ISSN 2076-1546

УДК 341.123 (045) DOI: 10.46972/2076-1546.2019.17.05

С. А. Запорожець

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Статтю присвячено дослідженню інформаційної безпеки України в умовах гібридної війни, протистоянню гібридним загрозам з боку Російської Федерації, а також пріоритетним напрямам ефективного забезпечення інформаційної безпеки в нашій державі. Аналіз даної проблеми показує, що сучасний стан системи інформаційної безпеки України характеризується, з одного боку, посиленням уже наявних загроз, а з іншого – появою нових викликів.

Технологічні інноваційні процеси, інформаційний прорив, глобалізація світу та тенденції регіональної інтеграції поряд із наданням колосальних можливостей для поступального розвитку країн зумовлюють багато негативних наслідків. Наприклад, активізувалося ведення гібридної війни між державами, зокрема проти України. Збільшується їх спроможність щодо проведення інформаційних та інформаційно-психологічних операцій, посилення чутливості суспільства до загибелі мирного населення та втрат особового складу військових формувань у воєнних конфліктах. У сучасних умовах глобалізації, технологічною основою якої стали глобальні інформаційно-телекомунікаційні мережі та єдиний інформаційний простір, спостерігається тенденція до зміни принципів і методів управління, зокрема у військовій справі. Здатність інформації впливати на світогляд та настрої людей дає можливість отримувати перевагу над противником, не вступаючи в силове протистояння з ним. Фактично правильна методика роботи з інформацією стала новим способом ведення збройної боротьби, а саме гібридної війни. З огляду на це в провідних країнах світу проходить поступова трансформація підходів до формування воєнної політики держави, які практично втілюються для забезпечення її інформаційної безпеки в умовах гібридної війни. Повномасштабна інформаційна війна Росії проти України продемонструвала важливість забезпечення інформаційної безпеки як однієї з основних складових національної безпеки. Саме тому перед державними і військовими органами управління постало завдання розробки ефективних заходів нейтралізації негативного інформаційного впливу Російської Федерації та протидії його подальшому розгортанню.

У статті також проаналізовано підходи до підвищення ефективності державного реагування на загрози національній безпеці в інформаційній сфері в умовах сучасного збройного конфлікту на сході України. Встановлено, що для досягнення відповідного рівня інформаційної безпеки необхідно сформувати єдиний державний механізм забезпечення інформаційної безпеки. Запропоновано спосіб вирішення завдань, які виникають у даній сфері.

Ключові слова: *інформаційна безпека; гібридна війна; інформаційна зброя; суспільство; державна політика.*

Постановка проблеми в загальному вигляді. Гібридна війна, у стані якої перебуває Україна, деструктивно впливає на свідомість українського населення. Наша держава, як

і більшість цивілізованого світу, у цілому виявилася не готовою до такої агресії з боку Росії. Підтвердження цьому – відсутність чітких правил поведінки в умовах інформаційної агресії та пропаганди. Одним із найбільш відчутних викликів для України є масштабна російська пропаганда, яка вже давно вийшла за межі кордонів. Тому інформаційна безпека є одним із основних чинників стабільного розвитку держави, що формується в руслі об'єктивних процесів забезпечення національної безпеки. Для усунення гібридних загроз національній безпеці або запобігання їх появі доводиться вдаватися до інформаційного захисту держави. У сучасних умовах на усіх рівнях: ідеології, релігії, історії, освіти – застосовуються інформаційні війни. Сьогодні гостро постає питання забезпечення інформаційної безпеки, а саме в умовах гібридної війни. Тому основними напрямами державної інформаційної політики повинно бути гарантування інформаційної безпеки особистості, яка характеризується захищеністю її психіки та свідомості від небезпечних інформаційних впливів, дезінформації та маніпулювання.

Аналіз останніх досліджень і публікацій. Авторами робіт, що становлять методологічну основу досліджень загальнотеоретичних питань інформаційної безпеки, є такі науковці: О. Левченко [15], Р. Грищук [5], В. Горбулін [9], М. Биченок [3], О. Тихомиров [13], І. Грабар [6], В. Антонюк [1], А. Кунинець [14], В. Бондаренко [4], Ю. Горбань [7], Ф. Медвідь [18], В. Ліпкан [17], Д. Дубов [11], Я. Жарков [20] тощо. Усі вони працювали над проблемою забезпечення інформаційної безпеки України, проте, незважаючи на дуже велику кількість наукових праць з цієї тематики, розкриття питання механізму забезпечення інформаційної безпеки держави в умовах гібридної війни не є комплексно спрямованим.

