Александр Михайлович Богданов, доктор технических наук, профессор, заведующий кафедрой, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.
E-mail: a_m_bogdanov@inbox.ru.

Олександр Михайлович Богданов, доктор технічних наук, професор, завідувач кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

Aleksander Bohdanov, doctor of technical sciences, professor, head of department, Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.

УДК 316.625

ВАЛЕНТИН ПЕТРИК,
ЮРІЙ КАНАРСЬКИЙ

МЕТОДИ ГІБРИДНОЇ ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ. НАПРЯМИ ПРОТИДІЇ

Розкриваються методи ведення агресії Російською Федерацію на території України в контексті повномасштабної «гібридної війни». Розглядаються та аналізуються напрями протидії цим загрозам. У висновках надаються пропозиції щодо вироблення загальних підходів до напрямів протидії «гібридним загрозам».

Ключові слова: гібридна війна, агресія, інформаційна безпека, інформаційно-психологічний вплив.

Глобальний розвиток інформаційних технологій та засобів масової комунікації дав початок появі нових технологій впливу на вирішення різноманітних конфліктів. Розвиток інформаційного суспільства дозволяє використовувати для вирішення політичних чи соціокультурних завдань можливості прихованого впливу на підсвідомість людей та масштабного маніпулювання суспільною думкою. Це призвело до появи нових форм і методів, завдяки яким провідні держави намагаються досягти своїх зовнішньополітичних цілей і владнати міждержавні розбіжності. На зміну суто військового аспекту війни приходять так звані «гібридні війни». Новий спосіб має суто прихований характер і використовується для досягнення цілей у політичній, економічній, інформаційній і соціальній сфері. Суть використання даного методу полягає в зміщенні центру зусиль з фізичного знищення супротивника в рамках масштабної війни до вживання засобів «м'якої сили» проти країни-супротивника з метою дезінтеграції та зміни її керівництва, включення до сфери свого впливу.

Актуальність теми є надзвичайно важливою в умовах неоголошеної війни проти нашої держави. Чітке визначення методів, які використовує Російська Федерація (РФ), дозволить побудувати надійну систему протидії окупантам та звільнити тимчасово окуповані території.

РФ застосувала проти України концепцію «гібридної війни», яка є унікальною з структурно-функціонального погляду, а за змістом – асиметричною. Характер нового типу протистояння спочатку продемонструвала анексія Російською Федерацією Криму навесні 2014 року, а потім – підтримка місцевих радикальних елементів та повномасштабне вторгнення російських підрозділів до східних областей нашої держави.

Аналіз останніх досліджень і публікацій. Визначення поняття «гібридна війна» відсутнє в міжнародно-правових документах. Ряд дослідників сучасності, для характеристики сучасних воєнних конфліктів, використовують саме термін «гібридна війна», однак систематизованого викладу причин виникнення, сутності, характеру і особливостей ведення таких війн в нашій державі, на жаль, немає. Тема «гібридних воєн» стала надзвичайно актуальною і широко висвітлюється в засобах масової інформації (ЗМІ). А також є предметом спеціальних досліджень. Такі дослідження проводились відомими американськими експертами світового рівня, як Френк Гофман [7], Деніел Ласіка, Джордж Девіс та Девіз Кілкаллен [4], а також нідерландцем Френком ван Каппеном [5].

Метою статті є з'ясування методів гібридної війни РФ проти України, визначення можливих напрямів протидії агресії.

Досягнення мети передбачає виконання таких **завдань**:

– охарактеризувати поняття «гібридна війна», розкриття її історичного аспекту, змісту та особливостей;

– розкрити методи, які використовує держава-агресор проти України;

– встановити необхідність забезпечення повної довіри військовослужбовців і населення країни до силових структур держави;

– визначити рекомендації щодо переосмислення загальних підходів до підтримання національної безпеки України.

Гібридна війна – війна з поєднанням принципово різних типів і способів ведення війни, які скоординовано задля досягнення спільних цілей.

Характерними елементами гібридної війни є використання:

– класичних прийомів ведення війни (Збройні Сили, техніка, уніформа);

– нерегулярних збройних формувань (повстанці, терористи, партизани);

– інформаційної, кібернетичної та економічної сфери.

