УДК 361.86:004:659.3

К. Г. БРИЧУК,
кандидат наук з державного управління,
головний редактор газети "Печерськ", м. Київ

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ПРІОРИТЕТНИЙ МЕХАНІЗМ ЗАХИСТУ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ ДЕРЖАВИ ВІД ГІБРИДНОЇ ЗАГРОЗИ

У статті досліджено інформаційну безпеку як головний складник захисту національних інтересів в умовах гібридної загрози для держави. Проаналізовано основні характеристики та визначено сучасні особливості розгортання інформаційних війн в умовах загроз кіберсередовищу системи державної влади та геополітичних інформаційних інтервенцій, спрямованих на справляння деструктивного впливу на суспільство. Обґрунтовано, що дезінформація як засіб зовнішньої загрози для безпеки та оборони держави в середовищі інтернет-комунікацій стає ефективним засобом ведення інформаційних війн через застосування симулятивних та фейкових механізмів маніпулятивного впливу на масову свідомість супротивника.
***Ключові слова*:** інформаційна безпека, гібридна загроза, інформаційна війна, маніпуляція свідомістю.

K. G. BRYCHUK,
Ph.D in Public Administration, Chief Editor of the "Pechersk" newspaper, Kyiv

INFORMATION SECURITY AS A PRIORITY MECHANISM FOR THE NATIONAL INTERESTS PROTECTION FROM A HYBRID THREAT

The article is devoted to the study of information security as a strategic resource and information as its main component in a hybrid threat in the modern world. The main characteristics and accents concerning the implementation of information wars in cybersecurity and informational interventions for the national interests of the states are outlined. It is emphasized that the information in the Internet communication environment due to manipulative influence on the mass consciousness and through misinformation, simulation and fake of the opposite side becomes a means of conducting information wars as a hybrid tool.
Key words: information security, hybrid threat, information war, manipulation of consciousness.

К. Г. БРИЧУК,
кандидат наук государственного управления, главный редактор газеты "Печерск", г. Киев

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ПРИОРИТЕТНЫЙ МЕХАНИЗМ ЗАЩИТЫ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ ГОСУДАРСТВА ОТ ГИБРИДНОЙ УГРОЗЫ

В статье исследована информационная безопасность как главный компонент защиты национальных интересов в условиях гибридной угрозы для государства. Проанализированы основные характеристики и определены современные особенности развертывания информационных войн в условиях угроз киберсреде системы государственной власти и геополитических информационных интервенций, направленных на осуществление деструктивного влияния на общество. Обосновано, что дезинформация как средство внешней угрозы для безопасности и обороны государства в среде интернет-коммуникаций становится эффективным средством ведения информационных войн из-за применения симулятивных и фэйковых механизмов манипуляторного воздействия на массовое сознание противника.
Ключевые слова: информационная безопасность, гибридная угроза, информационная война, манипуляция сознанием.

Постановка проблеми. Стратегії розвитку інформаційного суспільства, що зумовлені науково-технічним прогресом, не тільки суттєво скоригували життєдіяльність різних сфер суспільства, а й спричинили усвідомлення значення, ролі та відповідного ставлення до інформації як одного із стратегічних ресурсів, міцність і цілісність якого свідчить про рівень належної

безпеки та стабільності в тому чи іншому секторі. Особливо це актуалізувалося відтоді, коли інформація як ресурс стала інструментом впливу (часто деструктивного і руйнівного) в умовах суспільно-політичних і воєнних конфліктів та протистоянь. Загалом саме інформація в умовах глобалізованого світу вивела подібні конфлікти щодо перерозподілу сфер впливу за матеріальні ресурси, ідеологічний контроль та інші питання на новий рівень. Це виявилося, насамперед, у нечіткості використання прямих засобів впливу та можливості маніпулятивної наратії, що дало змогу значно розширити масштаби охоплення цілей та отримання результату.