Формулювання завдання дослідження. Мета статті – проаналізувати головні складові інформаційної безпеки України в умовах гібридної війни, адже дана проблема має давнє походження і стала особливо важливою у наш час, коли використання з боку сусідньої держави (Росії) інформаційних технологій поширилося практично у всі сфери нашого життя.

Виклад основного матеріалу. Останнє десятиліття XX століття було відзначене драматичними змінами на міжнародній арені. Крах біполярної геополітичної моделі світоустрою призвів до корінної зміни геополітичної ситуації у всьому світі. Закінчилася епоха відносної стабільності, відбувся фактично крах Ялтинско-Потсдамської системи безпеки. Значні перетворення на політичній карті Європи в 90-ті роки XX століття створили нові геополітичні умови, які призвели до реанімації старих і виникнення нових конфліктних ситуацій. Загострюється боротьба між окремими країнами за глобальне і регіональне лідерство, зокрема і за володіння природними ресурсами. Форми цієї боротьби різні, але її запеклість і безкомпромісний характер свідчать про актуалізацію питань забезпечення національної безпеки для кожної держави окремо, проблем виживання та розвитку в новому тисячолітті.

Глобальні процеси інформатизації суспільства та широке запровадження інформаційних технологій, їх вплив на всі сфери розвитку держав висувають на перший план питання забезпечення інформаційної безпеки. Від виваженої політики інформаційної

безпеки, від ступеня захищеності, достовірності та повноти інформації в цивілізованому сучасному світі залежить стабільна соціальна, економічна, правова ситуації в державі. На тлі всіх цих геополітичних перетворень інформація стає найпотужнішим глобальним стратегічним ресурсом, володіючи яким, суспільство і держава вже сьогодні можуть значно посилити свої позиції на міжнародній арені і управляти світовими політичними, економічними, соціальними, культурними та іншими процесами, що відбуваються в міжнародних системах.

Конвергенція комунікацій, комп'ютерних систем, індустрії розваг і побутової електроніки істотно змінює інформаційне середовище проживання людини. У результаті цих змін, які мають глобальний характер, інформаційна сфера все більшою мірою визначає не тільки технологічні інновації, а й соціокультурну основу суспільного життя, потреби особистості, менталітет і поведінку мільярдів людей. Зміна ролі інформації в житті людства, а також поява нових технологій обробки, передачі, зберігання та подання інформації дозволяють сьогодні говорити про те, що сучасна цивілізація змінює свій вигляд і входить у нову епоху, перетворюючись в інформаційну цивілізацію.

Поступово інформація зачіпає всі сфери життєдіяльності людини, що дозволяє говорити про неї як про нову форму влади. Вона не замінює повністю інші форми влади, а значно розширює можливості як усередині суспільств і держав, так і на міжнародній арені. Інформація пронизує буквально всі сфери життєдіяльності більш-менш розвинених сучасних держав. За допомогою неї та інформаційних технологій сьогодні нерідко скидають одні політичні еліти в державах і підтримують інші. У деяких випадках інформаційний вплив на окремі країни зведено в ранг інформаційної війни. Проблема забезпечення інформаційної безпеки в сучасному світі, особливо для України, набула важливого значення. Досягнення в інформаційній сфері створюють передумови для формування нового типу інформаційного суспільства, основою для якого є бурхливий розвиток та конвергенція інформаційних і телекомунікаційних технологій. Цей процес відбувається в умовах глобалізації [6].

Усе це призводить до того, що провадиться політика глобалізації у своїх інтересах найбільшими країнами, які поступово формують умови для створення керованого й підконтрольного їм суспільства менш захищених держав. Інформаційна глобалізація разом з глобалізацією економічною, політичною та культурною розмиває державні кордони.

У зв'язку з цим забезпечення інформаційної безпеки в умовах гібридної війни для нашої держави стає найпершою проблемою.