До особливостей «гібридних воєн» відносяться: початок агресії без офіційного оголошення війни, приховування країною-агресором своєї участі у конфлікті; використання нерегулярних збройних формувань; нехтування агресором міжнародних норм ведення бойових дій, домовленостей та угод; комплекс заходів політичного та економічного тиску; широкий та розгалужений апарат пропаганди та контрпропаганди з різноманітних методів інформаційно-психологічного впливу (інспірування ЗМІ, дискредитація органів влади противника, диверсифікація громадської думки, маніпулювання на високому політичному рівні, побудова агентури впливу, проведення спеціальних інформаційних операцій та акцій інформаційно-психологічного впливу, дезінформування, способи подання інформації та ін.); протистояння у кіберпросторі. Класичні війни стали вкрай небезпечними через наявність нових потужних видів зброї. Тому застосування саме «гібридної війни» цілком виправдане. Насамперед, це дозволяє уникнути масових жертв серед мирного населення, появі масштабних потоків біженців, руйнації транспортної та промислової інфраструктури. Використання даного методу дозволяє агресору применшити свою роль у розв'язання конфліктів задля уникнення санкцій з боку інших країни та міжнародних організацій, а також для недопущення втрати свого авторитету на міжнародній арені.

«Гібридна війна» дозволяє встановити свій контроль над об'єктами агресії, інтегрувати їх до своїх політичних та економічних систем без надмірних збитків, що можуть зашкодити досягненню економічних та геополітичних інтересів.

Однак, початок ведення «гібридної війни» достатньо виправданий крок, який потребує від агресора ряд вимог. Насамперед, держава повинна мати сильну і дієву владу, яка зможе зберегти своє ім'я в очах громадськості, згуртувати її навколо «ворога» та вільно пропагувати національні ідеї. Країна-агресор повинна володіти значним потенціалом та вагомою перевагою у військовій, економічній та інформаційній сферах, для здійснення комплексного економічного та морального-психологічного тиску на об'єкт агресії.

Важливим елементом успішного ведення війни цим методом передбачає наявність ряду недоліків у об'єкта агресії: слабкість влади, післяреволюційний стан, розкол у суспільстві,

деградація економіки, деморалізація силових структур, внутрішні протиріччя. Країна-агресор повинна бути готова до відсічі та підтримки об'єкта світовою спільнотою.

Відомими «гібридними війнами» сучасності є:

– Російсько-грузинська війна 2008 року – чіткий приклад застосування РФ комплексу інформаційного, економічного, кібернетичного та військового аспекту війни.

– Конфлікт Лівану та Ізраїлю 2006 року, в якому Хізбалла боролася із військово сильнішим противником Ізраїлем із використанням класичних військових дій, нерегулярних збройних формувань та інформаційних методів ведення війни, завдавши Ізраїлю стратегічної поразки.

– Збройна агресія РФ проти України стала довгостроковим чинником впливу на політичну, економічну, військову та соціальну сфери нашої держави. Внаслідок дій агресора впродовж 2014 року деформовано систему глобальної та регіональної безпеки, а також чинну систему міжнародного права. Майже всі міжнародні гарантії безпеки для України виявились недієздатними в умовах, коли агресором виступив один із гарантів – Російська Федерація.

Військова агресія РФ проти України являє собою якісно новий підхід ведення подібних кампаній, ключовим значенням у яких с психологічна обробка супротивника. Цьому чиннику кремлівські планувальники приділяють ледь не найголовнішу увагу, адже правильно спланована акція психологічного тиску на місцеве населення позбавляє від потреби відкритого використання збройних сил, обмежуючись лише заздалегідь підготовленими та нечисленними диверсійними підрозділами. Застосування жорсткої сили іміджевої дипломатії на підготовленому геопросторі дозволяє наразі не лише проводити активну приховану інтервенцію на Сході України у Донецькій та Луганській областях, а й відчужити на свою користь окремі території, зокрема Крим, таким чином змінюючи баланс сил в регіоні на свою користь. Серед засобів психологічного впливу варто розділяти такі, що спрямовані на зовнішнього користувача, на внутрішню російську аудиторію та на населення територій, де відбувається військова агресія.

