

УДК 316.77

ЛАПУТИНА Юлія Анатоліївна

РОЗВИТОК СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В СЛУЖБІ БЕЗПЕКИ УКРАЇНИ ЯК ЧИННИК СУТНІСНОЇ ТРАНСФОРМАЦІЇ ПІДХОДІВ ДО ПОБУДОВИ СУЧАСНОЇ УКРАЇНСЬКОЇ СПЕЦСЛУЖБИ

Постановка проблеми. Враховуючи, що відповідно до ст. 8 Закону України «Про основи національної безпеки України» [1] одним з основних напрямів державної політики з питань національної безпеки України є реформування правоохоронної системи з метою підвищення ефективності її діяльності, та беручи до уваги євроінтеграційний курс розвитку нашої країни, який передбачає наближення до сучасних стандартів взаємодії сектору безпеки та громадянського суспільства у подоланні викликів та загроз, вважається актуальним розглянути питання розвитку стратегічних комунікацій (далі – стратком) в Службі безпеки України в контексті сутнісної трансформації підходів до побудови сучасної української спецслужби.

Адже саме стратком відповідно до Воєнної доктрини України передбачає скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових

зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [2].

Аналіз останніх досліджень і публікацій. Аналіз сучасних досліджень свідчить про значну увагу науковців до проблематики стратегічних комунікацій. Разом з цим слід погодитись з думкою О. В. Кушнір [3] про те, що наукові праці зі словом «комунікація» в назві переважно політичної спрямованості стосуються філософських наук чи соціології. Також поняття «комунікація» розглядається як «інструмент політики, «система інституцій», «системна взаємодія».

Вітчизняні дослідники вивчають досвід міжнародних альянсів із запровадження та функціонування стратегічних комунікацій. Так, А. В. Баровська [4], аналізуючи досвід НАТО, зазначає, що діяльність Альянсу зі стратегічних комунікацій є усталеною практикою, що має місце з 2007 року. При цьому тема стратегічних комунікацій є предметом уваги провідних науково-експертних центрів, зокрема

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

RAND Corporation та Chattem House [5].

На думку С. А. Гуцала [6], проблематика стратегічних комунікацій є найменш дослідженою серед українських науковців і до певного часу поняття «стратегічних комунікацій» у вітчизняній науці циркулювало переважно у сферах маркетингу, менеджменту, політичних комунікацій.

Першу спробу визначити, систематизувати понятійний апарат у сфері страткому було здійснено Т. В. Поповою та В. А. Ліпканом у виданні «Стратегічні комунікації» [7].

В СБ України значну увагу дослідженням соціальних комунікацій приділялося Л. Ф. Компанцевою [8].

Зараз спостерігається спрямованість вітчизняних науковців на вивчення іноземного досвіду, організаційно-правових аспектів впровадження страткому, аналіз комунікативних викликів інститутам сектору безпеки та оборони, розгляд принципів планування та оцінювання діяльності у сфері страткому. Разом з цим в умовах трансформації структури викликів та загроз безпеці України, обрання нашою державою сталого курсу на євроінтеграцію найбільш актуальним є вивчення страткому в контексті пошуку сучасних шляхів оновлення методологічних підходів до організаційно-управлінської діяльності та побудови процесу оперативної роботи вітчизняної спецслужби.

Мета статті. З огляду на зазначене метою статті є викладення ре-

зультатів аналізу можливостей підвищення ефективності діяльності СБ України у разі запровадження страткому як механізму оптимізації організаційно-управлінської діяльності та способу реалізації оперативного процесу в умовах необхідності адекватної відповіді на сучасні виклики та загрози безпеці України.

Завданнями статті є:

– аналіз поняття та сутності страткому з урахуванням наявної нормативно-правової бази та наукових досліджень у контексті можливостей його запровадження в діяльності СБ України;

– виявлення особливостей та умов його застосування у міжнародній практиці;

– визначення переваг застосування стратегічних комунікацій як методологічного підходу в організації діяльності спецслужби;

– визначення пріоритетних напрямів розвитку страткому в діяльності СБ України;

– надання пропозицій щодо розвитку страткому в контексті адекватного реагування сектору безпеки на трансформацію сучасних викликів та загроз безпеці України.