Аналіз даного питання показує, що сучасний стан системи інформаційної безпеки України характеризується, з одного боку, посиленням вже наявних загроз, а з іншого – появою нових викликів. Інноваційні технологічні процеси, інформаційна революція, економічна та соціокультурна глобалізація світу, тенденції регіональної інтеграції поряд із наданням колосальних можливостей для поступального розвитку країн і регіонів зумовлюють багато негативних наслідків. Серед них – активізація ведення інформаційних та інформаційно-психологічних війн між окремими країнами, зокрема й проти України. Ці війни називають гібридними, вони виникають в умовах появи нових форм збройної

боротьби, піднесення сепаратистських рухів, посилення діяльності міжнародних терористичних організацій, зниження можливостей держав щодо контролю над процесами, які відбуваються в межах їх національних територій. У зв'язку з формуванням загальносвітового інформаційного простору неухильно зростає роль громадської думки, яка сьогодні стала потужним фактором управління, виховання і регулювання поведінки людей.

Такі процеси супроводжуються спробами встановити повний контроль Російської Федерації (РФ) над ситуацією в Україні, при цьому широко використовуються методи гібридної війни, а також маріонеткові політичні сили для захисту нібито "приниженого російськомовного населення". Тому основною метою Росії, що протистоїть Північноатлантичному альянсу, є утримання України під своїм контролем, використання наших територіальних, матеріальних, трудових, інформаційних та інтелектуальних ресурсів, перешкоджання приходу до влади проєвропейських сил, здатних відновити політичну, економічну та військову конкурентоспроможність держави.

Одним із важливих завдань РФ є позбавлення України її стратегічних і тактичних союзників у країнах НАТО, створення перешкод для досягнення нашою державою своїх національних інтересів у світі, а також для налагодження нових і збереження старих зв'язків із сусідами на пострадянському просторі.

Росія й Україна мають велику кількість пересічних інтересів у світі, щоб зберігати навіть видимість нейтралітету відносно одна одної. У сучасній імперській політиці Україні, як і раніше, відводиться місце домініону РФ, а отже, обмежуються її інтереси у світі. Подібна обставина об'єктивно не може довго існувати, оскільки суперечить не тільки статусу України як суверенної держави, а й здатності Росії тримати під контролем ситуацію в нашій державі.

Таке становище нестійкої рівноваги між Україною та РФ може призвести до значних світових потрясінь. За цих умов наша держава повинна докласти особливих зусиль для відстоювання життєво важливих інтересів, мати чітко вироблену концепцію протидії викликам і загрозам у політичній, економічній, військовій, а також в інформаційній сферах, щоб захистити власну безпеку.

Особливу увагу необхідно звернути на те, що українське суспільство зацікавлене в створенні державних захисних механізмів, які сприяли б формуванню за кордоном об'єктивного погляду на українську дійсність. Як показує практика, діяльність вітчизняних засобів масової інформації (ЗМІ) з роз'яснення закордонній аудиторії цілей і основних напрямків державної політики України, позицій щодо соціально значущих подій українського та міжнародного життя потребує вдосконалення. Це один із найбільш важливих об'єктів забезпечення інформаційної безпеки держави.

На сьогодні Україна має у своєму розпорядженні необхідні ресурси для забезпечення своєї інформаційної безпеки. Вони повинні бути використані в таких сферах: розробка основних напрямів державної політики в галузі вдосконалення інформаційного забезпечення зовнішньополітичного курсу; створення українським представництвам і організаціям за кордоном умов для роботи з нейтралізації поширюваної там дезінформації про зовнішню політику; удосконалення інформаційного забезпечення

з протидії порушення прав і свобод українських громадян та юридичних осіб на території РФ. Зміцнення свого інформаційного впливу у світі необхідно розглядати як найважливішу складову інформаційної політики України. Для успішної відсічі зовнішнім і внутрішнім інформаційним загрозам із боку Росії необхідна перш за все внутрішньополітична стабільність і єдність суспільства. Однак дійсність українського суспільства характеризується наявністю розколу на прихильників національної ідеї та так званого "руського миру", що послаблює протистояння інформаційним загрозам. Усе це вимагає від України посилити свій вплив в інформаційній безпеці з метою захисту інтересів держави, її цілісності та суверенітету.

Агресивні дії Росії проти України спричинили руйнування європейської та глобальної безпеки. Сам російсько-український конфлікт порушив регіональну стабільність та створив глобальні ризики. Термін "гібридна війна" виявився не тільки теоретично, а й практично найбільш придатним для специфіки дій агресора, який, поєднуючи дипломатичні, квазімілітарні, мілітарні, інформаційні, економічні засоби, залякуючи ядерним шантажем, намагається послідовно досягнути власних політичних цілей [9].

