УДК 35.078

ОСТРОУХОВ Володимир Васильович
ПРИСЯЖНЮК Микола Миколайович

ІНФОРМАЦІЙНІ ЗАГРОЗИ ДЕРЖАВНІЙ БЕЗПЕЦІ УКРАЇНИ У ГІБРИДНІЙ ВІЙНІ

Постановка проблеми. Існування, самозбереження та прогресивний розвиток України як суверенної держави залежать від здійснення цілеспрямованої політики щодо захисту її національних інтересів і забезпечення державної безпеки.

Швидкий розвиток процесів інформатизації на початку XXI століття спричинив виникнення нової глобальної соціотехнологічної проблеми – проблеми інформаційної безпеки людини, суспільства та держави.

Суть цієї проблеми полягає в тому, що найважливіші інтереси людини, суспільства, держави та й усієї світової цивілізації сьогодні визначаються станом навколишньої інформаційної сфери. Тому цілеспрямовані чи ненавмисні впливи на інформаційну сферу зовнішніх чи внутрішніх джерел можуть завдати шкоди цим інтересам і являють собою загрози інформаційній безпеці людини, суспільства та держави. Однією з таких загроз є зовнішня інформаційна експансія.

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Росія використовує найновіші інформаційні технології впливу на свідомість громадян із метою розпалювання національної та релігійної ворожнечі, пропаганди агресивної війни, зміни конституційного ладу насильницьким шляхом, порушення суверенітету та територіальної цілісності України [1].

Проведення гібридної агресії Російською Федерацією проти України несе в собі постійні виклики державній безпеці України.

Багатовимірність гібридних загроз державній безпеці потребує створення адаптивної системи протидії.

Із цією метою важливим є дослідження загроз державній безпеці в інформаційній сфері для розроблення адекватних ефективних заходів і засобів забезпечення захищеності державного суверенітету, територіальної цілісності та демократичного конституційного ладу в Україні.

Аналіз останніх досліджень і публікацій. У сучасних умовах геополітичний авторитет держави на міжнародній арені, її можливості впливати на світові події залежать не лише від економічної та військової

могутності. Зростає значення інформаційного фактора на фоні силових.

З'явилися нові форми протиборства. З поступальним розвитком людства відбувається й еволюція воєн та збройних конфліктів, змінюються їхні зміст, характер та особливості, з'являються нові форми й способи їх ведення.

Останніми роками виникла нова форма воєнного конфлікту, який починається з «мирних» антиурядових акцій, що переростають у жорстке громадянське протистояння, і завершується зовнішньою інтервенцією. Такі конфлікти можна назвати новим типом воєн сучасної епохи.

Відомий американський військовий теоретик Френк Хоффман один із перших зазначив: «... війни сучасної епохи характеризує процес гібридизації, у межах якого змішуються традиційні форми війни, кібервійни, організованої злочинності, іррегулярних конфліктів, тероризму і т. п.» [2].

Він запропонував термін «гібридна війна», що найточніше відображає важливі зміни в характері воєн при збереженні їхньої незмінної природи.

Однією з важливих складових гібридної агресії є інформаційна війна.

Більшість держав розглядають інформаційну війну як ефективний інструмент реалізації зовнішньої політики, що дає можливість здійснювати інтенсивний вплив на процеси всіх рівнів державного і суспільного устрою в будь-якому регіоні світу.

В умовах розвитку засобів масової інформації (далі – ЗМІ), інформаційних технологій і техніки інформаційне протиборство у світі стає масштабнішим і результативнішим. Поява технічних засобів нового покоління, що здатні ефективно впливати не тільки на психіку та свідомість людей, але й на інформаційно-технічну інфраструктуру держав та їхніх збройних сил, дає змогу розглядати інформаційну зброю як засіб масового ураження.