Виклад основного матеріалу.

На загальнодержавному рівні термін «стратегічні комунікації» визначено у Воєнній доктрині України [2] (далі – Воєнна доктрина) та згадується у таких концептуальних документах:

– Концепція розвитку сектору безпеки і оборони України [9];

State policy of Ukraine in the field of the information security of person, society and state

– Стратегія сталого розвитку «Україна – 2020» [10].

Відповідно до Воєнної доктрини (абзац 17 п. 4 розділу I) стратегічними комунікаціями є скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави.

Посилення розвідувальної діяльності в інтересах підготовки та проведення Україною стратегічних комунікацій, контрпропагандистських заходів та інформаційно-психологічних операцій розглядається Україною, крім інших основних заходів і дій, як основа кризового реагування на воєнні загрози та недопущення ескалації воєнних конфліктів (п. 32 розділу III Воєнної доктрини).

Воєнною доктриною також визначено, що «з метою досягнення переваги над воєнним противником мають бути посилені заходи з реалізації державної інформаційної політики на тимчасово окупованій противником території і міжнародній арені. Забезпечення інформаційної складової воєнної безпеки здійснюватиметься шляхом запровадження ефективної системи заходів стратегічних комунікацій у діяльність органів сектору безпеки» (п. 41 розділу III Воєнної доктрини).

Поняття страткому, його сутність, зміст, складові ретельно опрацьовано вітчизняними науковцями

А. В. Баровською [4], О. В. Кушнір [3], Г. Г. Почепцовим [11] та ін.

Заслужують на увагу результати дослідження П. Корніша, Ю. Ліндлі-Френча та К. Йорка, представлені у доповіді Chattem House. Зокрема, автори визначають, що у широкому сенсі «стратегічні комунікації» – це трансформація процесу сприйняття цільовими аудиторіями та зацікавленими сторонами в напрямку формування відповідної політики, планування та здійснення операцій на кожному рівні [5, с. 4].

Переважає більшість дослідників зазначає, що поява поняття та виокремлення страткому в самостійне явище в сфері соціальних комунікацій значною мірою було викликано необхідністю розробки адекватного механізму відповіді держав та суспільств на зміну викликам та загрозам, які характеризувалися асиметричними, нелінійними методами, мережевоцентричністю, використанню сучасних технологій в період стрімкого розвитку інформаційного суспільства.

Як справедливо зазначає Д. Дроздовський, небезпека мережевих війн полягає у тому, що «людина може спрямовувати сили одразу в кількох напрямках. Комп'ютерні технології дають можливість керувати зброєю на відстані в кілька тисяч кілометрів, спрямовувати удар так, як потрібно. І на все йде кілька секунд» [12].

Сталі, ієрархічно побудовані інститути сектору безпеки, зарегламентовані внутрішніми нормативно-

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

правовими обмеженнями та жорсткою вертикаллю прийняття рішень, засновані на принципі послідовності покрокових дій з необхідністю зворотного зв'язку у відповідь на кожну дію, не справлялися зі своєчасним реагуванням. Ситуація ускладнювалася браком комунікації держави з суспільством, що спричиняло збільшення рівня вразливості країн до нових загроз. Особливо показовими виявилися приклади з неспроможністю, навіть найбільш розвинутих країн, попередити низку руйнівних терактів та кібератак протягом останніх двох десятиліть.

Отже, поряд з традиційними формами протидії сучасність ознаменувала появу та розвиток нових видів ведення війни та у таких конфліктах, як військова агресія РФ проти України, віддання переваги саме мережевоцентричним, інформаційно-психологічним складовим. Адже цей вид протидії дозволяє з використанням інформаційно-психологічних впливів на свідомість/підсвідомість людини досягти зміни поведінки різних соціальних груп з метою досягнення односторонніх воєнних, соціально-політичних чи економічних переваг над супротивником [13].