Відтак будь-які інтервенції, навіть прямі військові конфлікти, що мали на меті певний деструктивний вплив, набували ознак гібридності саме завдяки використанню інформаційної складової. Такі обставини та ситуації стали прямим поштовхом до вдосконалення заходів інформаційної безпеки як загалом на рівні держав, так і особливо тих секторів, що мають вирішальне і стратегічне значення для життєдіяльності суспільства.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми. Проблематика інформаційних воєн у контексті розвитку сучасного цифрового суспільства знайшла відображення в деяких сучасних дослідженнях і публікаціях. З огляду на стан зарубіжних країн в умовах збройних конфліктів та геополітичних протистоянь особливо слід згадати праці Т.Андрієвського [1], В.Бурячок [2], В.Горбуліна [3], В.Куйбіди [4], О.Карпенка [4; 5], О.Курбана [6], О.Лалак [7], Г.Почепцова [8], В.Романової [9], С.Соколової [10], І.Сопілко [11], І.Феськова [12], Г.Четверик [13].

Однак невирішеною проблемою науки державного управління залишається обґрунтування виникнення феномену гібридної загрози в умовах збройного конфлікту на Сході України.

Мета статті – дослідити значення інформаційної безпеки як стратегічного ресурсу в умовах гібридної загрози.

Виклад основного матеріалу. Інформація в сучасному глобалізованому і технологічно насиченому світі – це важливий ресурс, втрата якого може мати непередбачувані наслідки. Втрата конфіденційних даних стратегічних об'єктів національного рівня криє в собі загрозу для національних інтересів, фінансових втрат, оскільки отримана інформація може використовуватися з деструктивною метою. Для запобігання таким ситуаціям необхідно вживати комплекс засобів щодо захисту на доктринально-стратегічному рівні захисту інформації.

Якість функціонування будь-якої інформаційної системи багато в чому визначається рівнем її захисту від зовнішнього впливу та можливих втручань. Крім того, що сфера забезпечення інформаційної безпеки має відповідати вимогам чинного законодавства в межах національної держави, пріоритетне значення має також орієнтація на міжнародні стандарти безпеки і життєдіяльності, розроблені та впроваджені передовими за рівнем економічного і технологічного розвитку країнами. Зростаюча потреба в надійному захисті даних у разі їх обробки в інформаційному середовищі ставить перед технологічною ІТ-індустрією безпрецедентні завдання щодо забезпечення захисту національних інтересів країни. Порушення функціональності цифровізованих систем, у тому числі й через порушення встановленого режиму захисту інформації, може призвести до серйозних наслідків. Це особливо важливо для систем управління критично важливих об'єктів – цифровізованих систем управління.

Система функціонування інформації, технічних систем і мереж та їх безпеки тісно пов'язана за рівнями як глобального масштабу, так і національних держав та індивідуально-особистісного. Інтересами особистості в інформаційній сфері є такі:

– реалізація конституційних прав людини і громадянина на доступ до інформації;

– використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку;

– захист інформації, що забезпечує особисту безпеку.

Інтереси суспільства в інформаційній сфері полягають у:

– забезпеченні інтересів особистості в цій сфері;

– зміцненні демократії, створенні правової соціальної держави, досягненні та підтримці суспільної злагоди.

Інтереси держави в інформаційній сфері полягають у:

– створенні умов для гармонійного розвитку інформаційної інфраструктури;

– реалізації конституційних прав і свобод людини та громадянина щодо отримання інформації і користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності країни;

– забезпеченні політичної, економічної та соціальної стабільності;

– безумовному забезпеченні законності й правопорядку;

– розвитку рівноправного і взаємовигідного міжнародного співробітництва.

На сьогодні на підставі численних теоретичних узагальнень та з огляду на напрацьований практичний досвід реалізації сформульовано два базових принципи інформаційної безпеки, яка має забезпечувати:

1) цілісність даних – захист від збоїв, що призводять до втрати інформації, а також неавторизованого створення або знищення даних;

2) конфіденційність інформації і одночасно її доступність для всіх авторизованих користувачів.

Слід зазначити, що інформаційне суспільство забезпечує залучення великої кількості людей до інформаційних ресурсів, сприяє покращанню обміну інформацією між різними суб'єктами інформаційних правовідносин, пришвидшує розвиток інформаційних відносин [11, с. 80]. Відповідно, усі ці чинники впливають на загальний стан інформаційного обміну і створення єдиного, але водночас диференційованого за різними відгалуженнями інформаційного віртуального простору, що постійно актуалізує проблему виваженого та комплексного підходу до інформаційної безпеки і захисту інформації.

Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Відповідно, сутність розуміння загроз, особливо гібридного характеру, полягає, насамперед, у тому, що загрози інформаційної безпеки – це зворотний бік використання цифрових технологій. Доцільний з методологічного погляду підхід до проблем інформаційної безпеки розпочинається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем.

Основним середовищем взаємовідносин у сфері інформаційного захисту і безпеки є кіберсередовище або віртуальний простір Інтернету. Кіберпростір не існує у фізичній формі, а виникає в результаті взаємодії людей, програмного забезпечення, інтернет-сервісів за допомогою технологічних пристроїв і мережевих зв'язків. Як зазначає В.Бурячок, під кіберпростором слід розуміти комунікаційне середовище, утворене системою зв'язків між об'єктами інформаційної інфраструктури (інформаційними ресурсами, системами і мережами всіх форм власності), що керуються автоматизованими системами управління (нині електронними та цифровими) й використовуються як для передавання інформації, яка в них циркулює, так й для впливу на аналогічні об'єкти протилежної сторони [2, с. 106].

За всього різноманіття цих визначень слід зауважити, що з огляду на чітку вказівку на пов'язаність кіберпростору з інформаційно-комунікативною інфраструктурою основна увага зосереджена не на технології, а на діяльності людей, які використовують ці технології. Важливо, що основний зміст кіберпростору полягає в роботі користувачів із цифровими (електронними) інформаційними ресурсами та інформаційно-комунікативною інфраструктурою.

Нині спостерігається різке зростання кількості інцидентів у сфері інформаційної безпеки, які дістали поширення і набувають загрозливого характеру. Багато з подібних атак зачіпають широке коло приватних, корпоративних і державних інтересів.

Зростання ролі інформації в сучасному світі призвело до розширення можливостей інформаційних протиборств. Для політиків і військових стало зрозумілим, що сучасне суспільство значно залежить від інформаційно-телекомунікаційних систем, і цей факт не може бути

не врахований під час розробки технологій впливу на свідомість людей шляхом маніпуляцій. Інформаційне протиборство завжди використовувалося у війнах держав за допомогою розвідки і контррозвідки, дезінформації, пропаганди та ін. [1].

Близько 20 держав перебуває в процесі трансформації власних військових потенціалів з огляду на можливості використання мережі Інтернет. Формуються спецпідрозділи, які мають на меті ведення розвідувальної роботи в мережах, захист власних мереж, блокування і "обвал" структур супротивника. Згідно з офіційними заявами такі підрозділи створено у США (U. S. Cyber Command), Великобританії (Cyber Security Operations Centre), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence) [13, с. 242].

Широке і масштабне використання інформації та інформаційних ресурсів з метою справляння будь-якого впливу спричинило формулювання нових понять у секторі інформаційних воєн, одне з яких пов'язане з феноменом гібридизації та похідних понять: гібридна війни та гібридна загроза.

Поняття "гібридна війна" ("hybrid warfare") і "гібридна загроза" ("hybrid warfare threats") уже усталені в офіційній термінології західної військової політики. Вчені фахівці включають у поняття загроз гібридної війни всі засоби, що сприяють завданню шкоди противнику, як традиційні (класичні), так і нові, такі як війни в інформаційному просторі, використання і розробка сценаріїв конфліктів низької інтенсивності на території противника, міжнародний тероризм, міграцію, розпалювання етнічних і релігійних конфліктів, транснаціональну злочинність, демографічні ризики, глобалізаційні виклики та ін. Подальшою метою вдосконалення таких інструментів є адаптувати в гібридній війні як традиційні методи, так і нетрадиційні [9, с. 294].

Вітчизняний дослідник І.Феськов до складових гібридної війни відносить використання методів класичної війни (проведення збройних військових операцій), інформаційної або інформаційно-психологічної, партизанської війни, "кібервійни", елементів тероризму та підривних дій, економічного та дипломатичного впливу. Гібридна війна небезпечна тим, що під час неї фактично стираються межі війни, сценарії її початку та закінчення. Часто буває важко визначити суперника, зміна стану з військового на мирний часто не вирішує конфлікт, у подальшому ситуація може загострюватися [12, с. 68].