Стрімкий розвиток ЗМІ не міг не спричинити активізацію інтересу до можливостей масштабного психологічного впливу на політичних і бізнесових опонентів. Розвиток новітніх технологій зумовив перехід від так званої класичної війни до війни нового типу – інформаційно-психологічної.

Інформаційна війна є узгодженою діяльністю з використання інформації як зброї для ведення не лише бойових дій, а й у періоди, коли немає відкритого воєнного протистояння [3].

У наукових дослідженнях у сфері ведення інформаційної війни звертається увага на цілу низку аспектів цього явища. Серед них політичні, економічні, соціальні, психологічні тощо. Досліджували цю проблематику закордонні та вітчизняні науковці, а саме: Ю. Бабенко, Д. Догерті, В. Желіховський, М. Лібікі, В. Ліпкан, Ю. Максименко, Г. Почепцов, В. Сливка та ін.

Водночас через складність, комплексність і багатоаспектність ця проблематика досі не вичерпана. Це також пов'язано зі стрімким розвитком інформаційних технологій і, відповідно, розвитком та використанням соціальних мереж для здійснення інформаційно-психологічного впливу.

Метою статті є дослідження інформаційних загроз державній безпеці України в гібридній війні Російської Федерації на тимчасово окупованих територіях Донецької та Луганської областей і в Автономній Республіці Крим як реальних загроз невоєнного характеру.

Завданнями статті є: 1) дослідження напрямів інформаційно-психологічного впливу, що здійснює Російська Федерація на тимчасово окупованих територіях Донецької та Луганської областей і в АР Крим; 2) визначення основних загроз державній безпеці в інформаційній сфері, спрямованих на дискредитацію вищого воєнно-політичного керівництва держави, провокування антидержавних настроїв в Україні та проведення пропагандистських заходів із метою формування культурної ідентичності населення окупованої території АР Крим із населенням Росії; 3) аналіз деструктивного інформаційно-психологічного впливу як складової загроз державній безпеці України в інформаційній сфері, спрямованих на ослаблення та розкол країни зсередини.

Виклад основного матеріалу. У сучасному світовому політичному процесі гібридну війну розглядають як цілеспрямований процес установлення тотального контролю над сферою державного управління, де одну з вирішальних ролей відіграють інформаційні засоби, що і призводить до капітуляції збройних сил противника.

Такі війни виходять за межі традиційних понять, вони набувають комбінованого характеру, перетворюючись на клубок політичних інтриг, запеклої боротьби за політико-економічне домінування над країною, за території, ресурси й фінансові потоки. Причому сторони вдаються до всіх можливих засобів і будь-яких, навіть найнебезпечніших, прийомів та дій – як силових, так і несилових.

В інформаційну епоху, коли роль і значення інформаційних комунікацій кардинально змінюються, розпочато ретельне вивчення впливу інформації на суспільство саме тому, що інформація стала основним продуктом виробництва й основним засобом впливу на масову свідомість.

Інформаційний вплив є частиною гібридної війни, а інформація – це реальна зброя, в якій ключове значення мають засоби масової інформації, інтернет-ресурси. Інформаційна зброя здатна знищити найважливіше, що є в людини, – її свідомість.

У сучасних умовах інформаційна безпека розглядається як пріоритет у системі національної безпеки. Тому слід зазначити, що без сучасної інформаційної політики в держави немає майбутнього.

Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII визначає основні сфери національної безпеки України, а саме: державну, зовнішньополітичну, воєнну, економічну, екологічну, інформаційну та кіберсферу. При чому інформаційна сфера (сфера інформаційної безпеки) є невід'ємною складовою кожної із сфер національної безпеки й водночас важливою самостійною сферою забезпечення національної безпеки України [4].

Безпека держави має стійку залежність від інформаційної безпеки, значення якої постійно зростає із розвитком інформаційних технологій.