Проведення аналізу «гібридної війни», яку здійснює РФ у межах довготривалої інформаційної кампанії проти України, дає змогу виокремити основні напрями та методи здійснення заходів, що зачіпають основні сфери національної безпеки України та становлять загрозу національним інтересам у:

1) зовнішньополітичній сфері – перешкоджання євроінтеграції України у спосіб формування упередженого ставлення світової спільноти до української влади, поширення недостовірної, неповної та викривленої інформації про Україну, висловлювання недоцільності євроінтеграції України;

2) внутрішньополітичній сфері – формування образу ворога – українця серед російськомовних громадян України та росіян, а також спроби формування упередженого ставлення світової спільноти до патріотичних рухів в Україні у спосіб поширення викривленої, недостовірної та упередженої інформації щодо становища в Україні росіян та інших етнічних груп, статусу російської мови;

3) сфері державної безпеки – посягання на державний суверенітет і територіальну цілісність України у спосіб порушення питань про приналежність АР Крим (відбувалося впродовж усіх років незалежності), наразі – про доцільність федералізації України та формування «Новоросії» на Сході України;

4) воєнній сфері – витіснення України зі світового ринку зброї у спосіб поширення недостовірної інформації щодо участі України у незаконному розповсюдженні зброї, оборонних технологій та низької якості української військової техніки тощо; на сьогодні – формування негативної громадської думки серед української та світової спільноти про дії Збройних сил України на Сході України у спосіб поширення недостовірної інформації про застосування військовими зброї проти мирного населення;

5) економічній сфері – витіснення України зі світового та російського ринків у спосіб розповсюдження недостовірної інформації про якість окремих груп товарів чи низький рівень наукових розробок у певних галузях; перешкоджання реалізації та дискредитація

здійснених заходів Україною щодо зниження енергетичної залежності від РФ, зокрема завдяки маніпулюванню інформацією щодо цін на енергоносії;

6) соціальній та гуманітарній сферах – протидія переосмисленню власної історичної спадщини, нівелювання українських культурних цінностей і формування проросійських настроїв у суспільстві у спосіб насаджування міфу про спільний «русский мир», заперечення існування окремої від росіян української нації з власною мовою, культурою та історією, ставлення під сумнів права української нації на самовизначення й утворення національної держави.

Проте якщо донедавна негативні інформаційно-психологічні впливи використовувалися РФ як допоміжний засіб для досягнення економічних, політичних чи інших зисків, то наразі, в умовах неоголошеної «гібридної» війни, яку веде РФ проти нашої держави, інформаційна зброя використовується так само, як і справжня зброя. У цій війні нового типу ставка робиться на формування «правильного» з точки зору агресора образу жертви в цій війні та використання цивільного населення для нагнітання масової істерії та спротиву законній владі. Саме тому для досягнення своєї мети в інформаційній війні проти нашої держави РФ використовує весь наявний арсенал традиційних і сучасних методів, засобів «гібридної війни».

До методів виливу варто віднести використання пропаганди, агітації, тенденційної інформації, напівправди та відвертої неправди («фейку»). Прикладами розміщення напівправди є інформаційні повідомлення під час анексії Криму, коли російські ЗМІ заявляли про масовий перехід українських силовиків на бік Російської Федерації або про добровільну здачу військових частин, складів, зброї, інших військових об'єктів російським військовим. Хоча таких випадків було значно менше. Як приклад розповсюдження тенденційної інформації можна згадати постійне цитування сайтами, пов'язаними із російськими спеціальними службами, таких осіб, як П. Робертс (працівник уряд) США за часів Р. Рейгана), Ф. Канінгем (екс-журналіст The Mirror, Irish Times та Inde pendent), В. Медсен та ін. Здебільшого вони дотримуються виразно антиамериканської лінії поведінки, а багато з них співпрацюють із дослідниками проблем «світової змови».

До засобів впливу, які використовує РФ в інформаційній боротьбі з Україною, відносяться медійні ресурси: телебачення, радіо, друковані ЗМІ і дедалі частіше – Інтернет-ЗМІ, а також кінопродукція та книги.

Зокрема, найпоширенішим засобом, який використовувала РФ в інформаційній війні з Україною, донедавна було телебачення. Цьому сприяли як соціокультурний в поєднанні з мовним фактором (російську мову розуміють понад 90 % населення України), так і той факт, що в результаті цілеспрямованої роботи російської сторони в кабельних мережах України здійснювали ретрансляцію «Первый канал», «НТВ-мир», «Россия 24», «РТР-Планета», «Звезда» та інші, які не лише подавали неправдиву інформацію про події в Україні, а й здійснювали спроби розпалювати міжнаціональну ворожнечу, закликали до федералізації та територіального поділу України, використовували деструктивні антиукраїнські гасла. Іншим за значенням засобом впливу на широкі маси населення в нашій державі з боку РФ є преса, зокрема газети. Цей чинник використовувався повною мірою, адже в інформаційній війні аналітичний чи розважальний матеріал може мати вплив на аудиторію не менший, ніж пряма політична реклама. В Україні видавалися загальнонаціональні українські версії російських видань, поширювались матеріали, що пропагували російську доктрину спрямовану на розвал України, закликали до повалення конституційного ладу, продовження та поглиблення агресії, розпалювання війни, ворожнечі, ненависті тощо. Деякі з них на сьогодні вже закриті, зокрема «Известия», «Коммерсантъ», проте й інші потребують прискіпливої перевірки.