Змістом гібридних (інформаційних) війн є конфлікт, за якого завданнями протиборчих сторін є захист власної інформації та інформаційних систем, маніпулювання інформацією противника або її спотворення, а також обмеження можливостей протиборчої сторони в доступі до неї та її обробки.

Гібридну війну також трактують як різновид протистояння, що поєднує в собі звичайні та нестандартні способи ведення війни: класичні прийоми боротьби із залученням військової техніки, військовослужбовців в уніформі; нерегулярні збройні формування (повстанці, терористи, партизани); інформаційну війну. Засоби кібервійни застосовують не лише для доступу до конфіденційних даних держави, а й для пропагандистського розповсюдження матеріалів, поширення політичного шпигунства і вандалізму [7].

Гібридна війна є складним явищем, що акумулює в собі всі види сучасної війни, а точніше комплексне застосування традиційного інструментарію для ведення оперативно-стратегічних (військових і спеціальних) операцій з метою фінансово-економічного тиску і перерозподілу ресурсів на території іншої держави, а також отримання морально-психологічних переваг, поширення і утвердження ціннісних пріоритетів для "перезавантаження" моделей і стереотипів поведінки громадян іншої країни, ініційованих за допомогою дипломатії, різних гуманітарних заходів, організованих на регіональному та міжнародному рівнях. Також із цією метою регулярно здійснюються мережеві, інформаційні операції (кібератаки), у тому числі військові дії. Сутність гібридних війн полягає в тому, що підбір, синтез, аналіз необхідної інформації має комплексний характер, оскільки джерелом організованого вторгнення виступає

не військова розвідка, а саме інформаційна інтервенція. Гібридна війна передбачає обов'язкове використання сучасних цифрових технологій, інформаційного простору, мережевих технологій, активне залучення спеціально підготовлених фахівців, воєнізованих формувань, угруповань терористів, які можуть використовуватися в поєднанні з діями збройних сил і спеціальних підрозділів [1].

Гібридній війні передує досить тривала і комплексна підготовка, а тому їй передують гібридні загрози, які, по суті, є викликами для держави. До таких загроз можна віднести: створення політичних і громадських рухів, які симпатизують майбутньому агресору; налагодження сприятливого інформаційного поля; пропаганду; нав'язування агресором власних історичних, культурних, ідеологічних цінностей тощо, тобто все те, що покликане за допомогою так званої "м'якої сили" схилити населення на бік агресора. Саме тому пропонується розмежувати поняття "гібридні загрози" і "гібридна війна". Звичайно, критерієм концептуального розмежування двох термінів має слугувати факт порушення суверенітету держави: перетин збройними або диверсійними формуваннями кордону, захоплення ними стратегічно важливих об'єктів, вбивство військовослужбовців тощо.

На відміну від гібридної війни, головними тенденціями розвитку гібридних загроз є такі:

– зростання кількості атак, багато з яких ведуть до великих втрат;

– підвищення складності атак, які можуть включати кілька етапів і застосовувати спеціальні методи захисту від можливих методів протидії;

– вплив практично на всі електронні (цифрові) пристрої, серед яких останнім часом все більшої значущості набувають мобільні пристрої, а вони найбільше схильні до ризиків у сфері інформаційної безпеки;

– випадки нападу на інформаційну інфраструктуру великих корпорацій, найважливіших промислових об'єктів і навіть державних структур;

– застосування найбільш розвиненими у сфері комп'ютерних технологій країнами засобів і методів кібернападів на інші держави.

Відповідно до реалій сучасності перед українською системою національної безпеки постають принципово нові виклики. Серед них можна виокремити загрози, які стосуються реалізації потреб людини і громадянина, суспільства та держави щодо продукування, споживання, поширення та розвитку національного стратегічного контенту та інформації [6, с. 60].

Одним із сучасних різновидів гібридних загроз є кібертероризм. Уперше його поняття на теоретичному рівні було опрацьовано в середині 1980-х рр. старшим науковим співробітником американського Інституту безпеки і розвідки Б.Колліном, який цим явищем позначав терористичні дії у віртуальному просторі, схожі з поняттями інформаційної війни та інформаційного криміналу. Одним із способів кібертероризму є політично мотивована атака на інформацію, яка полягає в безпосередньому управлінні соціумом за допомогою превентивного залякування. Це виявляється в загрозі насильства, підтримці стану постійного страху з метою досягнення певних політичних чи інших цілей, примусі до певних дій.