У Законі України «Про національну безпеку України» дається таке визначення: «державна безпека – захищеність державного суверенітету, територіальної цілісності і демократичного конституційного ладу та інших життєво важливих національних інтересів від реальних і потенційних загроз невоєнного характеру» [4]. Вона є важливою складовою національної безпеки України, її системних загальних та спеціальних заходів, які забезпечують стабільне існування держави як політичної організації всього суспільства.

Державна політика у сферах національної безпеки і оборони спрямована на захист: людини і громадянина – їхніх життя та 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 недоторканності; території, навколишнього природного середовища – від надзвичайних ситуацій; воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо.

Інформаційна безпека України – складова державної безпеки України, стан захищеності життєво важливих інтересів людини, суспільства та держави, при якому встановлюється ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, зокрема через координоване поширення недостовірної інформації, негативні наслідки застосування інформаційних технологій, несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека суспільства та держави характеризується ступенем їхньої захищеності, тобто усталеністю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, воєнної справи, суспільної свідомості тощо) стосовно небезпечних інформаційних впливів (дестабілізуючих, деструктивних, які ущемляють інтереси країни), причому як щодо впровадження, так і отримання інформації. Інформаційна безпека визначається спроможністю нейтралізувати ці впливи.

Загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [4].

Продовжуючи гібридну війну проти України, Російська Федерація системно застосовує політичні, економічні, інформаційно-психологічні, кібернетичні та воєнні засоби впливу. Посилюється наступальний потенціал угруповань збройних сил Російської Федерації, регулярно проводяться масштабні військові навчання поблизу державного кордону України, що свідчить про ймовірність загрози воєнного вторгнення. Зростає мілітаризація територій тимчасово окупованої Автономної Республіки Крим та міста Севастополя. Є загроза

з боку Російської Федерації вільному судноплавству у Чорному та Азовському морях, Керченській протоці.

Росія постійно здійснює деструктивний інформаційно-психологічний вплив як ззовні, так і всередині України; використовуючи суспільні суперечності, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність. Відсутність цілісної інформаційної політики держави, слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цих загроз.

Наступ на національну ідентичність українців є одним із проявів російської гібридної агресії. У наукових, політичних і громадських колах Російської Федерації цілком серйозно обговорюються ідеї штучності української мови, фальшивості української історії, фіктивності самої української нації.

Найрадикальнішою формою несприйняття української ідентичності є заперечення онтологічного статусу українства як такого.

Для ілюстрації можна навести лише деякі заголовки публікацій у російських ЗМІ та окремих видань: «Украинство как болезнь», «Украина – это не государство, это болезнь русского мира», «“Украйна” – это болезнь», «“Украинская” болезнь русской нации» тощо.

Однією з небезпечних форм заперечення української ідентичності є просування ідеології «русского мира» як транснаціонального поширення російської мови та культури. Особливість її застосування в Україні полягає в ототожненні людей російської культури або «російськомовних» із «російськими співвітчизниками» незалежно від їхньої національності.

За цих умов актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах із метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній

сфері, невизначеність стратегічного наративу, недостатній рівень медіакультури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [5].

Сприймаючи інформацію в будь-який спосіб, особа дає їй оцінку на основі лише їй відомих та часто неусвідомлених критеріїв. Аналітична оцінка інформації передбачає певний рівень професійних знань. Аналіз інформації з метою виявлення ознак інформаційних (психологічних) впливів, які можуть бути складовою спеціальної інформаційної операції, передбачає потребу охоплення величезних масивів інформації та, найчастіше, оброблення не їхнього тематичного змістового навантаження (економіка, культура, освіта), а контекстів, відтінків та прихованого і непомітного неозброєним оком змісту.