Також вагомим інструментом впливу РФ на українську аудиторію є радіомовлення. Зокрема, ще донедавна в українському радіо-просторі на хвилях «Радіо Ера» здійснювала своє мовлення радіостанція «Голос России», відома своєю антиукраїнською позицією.

В інформаційно-психологічній боротьбі РФ широко використовуй й Інтернет. При цьому застосовуються як наявні, так і спеціально створені Інтернет-ресурси, більшість із

яких розташована за межами України на закордонних серверах, зберігаючи лише приналежність до українського сегмента глобальної мережі. Такі Інтернет-видання («Новый регион», «Регнум». «Провокация» та ін.), популяризуючи серед української аудиторії ідеї сепаратизму, продовжують нести загрозу територіальній цілісності нашої держави.

Водночас вагомим ресурсом «гібридної» війни, яку здійснює РФ проти України на сучасному етапі, стали соціальні мережі. Так, експерти ще з початку Майдану в Києві помітили, що у соцмережах РФ, а також країн-сусідів (Польщі. Румунії, Угорщини, Австрії) почала з'являтися велика кількість негативних коментарів про Україну. Причому їх аналіз вказував на те, що така акція готувалася заздалегідь, адже під час написання коментарів у Польщі використовували молодіжний сленг, в Австрії – віденський діалект. Польські журналісти не полінувалися знайти, звідки розсилалися коментарі, і виявили, що це було зроблено з російських IP-адрес.

Важливим інструментом інформаційного впливу РФ на Україну є книжкова продукція антиукраїнського змісту, в якій заперечується існування окремої від росіян української нації з власною мовою, культурою та історією, ставиться під сумнів право української нації на самовизначення й утворення національної держави, а незалежність України характеризується як сепаратизм, розпалюються міжнаціональна та релігійна ворожнеча, у свідомості громадян РФ, а також російськомовних громадян України формується образ ворога – українця. Варто зауважити, що такі книги почали з'являтися ще у 2000-х роках, проте масово почали публікуватися цього року.

Одним із вагомих інструментів антиукраїнської пропаганди РФ є кінопродукція - численні серіали та фільми, які донедавна масово транслювалися загальнонаціональними українськими телеканалами. У такій кінопродукції українців показують як негативних персонажів, перекручують історичні факти про Україну, звеличують дії російських військових і силовиків, зокрема під час окупації українських земель тощо.

Окремим інструментом інформаційного впливу РФ є так звані науково-дослідні центри, що мають свої представництва в колишніх радянських республіках і, за прикладом європейських грантових організацій, набули статусу автономних некомерційних організацій («Институт стран СНГ», «Международный институт политической экспертизы», «Русский институт», «Институт национальных стратегий», «Кавказский институт демократии» та «Институт евразийских исследований»), спеціально-створені молодіжні «недержавні» організації (Кримський «Прорив», закарпатський Русинський «Прорив», «Євразійський союз молоді», та фонди («Русский мир»).

Нещодавно в мережі було викрито діяльність так званого «Агентства Інтернет-досліджень», котре перебуває на «бюджетному забезпеченні» Росії. Що характерно, штат цієї організації налічує сотні співробітників. У ньому є фахівці з дизайну й IT-технологій, блогери й коментатори, аналітики й перекладачі, відділи з моніторингу ЗМІ й соцмереж. Саме там народжується інформація, яка викладається на сайтах в Інтернеті та оприлюднюється на російських телеканалах, передусім таких, як «ОРТ», «Россия 1, «Россия 24», «НТВ», «РТР Планета», телеканал Міністерства оборони РФ «Звезда». При цьому російська пропаганда розрахована на три категорії споживачів: самих росіян, Україну й весь інший світ.

Таким чином, аналіз негативних інформаційно-психологічних впливів, які здійснює РФ на нашу державу, вказує на їх плановість, системність і координованість на найвищому державному рівні.