За висновками Н. О. Марути, М. В. Маркової, ведення інформаційно-психологічної війни дозволяє агресору в країні впливу досягти суспільної дестабілізації, стимулювати недовіру, загострення ворожнечі й боротьби за владу, провокувати

репресії з боку влади; ввести населення в оману в питаннях роботи державних органів влади, підірвати їх авторитет, дискредитувати дії; спровокувати соціальні, політичні, національно-етнічні, релігійно-конфесійні зіткнення; нівелювати історичну, національну самобутність народу; змінити системи цінностей та світогляд людей; маргіналізувати суспільство, спровокувати соціальну інертність, зниження потреб у пізнанні історичної спадщини у суспільстві; створити у народу країни, щодо якої здійснюється агресія, почуття меншовартості; підірвати міжнародний авторитет держави, її співпрацю з іншими державами; сприяти формуванню почуття невідворотності поразки, втрати волі до боротьби та перемоги; нав'язати власний спосіб життя як поведінки та світогляду майбутнього; ввести різні групи населення у стан фрустрації; підірвати моральний дух та психологічну стабільність населення та особливо армії [14].

Вказане досягається залякуванням населення образом ворога; дезорієнтацією, дезінформацією мас; послабленням переконань; внесенням у свідомість ворожих, шкідливих ідей, поглядів шляхом цілеспрямованого агресивного викривлення інформаційного простору з використанням особливостей психофізіології людини, маніпулювання суспільною свідомістю і політичною орієнтацією населення, прихованості механізму впливу (особливо на підготовчих стадіях до початку безпосередньої військової операції).

State policy of Ukraine in the field of the information security of person, society and state

Таким чином, сутність мережево-центричної війни полягає у досягненні перемоги над противником шляхом формування інформаційно-комунікативної та управлінської переваги над ним [15]. Вона також передбачає застосування заходів пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях.

Вивчення аналітичної записки Національного інституту стратегічних досліджень України (НІСД) щодо інформаційно-психологічної складової агресії РФ проти України свідчить, що намагання РФ провести кампанію проти України супроводжувалось діями, які мали всі ознаки підготовленої та продуманої за цілями, заходами та наслідками інформаційно-психологічної спецоперації, скерованої, в першу чергу, на російську, а з іншого боку, на українську та західну аудиторію.

Завданнями цієї спецоперації були: деморалізація населення України; деморалізація особового складу збройних сил та силових відомств, спонукування їх до державної зради й переходу на бік супротивної сторони; формування у громадян Росії та України викривленого «медіа-бачення» подій, що відбуваються, а не їх дійсних причин та наслідків; створення вигляду масової підтримки дій РФ з боку населення Південно-Східних регіонів; психологічна підтримка українських прихильників радикального зближення регіонів Сходу й Півдня України з РФ.

Зазначені завдання реалізувались через повний спектр каналів комунікацій з використанням методів інформаційно-психологічної боротьби. Також з метою посилення впливу вказаних каналів на населення застосовувалися традиційні заходи – перешкоджання діяльності ЗМІ на Кримському півострові, спроби блокування мережі Інтернет та окремих веб-ресурсів.

За своїми основними меседжами, стилем і внутрішньою логікою операція з дезінформації та інформаційно-психологічного тиску, розпочата РФ довкола питань «волевиявлення» населення в АР Крим і Південно-Східних регіонів України, виглядає складовою (можливо, черговим етапом) більш широкої спеціальної російської інформаційної кампанії, розв'язаної як мінімум у листопаді 2013 року, через події на Майдані.