Аналіз напрямів інформаційно-психологічного деструктивного впливу, який здійснювала протягом 2021 року Російська Федерація на населення (громадян) України, що проживає на тимчасово окупованих територіях Донецької та Луганської областей, Автономної Республіки Крим, дає змогу так класифікувати загрози державній безпеці в інформаційній сфері:

1) дискредитація вищого військово-політичного керівництва України:

– звинувачення української влади в дестабілізації ситуації на тимчасово окупованій території Донецької та Луганської областей (далі – ТОТ ДЛО);

– звинувачення уряду України в продовженні «громадянської війни»;

– звинувачення української влади в підготовці повномасштабного наступу;

– звинувачення керівництва держави в підготовці диверсій на ТОТ ДЛО;

– звинувачення української влади в гальмуванні процесу виконання Мінських домовленостей;

– звинувачення уряду України в непрофесіоналізмі;

– звинувачення української влади у збитті малайзійського Boeing МН-17;

– звинувачення української влади в розправі над опозиційними до влади ЗМІ;

– дискредитація Збройних сил України;

– звинувачення Збройних сил України у нарощуванні військового потенціалу в зоні проведення операції Об'єднаних сил (далі – ООС) поблизу лінії розмежування з ТОТ ДЛО;

– звинувачення підрозділів, задіяних в операції ООС, у порушенні Мінських домовленостей;

– звинувачення військовослужбовців підрозділів Збройних сил України, задіяних в ООС, у непрофесіоналізмі та порушенні військової дисципліни;

– звинувачення підрозділів Збройних сил України в підготовці фейкових (постановочних) матеріалів у вигідному для керівництва України світлі та розхитуванні обстановки в ТОТ ДЛО та РФ;

– звинувачення в поширенні коронавірусної інфекції в підрозділах ЗС України;

2) провокування антидержавних настроїв серед населення України, популяризація серед населення проросійської ідеології через діяльність представників регіональних проросійських політичних сил;

3) нівелювання зусиль української влади щодо реалізації заходів, спрямованих на повернення тимчасово окупованої Автономної Республіки Крим до складу України:

– дискредитація діяльності української влади щодо створення формату «Кримська платформа», метою якої є деокупація захопленої території Автономної Республіки Крим;

– створення перешкод у налагодженні міжнародної співпраці між Україною та Турецькою Республікою, спрямованої на формування передумов для деокупації захопленої території Автономної Республіки Крим дипломатичним шляхом;

4) проведення пропагандистських заходів, спрямованих на формування та підтримання культурної ідентичності населення окупованої території Автономної Республіки Крим із населенням Російської Федерації:

– включення курортних міст окупованої території Автономної Республіки Крим до федеральної програми Російської Федерації «Формування курортного міського середовища», в межах якої передбачено фінансування розвитку туристичної інфраструктури курортних міст;

– поширення відомостей про обсяги іноземних інвестицій у регіональний розвиток окупованої території Автономної Республіки Крим;

– підготовка до проведення окупаційною владою незаконних виборів до місцевих органів влади на окупованій території Автономної Республіки Крим у так званий «Єдиний день голосування» у Російській Федерації;

– популяризація фактів виділення серед інших російської вакцини «Спутник V» для боротьби з поширенням коронавірусної інфекції на окупованій території Автономної Республіки Крим;

– проведення комплексу інформаційних і фінансових заходів, спрямованих на підготовку до відзначення «Дня перемоги»;

5) популяризація діяльності окупаційної влади на окупованій території Автономної Республіки Крим:

– популяризація діяльності, спрямованої на нарощування військової присутності на окупованій території Автономної Республіки Крим;

– формування упередженого ставлення населення окупованої території Автономної Республіки Крим до української влади, населення материкової частини України та кримськотатарської національної меншини шляхом створення видимості існування проблем на фоні міжнаціональних та міжрелігійних відносин і так званої профілактики терористичних та екстремістських проявів;

– формування у свідомості населення образу ефективної роботи окупаційної влади щодо вирішення проблеми забезпечення місцевого населення питною водою;

– популяризація заходів, спрямованих на розвиток альтернативних джерел забезпечення населення окупованої території Автономної Республіки Крим питною водою.