Що є гібридної війною? На це питання існує безліч тверджень та думок, але якщо все ж спробувати дати узагальнену відповідь на зазначене питання, то безперечним зараз є розуміння того, що це поєднання численних військових і невійськових типів атак та впливів на противника заради досягнення своєї мети. У процесі гібридної агресії ворог використовує в основному слабкості, недоліки або характеристики противника, які в цілому в мирний час не сприймаються як слабкі сторони. На сучасному етапі для агресора головними методами ведення гібридної війни є використання ЗМІ та соціальних мереж.

Гібридну війну можна трактувати як модель війни, за якої намагаються приховати її військовий характер, а також участь у ній державних структур. Саме тому в ній різко зростає роль інформаційної складової, оскільки реальні фізичні контексти замінюються неадекватними їм інформаційними, що приховують реальний стан справ більш інтенсивно, ніж це має місце у війні звичайного порядку [2]. Гібридна війна має невелику ділянку реально бойових дій, але поширюється в усьому мирному просторі, підключаючи до конфліктних ситуацій абсолютно всі ресурси, включаючи артистів, письменників, політичних діячів інших країн. Говорити про гібридну війну як про невійськову потрібно, адже в ній військові видозмінюються на цивільних, чиновники – на гравців недержавного рівня. Прикладом трансформації "військові – цивільні" є "зелені чоловічки" в Криму, яких російська пропаганда досить довго відмовлялася визнавати військовослужбовцями збройних сил, оскільки у них не було розпізнавальних знаків. Щоправда зброя була, але вони намагалися її не застосовувати, вона слугувала засобом залякування.

Російська гібридна війна в Україні схожа на китайську концепцією "війни без обмежень", у якій багато невійськових інструментів. До російський "гібридних елементів" можна віднести: фінансування політичних партій; інвестиції; придбання недійсного ресурсу; входження до європейських структур російських розвідувальних органів; використання заморожених конфліктів на етнічному підґрунті та релігійних інституцій; підтримка російських ЗМІ за кордоном; кібератаки та їх координація. Країна, що

проводить інформаційно-психологічні заходи, повинна довести справедливість своїх дій як для власного суспільства, так і для народу, на який вони націлені. У неоголошеній війні атакованій країні досить важко давати відсіч. Гібридна війна стала надбанням нового часу саме тому, що багато потрібних для неї завдань можна виконати за рахунок інформаційного компонента. Чим потужніший його розвиток, тим легше досягти поставлених цілей.

Недостатня ефективність наявної на сьогодні інформаційної безпеки в умовах динамічного та малопередбачуваного впливу сучасних факторів геополітичної конкуренції, глобалізації й найбільш гострих форм інформаційного суперництва, яке відобразилося у збройному конфлікті на сході України, вимагає зміни всієї чинної концепції інформаційної безпеки з метою її адаптації до сучасних умов. Істотні труднощі в забезпеченні інформаційної безпеки в умовах гібридної війни дозволяють нам говорити про особливі умови її реалізації та необхідність вироблення механізмів впливу, спеціальних методів, адекватних тим змінам, які відбуваються в суспільстві [3].

Реалізація особливих умов забезпечення інформаційної безпеки в умовах гібридної війни полягає в:

глобальному формуванні інформаційного суспільства;

соціально-політичній, інформаційній, психологічній глобалізації;

геополітичній конкуренції інформаційного простору;

інформаційно-психологічному протистоянні як складовій збройного конфлікту, що виник на окремих окупованих територіях України [5].

На початку війни в 2014 році наша країна зіткнулася з використанням проти неї пропагандистської системи Росії, що діє одночасно на всіх напрямах (українському, російському, міжнародному), застосовуючи всі різновиди засобів масової комунікації.

Аналіз сучасної воєнно-політичної ситуації, що складалася довкола України та на її території, дає підстави вважати, що наша держава від самого початку, коли проголосила незалежність, стала об'єктом для пропагандистських дій (операцій) та довготривалого психологічного впливу з боку РФ.

Гібридна війна при цьому є якісно новим підходом ведення воєнної кампанії, у якій закладена психологічна та інформаційна обробка громадян, застосування жорсткої сили іміджевої дипломатії на підготованій території, що дало змогу реалізувати активну приховану інтервенцію в Україну заздалегідь добре навчених нечисленних диверсійних груп (озброєних сучасною бронетехнікою, ефективними засобами наступу й оборони), які з легкістю анексували на свою користь окремі території, зокрема АР Крим [10].