Абсолютна більшість російських традиційних ЗМІ включились в інформаційно-психологічну боротьбу проти України, намагаючись підтримати проведення військової операції. Такі видання, як «Известия», «Российская газета», «Московский комсомолец», «Коммерсантъ», «Взгляд», а також інформаційні агенції «РИА Новости», «ИТАР-ТАСС», «РОСБАЛТ», «АИС» не лише передруковували неперевірені новини, але й самі були помічені у створенні цілком неправдивих повідомлень (наприклад, щодо переходу на бік Росії корабля ВМС України «Гетьман Сагайдачний»).

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

Якщо порівняти наведені вище теоретичні викладки стосовно сучасних особливостей ведення війни з аналізом, проведеним НІСД України щодо агресії РФ проти нашої держави, можна зробити висновок, що на нинішньому історичному етапі проти України застосовуються всі основні види військового протидіяння. Особливо активними при цьому виступають мережевоцентричні та інформаційно-психологічні методи агресії. Це є однією з найбільш важливих характеристик оперативної обстановки, яка має бути прийнята до уваги СБ України при розробці ключових напрямів діяльності по забезпеченню безпеки України.

Крім цього, саме такий характер оперативної обстановки вимагає розробки та застосування адекватних моделей реагування на вказані виклики в контексті не тільки реактивної відповіді, але й запровадження проактивної наступальної моделі діяльності.

В умовах, коли проти нашої держави активно застосовуються методи інформаційно-психологічних та мережевоцентричних війн, що характеризуються перевагами горизонтально побудованих мереж з паралельним, а не послідовним способом взаємодії ланок, проактивність відповіді спецслужб полягає не тільки у виявленні, попередженні та припиненні діяльності ворожих мереж, але й у своєчасній зміні методології організаційно-управлінської побудови СБ України.

В її основу має бути покладений механізм стратегічної комунікації, який дозволить створити у державі ефективну парасольку захисту від сучасних загроз, нейтралізація яких сталими, загальноприйнятими та незмінними за радянських часів способами не виявляється достатньо ефективною.

У цьому контексті цікавими є результати дослідження НІСД України щодо найбільш ефективних шляхів стримування агресивних дій РФ у період розгубленості державних органів України, слабкості та нестабільності влади. Так, за висновками, що містяться в аналітичній записці, найбільш ефективним механізмом протидії (як на інформаційному, так і реальному рівні) стало використання громадської журналістики та максимально широке висвітлення того, що відбувається в режимі он-лайн. Коли російська сторона намагалась створити виключно прийнятне для неї «постановочне» тло подій, онлайніві трансляції з використанням «Stream-TV» дозволили дезавувати більшість провокаційних заяв, а в окремих випадках – попередити провокації з боку озброєних людей.

Саме формат онлайнівого стріму, який здійснювався під час Майдану, став суттєвою проблемою для російських військових, які не знали як реагувати на таких «громадянських журналістів». Заклик «Максимальне висвітлення!» дійсно став адекватним до цієї ситуації [16].

State policy of Ukraine in the field of the information security of person, society and state

Аналогічним шляхом спрацювала система «Зелло», яка дозволяла активним громадянам он-лайн комунікувати, своєчасно попереджати один одного про провокації та спрямовувати зусилля на стримування агресивних дій. Отже, здатність соціуму організовуватися у мережі та сучасна готовність технологічної підтримки цим процесам стала ледь не єдиним механізмом протидії достатньо потужній як в ресурсному, так і у військовому, політичному, інформаційному сенсі агресивній кампанії РФ проти України.

Висновки. Оперативна обстановка висуває перед СБ України вимоги нагальної зміни методологічних підходів до організаційно-управлінської побудови, здійснення оперативного процесу в контексті підвищення її інституційної спроможності та адекватного реагування на сучасні загрози безпеці України.

Необхідність вчасного реагування на виклики та загрози в епоху інформаційного суспільства потребує від спецслужби приведення механізму реагування у відповідність до особливостей, структури та процесу практичної реалізації дій, які можуть вважатися ознаками загроз.