Узагальнювальним напрямом є деструктивний психологічний вплив на місцеве населення окупованих територій із метою: підтримання почуття ненависті, сформованого з використанням гучних інформаційних приводів (щодо обстрілів, поранень чи смертей, соціальних негараздів), підтримання політичних і воєнних рішень керівництва Російської Федерації на міжнародному рівні з боку населення Росії та підконтрольних російській владі територій; нівелювання та викривлення рішень воєнно-політичного керівництва України, порушення діяльності органів військового управління; зниження морально-психологічного стану особового складу Збройних сил та інших силових структур України; деморалізації населення України, формування у громадян Росії та України викривленого «медіабачення» подій, що відбуваються, а не їхніх дійсних причин і наслідків. При цьому місцеве населення окупованих територій отримує виключно дозовану, неповну та викривлену інформацію через інформаційні канали російського інформаційно-психологічного впливу.

Зазначені напрями інформаційно-психологічного впливу, який здійснює Російська Федерація на ТОТ ДЛО, окупованій території Автономної Республіки Крим, реалізуються через майже повний спектр каналів комунікацій, до яких передусім належать: друковані ЗМІ (газети, журнали тощо), електронні ЗМІ (телебачення, радіомовлення), інтернет-ЗМІ та соціальні мережі.

Проти України ведеться інформаційна війна з боку Росії, що негативно відбивається на формуванні її міжнародного іміджу.

Однією з найактивніших зон «бойових дій» є інформаційні ресурси та соціально орієнтовані мережі, які використовуються Російською Федерацією й підконтрольними їй самопроголошеними анклавами «ЛНР-ДНР» для здійснення масштабних кампаній інформаційно-психологічного впливу як на мешканців тимчасово окупованих територій Сходу України, так і на жителів інших регіонів держави.

Можна визначити такі внутрішні загрози інформаційній безпеці України:

– використання загальнодоступних і соціально орієнтованих ресурсів мережі «Інтернет» для здійснення протиправної діяльності, прихованої під виглядом сепаратизму, екстремізму, фінансування тероризму, що ніби не пов’язана з діяльністю країни-агресора;

– залучення мешканців тимчасово окупованих територій до лав незаконних збройних формувань самопроголошених «ДНР/ЛНР» задля власного збагачення у зв’язку з низьким рівнем матеріально-технічного, грошового й фінансового забезпечення та їхня співпраця з представниками спецслужб РФ із поширення деструктивного контенту у мережі «Інтернет», спрямованого на дестабілізацію ситуації в країні та за її межами;

– посягання на інформаційну безпеку країни та за її межами у зв’язку із зосередженням сил і засобів електронного інформаційного простору на території країни-агресора.

До основних зовнішніх загроз належать:

– використання спецслужбами РФ найпопулярніших серед користувачів мережі «Інтернет» звільнених і тимчасово окупованих територій України соціальних мереж «Вконтакте» та «Одноклассники» для проведення деструктивної діяльності на шкоду інформаційній безпеці держави, залучення громадян України до незаконних збройних формувань так званих «ДНР/ЛНР», пропагування ідей «русского мира», історичного повернення РФ до моделі СРСР;

– використання спецслужбами РФ соціальних ресурсів мережі «Інтернет» із метою поширення закликів до повалення конституційного ладу силовим шляхом, зміни меж території України, фінансової та матеріальної допомоги самопроголошеним республікам, здійснення антиконституційних дій, спрямованих на дестабілізацію ситуації в Україні;

– проведення спецслужбами РФ масштабних зовнішніх інформаційних впливів на шкоду національним інтересам України шляхом розповсюдження дезінформації стосовно діяльності військовослужбовців ЗС України в зоні ООС у проросійських ЗМІ та підконтрольних ресурсах;

– використання спецслужбами РФ соціальних мереж із метою збирання та аналізу інформації стосовно громадян України у зв'язку з відсутністю вітчизняних аналогів соціальних мереж.