Натхненна практично безкровним захопленням і «тихою» окупацією Автономної Республіки Крим, Росія зухвало продовжує політику подальшої реалізації агресивних намірів стосовно України, спрямованих на порушення її національного суверенітету й територіальної цілісності. Упроваджуючи тактику створення обстановки нестабільності в регіонах на Сході України, Росія безпосередньо не перетинає кордон своїми збройними силами. Водночас російські регулярні військові формування під виглядом відпрацювання «планових» заходів оперативної, бойової підготовки постійно перебувають у безпосередній

близькості до кордону з Україною, маючи на меті створення постійної напруженості в цих регіонах. Визначені виконавці виконують завдання, які Росія (як держава) в рамках міжнародного права робити не може, тому використовує методи «гібридної війни».

Висновки. Надаючи загальну характеристику проявів нових форм сучасних воєнних конфліктів, особливостей їх застосування в Україні, варто виробити загальні підходи до напрямів протидії «гібридним загрозам» І в цьому плані слід виокремити деякі ключові моменти.

По-перше, сьогодні абсолютно очевидно, що досягнення перемоги у війнах такого типу неможливе без адаптації чинної Воєнної доктрини України до нових реалій, без оновлення й удосконалення Стратегії національної безпеки України та інших базових документів, які мають бути скориговані з урахуванням нинішньої воєнної та суспільно-політичної ситуації в країні. Треба усвідомити, що в «гібридних війнах» традиційні, конвенціональні методи ведення воєнних дій не завжди ефективні, що війни такого типу, як правило, ведуться тривалий час, що супротивник намагатиметься максимально розширяти географію конфлікту і утягуванням у нього дедалі більшої кількості населення.

По-друге, важливим завданням, яке необхідно вирішувати в умовах «гібридної війни», є забезпечення повної довіри військовослужбовців і населення країни до силових структур держави. Затяжний характер «гібридних конфліктів» може викликати певне невдоволення та критику як з боку особового складу силових формувань, так і з боку громадян країни, політиків, засобів масової інформації на адресу військового командування, звинувачення їх у невмілому плануванні, організації управління тощо. Не можна забувати і про одну з важливих складових розуміння сутності «гібридної загрози», зокрема усвідомлення факту ігнорування супротивником моральних та етичних обмежень під час ведення операцій.

Воєнно-політична обстановка, що склалася сьогодні довкола держави, вимагає повного переосмислення загальних підходів до підтримання національної безпеки України, кардинальної перебудови всього сектора безпеки та оборони держави з метою приведення у відповідність до нових викликів та загроз. Для вирішення цього важливого стратегічного завдання необхідно вжити низку невідкладних заходів:

1. Переглянути базові принципи побудови системи національної безпеки держави з метою пошуку та приєднання України до надійної системи колективної безпеки, яка б гарантовано захищала незалежність, суверенітет і територіальну цілісність нашої держави.
2. Реформувати Збройні Сили та інші силові структури України до ведення воєнних дій у нових умовах сучасного протистояння з агресором, враховуючи досвід АТО на Сході країни у протистоянні «гібридній війні».
3. Створити ефективну систему забезпечення інформаційної та кібернетичної безпеки держави як інструменту протидії зовнішнім інформаційним загрозам та інформаційної підтримки зовнішньої і внутрішньої політики України.

Внаслідок розвитку глобального інформаційного простору інформаційне протиборство в контексті ведення «гібридної війни» утверджується як основний вид боротьби за сфери впливу, ресурси, влади, «мізки» людей та інші інтереси. Поширення і використання інформаційних технологій, ресурсів, продукції та послуг торкається інтересів усієї міжнародної спільноти і лише широке міжнародне співробітництво та міжнародно-правове регулювання здатне забезпечити їх безпечне використання в інтересах кожної держави. Міжнародне співробітництво в галузі інформаційної безпеки має будуватися на основі поєднання національних інтересів в даній сфері, чітких уявлень про реальні та потенційні виклики та загрози, методи, засоби і напрями їх запобігання, виявлення, припинення і протидії, а також належного правового забезпечення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Черниш В. Що відбувається на Сході України. Ще раз про термінологію. [Електронний ресурс] / В. Черниш. – Режим доступу : http://osvita.mediasapiens.ua/media_law/

law/scho_vidbuvaetsya_na_skhodi_ukraini_sche_raz_pro_terminologiyu. – Дата доступу : лютий 2015. – Назва з екрану.

2. Кравченко В. Психологічні аспекти «гібридної війни» Росії в Україні [Електронний ресурс] / В. Кравченко. – Режим доступу : https://www.academia.edu/7229745. – Дата доступу : лютий 2015. – Назва з екрану.

3. Губарев В. А. Особенности моделирования сложного коалиционного конфликта в условиях противодействия / В. А. Губарев, Ю. Л. Козирацкий // Радиотехника. – 1997. – № 6. – С. 9-14.