Зважаючи на викладене вище, пропонуємо спосіб вирішення таких завдань, які повинні покращити забезпечення інформаційної безпеки України в умовах гібридної війни. На рис. 1 відображено основні пріоритетні напрями та організаційні питання в цій сфері.

Отже, майбутнє України залежить від ефективності забезпечення інформаційної безпеки, здатності самої держави захистити й відстояти у своєму інформаційному просторі національні та духовні цінності, забезпечити стійку працездатність державних структур щодо прийняття адекватних рішень у складних ситуаціях та обстановці невизначеності.

Для підвищення ефективності державного реагування на загрози забезпечення інформаційної безпеки в умовах гібридної війни та сучасного збройного конфлікту на території України виокремимо основні чинники реагування (рис. 2).

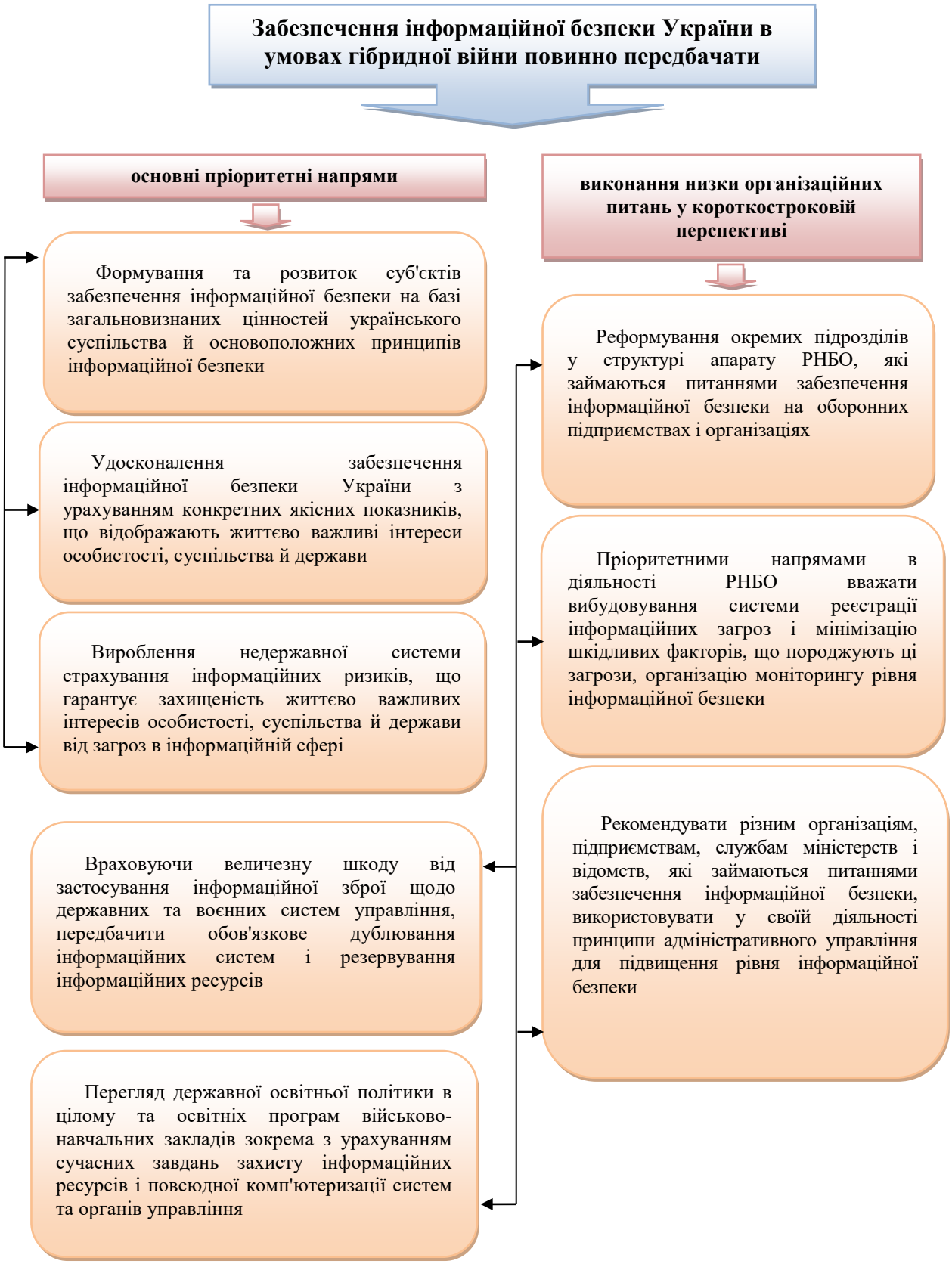

Рис. 1

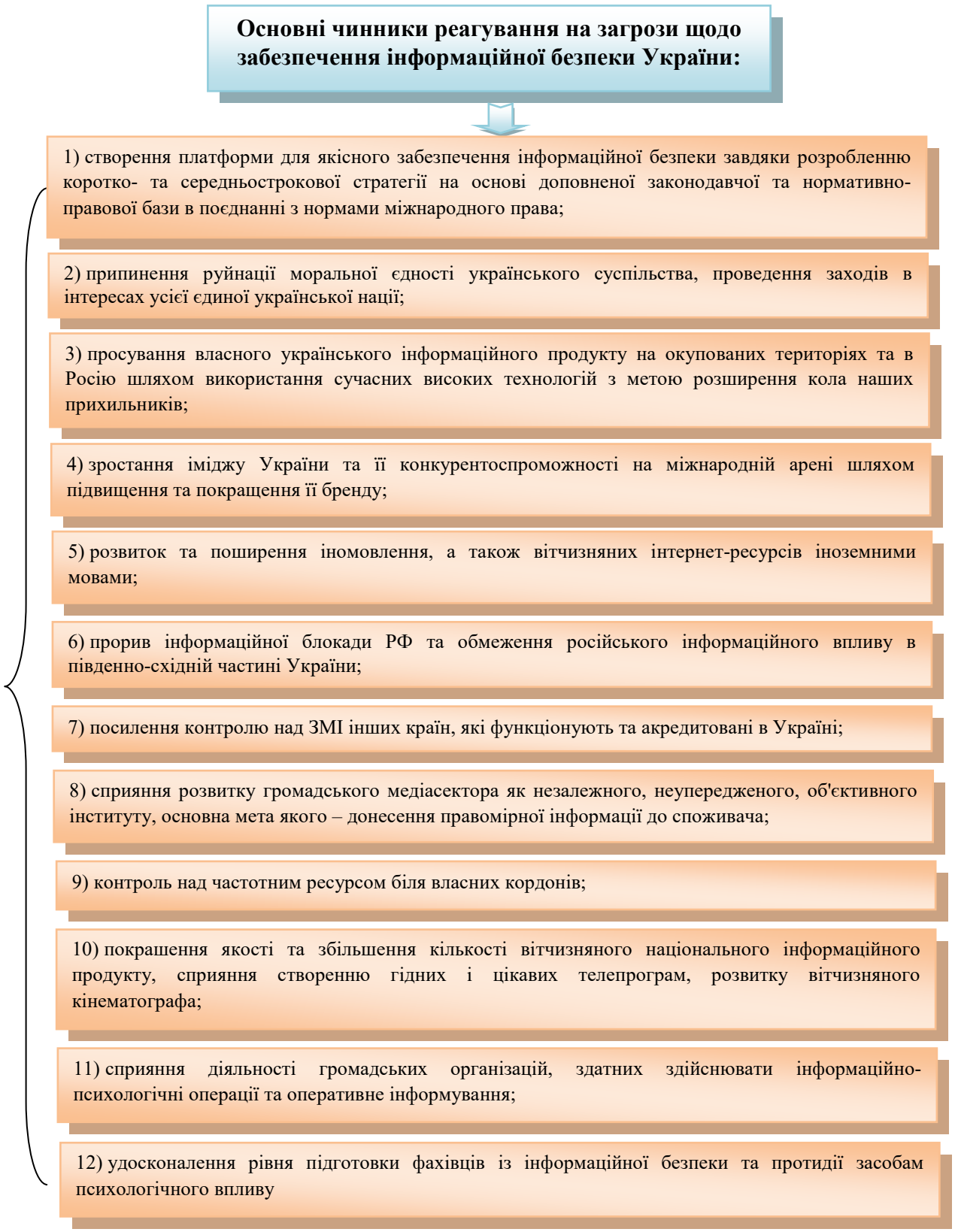

Рис. 2

Підсумовуючи викладене вище, слід визначити відповідний рівень забезпечення інформаційної безпеки України в умовах гібридної війни та сформувати єдиний державний механізм на основі вирішення таких завдань (рис. 3).