Аналіз інформаційних загроз дає змогу виділити головні напрями дій російських пропагандистів в інформаційній війні проти України, а саме:

– сіяння страху та паніки серед широких верств населення;

– формування громадської думки щодо конкретних тактичних дій РФ і її стратегії в цілому;

– спонукання населення та політичних лідерів України до саморуйнівних дій;

– поширення дезінформації;

– заклики до саботування розпоряджень української влади;

– підрив бойового духу українських бійців і населення;

– дискредитація політичного та військового керівництва України;

– провокування конфліктів в Україні та у середовищі її політичних сил;

– провокування користувачів соціальних мереж із метою збирання інформації;

– апелювання до світової спільноти для виправдання російської агресії проти України та дискредитації України;

– вербування «живої сили» для участі в конфлікті на Донбасі на боці сепаратистів;

– використання постів у соціальних мережах як джерела для подальшої легалізації дезінформації у ЗМІ.

Очевидно, що чітке розуміння технологій ведення гібридної війни є необхідною складовою воєнної майстерності будь-якої держави, яка прагне перемоги в майбутніх протистояннях, котрі мають дедалі більше виражену інформаційно-психологічну домінанту. Саме тому аналіз дій

російських пропагандистів в інформаційній сфері та розроблення ефективних контрзаходів на майбутнє є життєво важливими кроками для захисту безпеки української державності.

Серед негативних чинників, які ускладнюють протидію веденню інформаційної війни проти України, можна виділити такі:

– відсутність чітко сформованих політико-правових механізмів державного управління інформаційно-психологічною безпекою України;

– відсутність концепції щодо ролі України у світовій інформаційній війні та нормативно-правових документів, що визначають засади участі України в інформаційній війні;

– відсутність комплексної програми захисту населення країни від деструктивних впливів інформаційної війни, масової просвіти населення, включно з дітьми шкільного віку, студентською молоддю, пенсіонерами.

Висновки. У сучасних умовах суттєво змінився характер збройної боротьби, яка набула ознак гібридної війни. Акценти збройної боротьби зміщуються в бік практичної реалізації інформаційних технологій. Дедалі більшого значення в досягненні політичних і воєнних цілей набувають інформаційно-психологічні операції, акції та дії.

Недооцінювання можливостей інформаційно-психологічного впливу, заходів протидії впливам та неврахування особливостей конкретної території можуть стати фатальними під час подальшого загострення воєнно-політичної обстановки навколо України. В інформаційній агресії проти Української держави тепер основним є спрямування на те, щоб будь-яким шляхом ослабити та розколоти її зсередини, штучно створюючи та загострюючи вже існуючі політичні, соціально-економічні, регіональні, етнічні й інші суперечності. Зокрема, посилюються інформаційні кампанії, спрямовані на дискредитацію чинної української влади, інституцій Президента України, уряду, силових структур, що забезпечують державну безпеку держави.

Результати аналізу інформаційно-психологічного впливу, що здійснює Російська Федерація на населення України, свідчать про використання таких його форм і способів, як: маніпулювання суспільною свідомістю та політичною орієнтацією соціальних груп населення країни з метою створення політичної напруженості та контрольованого хаосу; створення атмосфери негативного ставлення до культурної спадщини, втрати національної свідомості; дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби; зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень; дезінформування населення стосовно роботи державних органів, підрив їхнього авторитету, дискредитація органів управління; провокування соціальних, політичних, національних і релігійних сутичок; ініціювання страйків, масового безладу й інших акцій економічного протесту; утруднення прийняття органами управління важливих рішень, тиск під час їх

прийняття; підрив міжнародного авторитету держави, її співробітництва з іншими країнами. Застосування таких форм і способів впливу спричиняє загрози інформаційній сфері, що загалом впливає на державну безпеку. Тому важливим завданням усіх державних, громадських, наукових, експертних, журналістських інституцій має стати розроблення ефективних заходів щодо нейтралізації інформаційної агресивної діяльності Російської Федерації проти України та протидія її подальшому розгортанню. Ураховуючи виклики, що постали перед Україною, потрібне також вжиття ефективних організаційно-правових заходів із метою модернізації всієї системи інформаційної та державної безпеки країни.