4. Kilcullen D. The Accidental Guerrilla : Fighting Small Wars in the Midst of a Big One / D. Kilcullen. – Oxford : Oxford University Press, 2011. – 384 p. – ISBN 978-0199754090.

5. Соціально-правові основи інформаційної безпеки : навч. посіб. / [В. М. Петрик, А. М. Кузьменко, В. В. Остроухов та ін.]; за ред В.В Остроухова. – К. : Росава, 2007. – 496 с. – ISBN 966-96-220-5-0.

6. Слиттченко В. И. Войны шестого поколения : оружие и военное искусство будущего / В. И. Слиттченко. – М. : Вече, 2002. – 384 с.

7. Хоффман Ф. Гибридные угрозы [Электронный ресурс] / Ф. Хоффман. – Режим доступа : https://www.academia.edu/7229745. – Дата доступа : март 2015. – Название с экрана.

Стаття надійшла до редакції 18.03.2015.

REFERENCE

1. Chernysh, V. (2014), What is happening in eastern Ukraine. Once again about terminology [*Shcho vidbuvaietsia na Skhodi Ukrainy. Shche raz pro terminolohiiu*], available at : http://osvita.mediasapiens.ua/media_law/law/scho_vidbuvaetsya_na_skhodi_ukraini_sche_raz_pro_terminologiyu (accessed 22 February 2015).

2. Kravchenko, V. (2015), *Psychological aspects of Russian "hybrid war" in Ukraine* [*Psykholohichni aspekty «hibrydnoi viiny» Rosii v Ukraini*], available at : https://www.academia.edu/7229745 (accessed 27 February 2015).

3. Hubarev, V. A., Kozyratskyi, Yu. L. (1997), *Features of modeling a complex coalition conflict in the face of opposition* [*Osobennosti modelirovaniia slozhnogo koalitcionnogo konflikta v usloviiakh protivodeistviia*], Radiotekhnika, No 6, pp. 9-14.

4. Kilcullen, D. (2011), *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*, Oxford University Press, Oxford, 384 p., ISBN 978-0199754090.

5. Petryk, V. M., Kuzmenko, A. M., Ostroukhov V. V. and other (2007), *Social and Legal Principles of Information Security : tutorial* [*Sotsialno-pravovi osnovy informatsiinoi bezpeky : navch. posib.*], Rosava, Kiev, 496 p., ISBN 966-96-220-5-0.

6. Slittchenko, V. I. (2002), *War of the sixth generation: weapons and military art of the future* [*Voiny shestogo pokoleniia: oruzhie i voennoe iskusstvo budushchego*], Veche, Moskow, 384 p.

7. Khoffman, F. (2013), *Hybrid threat* [*Gibridnye ugrozy*], available at : https://www.academia.edu/7229745 (accessed 05 March 2015).

ВАЛЕНТИН ПЕТРИК,
ЮРИЙ КАНАРСКИЙ

МЕТОДЫ ГИБРИДНОЙ ВОЙНЫ РОССИИ ПРОТИВ УКРАИНЫ. НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ

Раскрываются методы ведения агрессии Российской Федерацией на территории Украины в контексте полномасштабной «гибридной войны». Рассматриваются и анализируются направления по противодействию этим угрозам. В выводах показано предложения по выработке общих подходов к направлениям противодействия «гибридным угрозам»

Ключевые слова: гибридная война, агрессия, информационная безопасность, информационно-психологическое воздействие.

VALENTYN PETRYK,
YURII KANARSKYI

METHODS HYBRID WAR OF RUSSIA AGAINST UKRAINE. AREAS COUNTER

Disclosed methods of aggression by the Russian Federation in Ukraine in the context of a full-scale «hybrid war». Considered and analysed trends to counter these threats. The findings show proposals for the development of common approaches to areas of combating «hybrid threats».

Key words: hybrid war, aggression, information security, information and psychological impact.

Валентин Михайлович Петрик, кандидат наук з державного управління, доцент, доцент кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.
E-mail: vmp2012@rambler.ru.

Юрій Володимирович Канарський, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.
E-mail: kanarskiy_yuriy@ukr.net.

Валентин Михайлович Петрик, кандидат наук с государственного управления, доцент, доцент кафедры, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Юрий Владимирович Канарский, курсант, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Valentyn Petryk, candidate of state-owned management, associate professor, associate professor of the department, Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.

Yurii Kanarskyi, cadet, Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.