Однією з ключових характеристик середовища, яке може вважатися потенційно агресивним для держави та суспільства у безпековому вимірі, є мережева організація, яка передбачає синхронний, а не послідовний спосіб комунікації. Саме так діють

терористичні угруповання, створюючи невидимі для лінійно організованих безпекових структур мережі. Подібними методами організуються хвилі негативного впливу на безпеку держави у медіа та соціальних мережах тощо.

Отже, у сучасному світі для того, щоб бути ефективною, спецслужба має перейти від принципу послідовності організаційно-управлінського циклу до принципу синхронності.

Традиційно прийнятий в безпекових структурах після Другої світової війни принцип послідовного реагування на загрози – від проблеми до її рішення, з проміжними оціночними критеріями, системою показників ефективності – до цього часу вважався найбільш успішним у багатьох країнах. Переважала також думка про те, що чим складніше проблема, тим краще керуватися саме послідовним принципом: ідентифікація, збирання даних, узагальнення, аналіз із використанням різних методик, формування підґрунтя для прийняття рішення, безпосереднє прийняття рішення та його реалізація.

Суттєвими недоліками такого підходу є те, що, з одного боку, він не відповідає закладеним природою людини механізмам здійснення когнітивних процесів, адже процес розумової діяльності не є лінійним; з іншого – заважає гнучкості реагування на загрози у зв'язку з неможливістю вчасної відповіді на виклики через тривалий процес послідовної взаємодії ланок.

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

Крім цього, у середовищі європейських аналітиків також існує думка про те, що орієнтація на циклічність та послідовність організації діяльності спецслужб має ще один недолік: циклічність використовується відповідними адміністраторами та керівниками, які заважають прогресивним змінам, що гальмує процес діяльності. «Безкомпромісна орієнтація на цикл є однією з причин недостатнього обміну ідеями та неповного спільного використання інформації як в середині агентства, так і між агентствами», – вважає Ф. Шреєр [17].

Отже, альтернативою класичному організаційно-адміністративному механізму управління у сфері діяльності спецслужб в сучасних умовах може стати цілеорієнтований підхід, сконцентрований на відповідній мішені (загрозі). При цьому вище керівництво країни, яке формулює запит на інформацію, також стає частиною загальнодержавного механізму реагування. Враховуючи нелінійний характер побудови мережі, усі її учасники фокусуються на меті та отримують можливість скласти свою картину об'єкта впливу, додавши до його образу елементи, які можуть бути вивчені ексклюзивно тільки ними.

Маючи горизонтальний спосіб організації, процес вивчення об'єкта-мішені завдяки багатоаспектності кожного члена мережі дозволить створити найбільш реальну незалежну картину та забезпечить вчасне реагування завдяки відсутності зайвих управлінських ланок та цілеорієнтованості,

а не «процесоорієнтованості» діяльності. Підвищенню ефективності реагування при цьому також сприятиме взаємна незалежність учасників мережі від вертикально побудованої бюрократичної системи.

Таким чином, цілеорієнтоване співробітництво створюватиме умови до гнучкого формування в структурі сектору безпеки ефективних фахових команд реагування на загрози та зміни в їх структурі, примножуючи при цьому комунікативні спроможності держави та розширюючи безпекову мережу.

Інформаційна революція здійснила вплив на структуру діяльності усіх сфер. Разом з цим, ураховуючи особливості розвитку приватного сектору, орієнтованість на конкуренцію та отримання прибутку, слід зазначити, що він випередив державну бюрократичну машину у швидкості та якості адаптації до збирання, аналізу інформації та реагування на виклики. Особливо це стосується спроможностей отримання, узагальнення, аналізу та використання інформації з відкритих джерел.

Саме тому одним із шляхів підвищення діяльності спецслужби сьогодні виявляється запровадження ефективних моделей комунікації з громадянським суспільством, приватним сектором, науково-експертним середовищем, медіа-спільнотою з безпекових питань. Розвиток комунікативних платформ, майданчиків сприятиме розширенню та зміцненню безпекових мереж та створюватиме умови

State policy of Ukraine in the field of the information security of person, society and state

для гнучкого вчасного реагування на загрози різних рівнів.