Отже, у процесі дотримання курсу стратегії національної безпеки України з урахуванням основних тенденцій розвитку інформаційного суспільства набуває особливого значення розроблення актуальних напрямів організації забезпечення інформаційної безпеки держави, прискорення розроблення та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами.

Список використаних джерел

1. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. та ін. Інформаційна безпека : підручник / під ред. В. В. Остроухова. Київ : Ліра-К, 2021. 412 с.

2. Hoffman Frank G. Hybrid Warfare and Challenges. *Joint Force Quarterly* (JFQ). 2009. Issue 52, Forth Quarter. P. 34–39.

3. Libicki M. C. What Information Architecture for Defence / New Challenges, New Tools for Decissiommaking. RAND Corporation. 2003. 317 p.

4. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII.

5. Про рішення Ради національної безпеки і оборони України» від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017.

Аннотация. В статье исследованы направления информационно-психологического воздействия, которое Российская Федерация оказывает на временно оккупированных территориях Донецкой и Луганской областей и в АР Крым, как реальные угрозы невоенного характера государственной безопасности Украины. Проводится анализ основных угроз в информационной сфере, направленных на дискредитацию высшего военно-политического руководства государства, провоцирование антигосударственных

Abstract. The article examines the ways of applying methods of information and psychological influence by the Russian Federation (RF) on the temporarily occupied territories of Donetsk and Luhansk regions and in the Autonomous Republic of Crimea which pose real non-military threats to the state security of Ukraine. There analyzed major threats in the information sphere aimed at discrediting the top military and political leadership of the state, provoking anti-state sentiment in Ukraine and conducting information operations to mold the cultural

настроений в Украине и проведение пропагандистских мероприятий по формированию культурной идентичности населения оккупированной территории АР Крым с населением России. Раскрыты намерения РФ относительно деструктивного информационно-психологического воздействия как извне, так и внутри Украины, направленные на то, чтобы, искусственно создавая и обостряя существующие политические, социально-экономические, этнические и другие противоречия, любым путем ослабить и расколоть страну изнутри.

Ключевые слова: государственная безопасность, информационные угрозы, гибридная война, информационная война, информационно-психологическое воздействие.

oneness of the population on the occupied territory of Crimea and the population of Russia. There revealed Russia's intentions regarding destructive methods of information and psychological influence both from outside and inside Ukraine, aimed at weakening and splitting the country from within through engineering and exacerbating existing political, socio-economic, ethnic and other contradictions.

Key words: state security, information threats, hybrid war, information war, information-psychological influence.

УДК 32.019.51
DOI

ХОДАНОВИЧ Віталій Олександрович

ПРОТИДІЯ ІНФОРМАЦІЙНИМ ВПЛИВАМ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ: НАЦІОНАЛЬНИЙ ДОСВІД

Постановка проблеми. Інформаційна кампанія, яку розгорнула Російська Федерація (далі – РФ) останніми роками, має всі ознаки чітко спланованої багаторівневої агресії проти основ міжнародного порядку. Через своє геополітичне положення Україна опинилася в епіцентрі зони ворожого впливу й стала для країни-агресора «полігоном» для відпрацьовування нових технологій інформаційного впливу, переважно деструктивного, на українських громадян, суспільство, органи влади й управління. Від початку гібридної агресії у 2014 році вітчизняний інформаційний простір щоденно зазнавав втручань різного характеру з російського боку: від тенденційного висвітлення російськими ЗМІ подій в Україні й до відвертої неправди, яка виходила з вуст представників влади РФ, на-