanced technological and coordinating structure of communication-and-content security of Ukraine which can protect the state and society from modern streaming public negatives (challenges, risks, and threats) as well as geostrategic streams of public aggression. It includes a model of producing public positives in the present and future in the national and global dimensions.

Practical application of the proposed approach for implementing technological solutions could be a development of adequate industrial-scale, legal, and functional situational service for monitoring, analysis, and solution scenario modeling as a response to strategic and geostrategic levels for public challenges, risks, and threats not only in the national security dimension but also on the international level.

Key words: information security, communication-and-content security, security sector, hybrid-messianic aggression, streams of information, situational service, sociolinguistics.

Стаття надійшла до редколегії 15 грудня 2016 року
Прийнята до друку 18 жовтня 2017 року