У сучасних умовах у споживачів інформації від спецслужб, а саме у вищого військово-політичного керівництва країни, виникає гостра потреба у своєчасному отриманні практично значущої та попереджувальної інформації. Вирішення цієї проблеми також значною мірою лежить у площині оптимізації комунікативних спроможностей у секторі безпеки. У цьому контексті заслуговує увагу тенденція до продовження дії старих бюрократичних нормативно закріплених правил обміну інформації між різними ланками сектору безпеки на фоні практичної зміни каналів обміну інформацією з урахуванням появи нових сучасних технологічних можливостей. Адже за останні роки створилося багато різних за характером

організації, структурою та технологічними особливостями комунікативних майданчиків та платформ, що значно прискорюють обмін інформацією та прийняття рішень. З метою оптимізації прийняття рішень у секторі безпеки та підвищення ефективності реагування, використання вказаних платформ має бути інституалізовано та практично запроваджено в систему мережевоцентричної організаційно-управлінської побудови процесу діяльності спецслужби.

Таким чином, вважається, що стратегічні комунікації можуть стати дієвим механізмом удосконалення реагування СБ України на сучасні виклики та загрози в умовах активізації застосування проти України мережевоцентричних сценаріїв ведення агресивної війни.

Список використаних джерел

1. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

2. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» від 24 вересня 2015 року № 555/2015.

3. Кушнір О. В. Поняття та сутність стратегічних комунікацій у сучасному українському державотворенні [Електронний ресурс] / О. В. Кушнір. – Режим доступу : [http://goal-int.org/ponyattya-ta-](http://goal-int.org/ponyattya-ta-sutnist-strategichnix-komunikacii-u-suchasnomu-ukrainskomu-derzhavotvorenni/)

[sutnist-strategichnix-komunikacii-u-suchasnomu-ukrainskomu-derzhavotvorenni/](http://goal-int.org/ponyattya-ta-sutnist-strategichnix-komunikacii-u-suchasnomu-ukrainskomu-derzhavotvorenni/).

4. Баровська А. В. Стратегічні комунікації: досвід НАТО [Електронний ресурс] / А. В. Баровська. – Режим доступу : <http://sp.niss.gov.ua/content/articles/files/24-1436781085.pdf>.

5. Strategic Communications and National Strategy : A Chatham House Report / Paul Cornish, Julian Lindley-French and Claire Yorke. – London, 2011. – 42 p.

6. Гуцал С. А. Публічна дипломатія та стратегічні комунікації: визначення концептуальних основ [Електронний ресурс] / С. А. Гуцал. – Режим доступу :

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/2769/24736.

7. Попова Т. В. Стратегічні комунікації: [словник] / Т. В. Попова, В. А. Ліпкан / за заг. ред. В. А. Ліпкана. – К. : ФОП О. С. Ліпкан, 2016. – 400 с.

8. Компанцева Л. Ф. Комунікативні виклики інститутам сектору безпеки та оборони світу як передумови виникнення страткому / Л. Ф. Компанцева // Інформаційна безпека людини, суспільства, держави. – К. : НА СБ України. – 2017. – № 1(12). – С. 17–29.

9. Концепція розвитку сектору безпеки і оборони України : затверджена Указом Президента України від 14 березня 2016 року № 92.

10. Стратегія сталого розвитку «Україна – 2020» : схвалена Указом Президента України від 12 січня 2015 року № 5.

11. Почепцов Г. Г. Стратегические коммуникации: стратегические коммуникации в политике, бизнесе и государственном управлении / Г. Г. Почепцов. – К. : Альтерпрес, 2008. – 216 с.

12. Дроздовський Д. Людина інформаційна Яку загрозу несе для нас епоха інтернету? [Електронний ресурс] / Д. Дроздовський. – Режим доступу : <https://day.kyiv.ua/uk/article/cuspilstvo/lyudina-informaciyna>.

13. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій : навчальний посібник [Текст] /

В. М. Петрик, О. А. Штоквиш, В. В. Кальниш [та ін.]. – К. : Росава, 2006. – 208 с.