Періодично в інформаційне середовище "вкидаються" провокаційні фейки (неправдиві фото або відео, новини, які подаються як реальність), загострюючи ті чи інші конфлікти та суперечки й відносини між державами. Головним завданням фейків є дезінформація суспільства, при цьому не тільки тієї держави, проти якої спрямований фейк, а й інших держав. У результаті люди, сприймаючи ці фейки, формують хибну думку про певну подію чи явище.

Стало очевидним, що якщо ще недавно Інтернет мав переважно інформаційну складову, то тепер у ньому все більшу силу набирає сектор агітаційний, пропагандистський, що відрізняється яскраво вираженою агресивністю. Традиційні ЗМІ все активніше працюють з інтернет-ресурсами як джерелами інформації і засобами впливу на масову свідомість. Інформація в інтернет-мережі стає все більш масово затребуваною, швидко поширюється і набуває суспільного значення.

Висновки і перспективи подальших досліджень. З огляду на викладене можна зробити висновок, що комплексна інформаційна безпека має бути пріоритетним механізмом захисту національних інтересів держави, особливо в ситуації, коли прагнення до інформаційного домінування, зокрема в геополітичному просторі, має гібридний характер, об'єктивно вимагаючи впровадження методів системної протидії гібридним ризикам і загрозам гібридних війн. Гібридні загрози та гібридні війни є породженням сучасних новітніх цифрових та маніпулятивних технологій і повністю виправдовують свою назву. Ці феномени виникають унаслідок світової терористичної загрози, відображаючи нові інформаційно-технологічні можливості нашого часу в аспекті деструктивної соціально-психологічної, політичної та військової діяльності. Гібридні загрози пов'язані з формуванням єдиного віртуального світу та медіа-простору, глобалізацією і протиборством держав та цивілізацій у цифровій реальності. Такі протиборства є новими за змістом, масштабами, метою та способами її досягнення, уключаючи як відомі, так і потенційно можливі методи боротьби та впливу на масову свідомість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андриевский Т. Гибридная война: сущность и базовые стратегии / Т. Андриевский. – Desecuritate. – 2017. – № 1(3). – С. 158–166.

2. Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / В. Л. Бурячок // Сучас. спеціал. техніка. – 2011. – № 3 (26). – С. 104–114.

3. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – Київ : Інтертехнологія, 2009. – 164 с.

4. Інформаційно-комунікативна діяльність органів публічної влади : монографія / В. С. Куйбіда, О. В. Карпенко, А. В. Дуда [та ін.] ; за заг. ред. В. С. Куйбіди, О. В. Карпенка. – Київ : ЦП "Компринт", 2018. – 364 с.

5. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : дис. ... д-ра наук з держ. упр. : спец. 25.00.02 / Карпенко Олександр Валентинович. – Київ, 2016. – 466 с.

6. Курбан О. В. Основи сучасної національної інформаційної безпеки України / О. В. Курбан // Вісн. ХДАК. – 2017. – Вип. 50. – С. 55–62.

7. Лалак О. А. Ризики і виклики кібербезпеки: досвід України та Польщі / О. А. Лалак, L. Klich // Міжнародні відносини. Серія "Політичні науки". – 2017. – № 13. – URL: journals.iir.kiev.ua/index.php/pol_n/article/view/3001. – Назва з екрана.

8. Почепцов Г. Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах / Георгій Почепцов ; пер. з рос. Т. Гуменюк. – Київ : Києво-Могилян. акад., 2016. – 312 с.

9. Романова В. А. Информационная составляющая гибридных войн современности / В. А. Романова // Государственное и муниципальное управление : ученые зап. СКАГС. – 2015. – № 2. – С. 293–299.

10. Соколова С. Н. Риски и угрозы гибридных войн в современном обществе: парадоксы реальности / С. Н. Соколова // Вест. Полес. гос. ун-та. – 2017. – № 2. – С. 35–40. – (Серия обществ. и гуманит. наук).

11. Сопілко І. М. Становлення мережевого суспільства та питання кібербезпеки / І. М. Сопілко // Юрид. вісн. – 2016. – № 1 (38). – С. 79–85.