Рис. 3

Висновки. Отже, можна стверджувати, що виконання зазначених вище заходів дасть змогу протидіяти гібридним загрозам як традиційними, так і новими центрами протистояння, унеможливить подальше маніпулювання свідомістю суспільства в ході масштабної російської експансії та сприятиме захисту інформаційної безпеки нашої держави.

Можливості забезпечення інформаційної безпеки в умовах гібридної війни залежать від результативності, ефективного впливу на населення України, зростання в суспільстві довіри до керівництва держави, вітчизняних ЗМІ, зниження рівня дестабілізаційної обстановки в країні. Успішне забезпечення інформаційної безпеки сприятиме стійкості українського суспільства до різноманітних деструктивних інформаційно-психологічних впливів, що породжуються з реалізацією гібридних загроз. Ефективний інформаційний вплив з боку України на іноземну цільову аудиторію сприятиме поступовому формуванню проукраїнських поглядів у міжнародній спільноті.

СПИСОК ЛІТЕРАТУРИ

1. Антонюк В. В. Ієрархія керівних документів державної політики з питань забезпечення інформаційної безпеки: шляхи впорядкування // Актуальні проблеми державного управління, педагогіки та психології. 2013. Вип. 2. С. 11–16.

2. Богуш В., Юдін О. Інформаційна безпека держави / Гол. ред. Ю. О. Шпак. Київ : "МК-Прес", 2005. 432 с.
3. Биченок М. М., Шемаєв В. М. Формалізація та оцінювання інформаційних загроз національним інтересам // Труди університету. Київ : НУО України, 2011. № 1 (100). С. 54–61.
4. Бондаренко В. О., Литвиненко О. В. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: http://www.crime-research.iatp.org.ua/library/strateg.htm (дата звернення: 15.10.2019).
5. Грищук Р. В., Молодецька-Гринчук К. В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах // Сучасний захист інформації. 2017. № 3 (31). С. 86–96.
6. Грабар І. Г., Грищук Р. В., Молодецька К. В. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / За заг. ред. Р. В. Грищука. Житомир : ЖНАЕУ, 2019. 280 с.
7. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення URL: http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf (дата звернення: 15.10.2019).
8. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть // Вісник Київського ун-ту ім. Т. Шевченка. 1999. Вип. 14: Міжнародні відносини. С. 46–48.
9. Горбулін В. П. Світова гібридна війна: український фронт : монографія. Київ : НІСД, 2017. 496 с.
10. Горбулін В. П., Биченок М. М., Копка П. М. Актуальні проблеми системного забезпечення інформаційної безпеки України // Зб. мат. Міжнар. наук.-практ. конф. ("Форми та методи забезпечення інформаційної безпеки держави", м. Київ, 13 березня 2008 р.). Київ : Нац. академія СБ України, 2008. С. 79–85.
11. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. Київ : НІСД, 2011. 30 с.
12. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Вид. дім "Києво-Могилянська академія", 2015. 497 с.
13. Тихомиров О. О. Забезпечення інформаційної безпеки: теоретико-правовий аспект // Право України. 2011. № 4. С. 252−259.
14. Кунинець А. І, Грицюк Ю. І. Інформаційні загрози та проблеми забезпечення інформаційної безпеки промислових компаній // Науковий вісник НЛТУ України. 2013. Вип. 23 (2). С. 352–360.
15. Левченко О. В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки // Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 3 (20). С. 47–50.
16. Литвиненко О. Інформація і безпека // Нова політика. 1998. № 1. С. 47–49.
17. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.
18. Медвідь Ф. Інформаційна безпека України: виклики та загрози. URL: http://www.nato.ru.if.ua/journal/2009-2-28.pdf (дата звернення: 15.10.2019).
19. Хоффман Л. Дж. Современные методы защиты информации / [пер. с англ.]. Москва : Советское радио, 1980. 57 с.

20. Історія інформаційно-психологічного протиборства : підруч. / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов та ін.] ; за заг. ред. Є. Д. Скулиша. Київ : Наук.-вид. відділ НА СБ України, 2012. 212 с.