14. Марута Н. О. Інформаційно-психологічна війна як новий виклик сучасності: стан проблеми та напрямки її подолання / Н. О. Марута, М. В. Маркова // Український вісник психоневрології. – 2015. – Т. 23, вип. 3. – С. 21–28. – Режим доступу : http://nbuv.gov.ua/UJRN/Uvr_2015_23_3_5.

15. Дацюк А. В. Особливості сучасних збройних конфліктів: від конвенційного протистояння до гібридної та мережевоцентричної війни [Електронний ресурс] / А. В. Дацюк. – Режим доступу : <http://matrix-info.com/2017/03/21/osoblyvosti-suchasnyh-zbrojnyh-konfliktiv-vid-konventsijnogo-protystoyannya-dogibrydnoyi-ta-merezhevo-tsentrychnoyi-vijny/>.

16. Щодо інформаційно-психологічної складової агресії Російської Федерації проти України (за результатами подій 1–2 березня 2014 року) : аналітична записка [Електронний ресурс]. – Режим доступу : <http://www.niss.gov.ua/articles/1476/>.

17. Шреер Ф. Трансформирование разведывательных служб: как сделать их более сильными, динамичными, результативными и эффективными : монография / Ф. Шреер. – К.; Женева : Янтарь, 2011. – 305 с.

18. NATO Strategic Communications Policy [Електронний ресурс]. – Режим доступу : <http://info.publicintelligence.net/NATO-STRATCOM-Policy.pdf>.

Рецензенти:

доктор філологічних наук, професор

Л. Компанцева,

доктор юридичних наук, професор

А. Марущак

State policy of Ukraine in the field of the information security of person, society and state

Аннотация. В статье изложены возможности повышения эффективности деятельности СБ Украины при внедрении страткома как механизма оптимизации организационно-управленческого функционирования и способа реализации оперативного процесса. Автор анализирует понятие и сущность страткома с учетом имеющейся нормативно-правовой базы и научных исследований по этой теме, описывает особенности и условия его использования в международной практике, отмечает преимущества и приоритетные направления применения стратегических коммуникаций как методологического подхода по организации деятельности спецслужбы и вносит предложения по развитию страткома в условиях трансформации современных вызовов и угроз безопасности Украины.

В статье делаются выводы о возникшей насущной проблеме в своевременном получении практически значимой и упреждающей информации структурами спецслужб и государственными институтами, решение которой в значительной степени лежит в плоскости улучшения коммуникативных возможностей. Кроме того, указывается, что в целях оптимизации принятия решений в секторе безопасности и повышения эффективности реагирования использование указанных платформ должно быть институционализировано и практически внедрено в систему сетецентрического организационно-управленческого построения процесса деятельности спецслужбы.

Ключевые слова: стратегические коммуникации, координация коммуникативных возможностей государства, публичная дипломатия, связи с общественностью, военные связи, информационные операции, психологические операции.

Abstract. The article deals with intensification possibilities of the Security Service of Ukraine in the course of strategic communications implementation as a tool of managerial functioning optimization and optimization of operational process realization. The author analyzed the definition and essence of strategic communications taking into account the present regulatory and legal framework and scientific researches on the topic. The author depicted the peculiar features and conditions of strategic communications usage in the international practice; denoted the advantages and priority guidelines of strategic communications usage as a methodological approach to the secret service activity arrangement; and submitted an offer how to improve strategic communications under the conditions of modern challenges transformation and Ukraine security threats.

There were made a conclusion about a vital challenge to get timely the crucial and warning information by the secret services and state institutions, the problem solving was centered around communication abilities improving. As well as it was noticed the use of mentioned framework should be institutionalized and implemented into the network managerial process structure of secret service activity to optimize the decision making in security sector and increase the security response effectiveness.

Key words: strategic communications, coordination of state communication abilities, public diplomacy, public affairs, military communications, information operations, psychological operations.