Подано 25.11.2019

С. А. Запорожец

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УКРАИНЫ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ

Статья посвящена исследованию информационной безопасности Украины в условиях гибридной войны, противостоянию гибридным угрозам со стороны Российской Федерации, а также приоритетным направлениям эффективного обеспечениия информационной безопасности в нашей стране. Анализ данной проблемы показывает, что современное состояние системы информационной безопасности Украины характеризуется, с одной стороны, усилением уже существующих угроз, а с другой – появлением новых вызовов.

Технологические инновационные процессы, информационный прорыв, глобализация мира и тенденции региональной интеграции наряду с предоставлением колоссальных возможностей для поступательного развития стран несут много негативных последствий. Например, активизировалось ведение гибридной войны между государствами, в том числе против Украины. Увеличивается их способность по проведению информационных и информационно-психологических операций, усилению чувствительности общества к гибели мирного населения и потерям личного состава воинских формирований в военных конфликтах. В современных условиях глобализации, технологической основой которой стали глобальные информационно-телекоммуникационные сети и единое информационное пространство, наблюдается тенденция к изменению принципов и методов управления, в том числе в военном деле. Способность информации влиять на мировоззрение и настроения людей дает возможность получать преимущество перед противником, не вступая в силовое столкновение с ним. Фактически правильная методика работы с информацией стала новым способом ведения вооруженной борьбы, а именно гибридной войны. Учитывая это, в ведущих странах мира проходит постепенная трансформация подходов к формированию военной политики государства, которые практически воплощаются для обеспечения информационной безопасности в условиях гибридной войны. Полномасштабная информационная война России против Украины продемонстрировала важность обеспечения информационной безопасности как одной из основных составляющих национальной безопасности. Именно поэтому перед государственными и военными органами управления стоит задача по разработке эффективных мер нейтрализации негативного информационного воздействия Российской Федерации и противодействия его дальнейшему развертыванию.

В статье также проанализированы подходы к повышению эффективности государственного реагирования на угрозы национальной безопасности в информационной сфере в условиях современного вооруженного конфликта на востоке Украины. Установлено, что для достижения соответствующего уровня

информационной безопасности необходимо сформировать единый государственный механизм обеспечения информационной безопасности. Предложен способ решения задач, возникающих в данной сфере.

Ключевые слова: *информационная безопасность; гибридная война; информационное оружие; общество; государственная политика.*

S. A. Zaporozhets

INFORMATION SECURITY OF UKRAINE IN THE CONDITIONS OF THE HYBRID WAR

The article is devoted to the study of information security of Ukraine in the conditions of hybrid war, confrontation of hybrid threats from the Russian Federation, as well as priority directions for the effective provision of information security in our country. The analysis of this problem shows that the current state of Ukraine's information security system is characterized by an increase in existing threats, and on the other hand by the emergence of new challenges.

Technological innovation processes, information breakthroughs, globalization of the world and tendencies of regional integration, along with providing enormous opportunities for the country's progressive development, have many negative consequences. One of the consequences has been the intensification of hybrid warfare between world countries, including against Ukraine. States' capacity to conduct information and information-psychological operations, to increase the sensitivity of society to the death of civilians and to the loss of military personnel in military conflicts are increasing. In the current conditions of globalization, the technological basis of which is the global information and telecommunication networks and a single information space, there is a tendency to change the principles and methods of management, including in military affairs. The ability of information to influence people's worldview and moods gives them the opportunity to gain an advantage over an adversary without engaging in a forceful confrontation with him. In fact, the correct method of working with information has become a new way of conducting an armed struggle, namely a hybrid war. In this regard, the leading countries of the world are undergoing a gradual transformation of approaches to the formulation of military policy of the state, which are practically embodied in ensuring the information security of the state in the conditions of hybrid war. The full-scale information war of Russia against our state has demonstrated the importance of ensuring information security as one of the main components of national security. In view of the above, the state and military authorities of the country were tasked with developing effective measures to neutralize the negative information impact of the Russian Federation and counteract its further deployment.

The article also analyzes well-known approaches to improving the effectiveness of state response to national security threats in the information sphere in the context of the current armed conflict in eastern Ukraine. It is established that in order to achieve the appropriate level of information security it is necessary to create a single state mechanism for ensuring information security. A method for solving problems arising in this field is proposed.

Keywords: *information security; hybrid war; information weapons; society; public policy.*