12. Феськов І. В. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві / І. В. Феськов // Актуал. пробл. політики. – 2016. – Вип. 58. – С. 66–76.

13. Четверик Г. Г. Напрямки реалізації державної політики у сфері кібернетичної безпеки / Г. Г. Четверик // Вісн. Дніпропетр. ун-ту. Політологія. – 2012. – № 9/2. – Вип. 22. – С. 241–246.

REFERENCES

1. Andryevskyy T. Hybrid War: Essence and Basic Strategies. Desecuritate 2017. – N 1 (3). – P. 158–166.

2. Buryachok V. L. Cybernetic security – a key factor of the sustainable development of a modern information society. Suchasna spetsialna tekhnika N 3 (26), 2011. – P. 104–114.

3. Horbulin V. P. Information Operations and Society Safety: Threats, Opposition. Modeling: monograph / V. P. Gorbulin, O. G. Dodonov, D. V. Lande – K . : Intertekhnolohiya, 2009. – 164 p.

4. Information and communicative activities of public authorities: monograph / V. S. Kuibida, O. V. Karpenko, A. V. Duda [and others]; per community Ed. V. S. Kuibidy, O. V. Karpenko. – Kyiv: CP "Komprint", 2018. – 364 p.

5. Karpenko O. V. Mechanisms of the formation and implementation of service-oriented state policy in Ukraine: Dis ... doctor of sciences in public administration: specialty 25.00.02 "Mechanisms of public administration" / Karpenko Alexander Valentinovich; National Acad state exercise under the President of Ukraine. – K., 2016. – 466 p.

6. Kurban O. V. Fundamentals of modern national information security of Ukraine. Herald of KDAK. 2017. – Issue 50. – P. 55–62.

7. Lalak O. A., Klich L. Risks and challenges of cybersecurity: the Ukraine and Poland experience . Mizhnarodni vidnosyny Seriya "Politychni nauky". 2017. – № 13. URL: journals.iir.kiev.ua/index.php/pol_n/article/view/3001 – Title from the screen.

8. Pocheptsov G. G. The Sense and War: Ukraine and Russia in information and semantic wars / Georgi Pocheptsov; per. from Russian T. Humenyuk – Kyiv: Kyiv-Mohyla Academy, 2016. – 312 p.

9. Romanova V. A. Information component of hybrid wars of the present. Hosudarstvennoe y munytsypal′noe upravlenye. Uchenye zapysky SKAHS, 2015. – N 2. – P. 293–299.

10. Sokolova S. N. Risks and threats of hybrid wars in modern society: paradoxes of reality. Vestnyk Polesskoho hosudarstvennoho unyversyteta. Ceryya obshchestvennykh y humanytarnykh nauk, 2017. – N 2. – P. 35–40.

11. Sopilko I. M. Establishment of a network society and issues of cyber security. Legal Gazette, 2016. – N 1 (38). – P. 79–85.

12. Feskov I. V. Basic methods of conducting hybrid war in the modern information society. Actual problems of politics, 2016. – Issue. 58. – C. 66–76.

13. Chetveryk H. H. Directions of realization of the state policy in the field of cybernetic security. Visnyk Dnipropetrovs′koho universytetu. Politolohiya, 2012. – N 9/2. – Vip 22. – P.241–246.

SUMMARY

The article is devoted to the study of information security as a strategic resource and information as its main component in a hybrid threat in the modern world. The main characteristics and accents concerning the implementation of information wars in cybersecurity and informational interventions for the national interests of the states are outlined. It is emphasized that the information in the Internet communication environment due to manipulative influence on the mass consciousness and through misinformation, simulation and fake of the opposite side becomes a means of conducting information wars as a hybrid tool.

The information society development strategies, driven by the scientific and technological progress, significantly corrected not only the vital functions of various spheres of society, but also contributed to the development of the importance, role and relevance of information as one of the strategic resources, the strength and integrity of which indicates the level of proper security and stability in one sector or another. This is especially true since information as a resource has become an instrument of influence (often destructive and destructive) in the context of socio-political and military conflicts and confrontations.

The issues of information wars in the context of the modern digital society development has been reflected in some modern studies and publications, especially in view of the foreign countries

experience in conditions of armed conflicts and geopolitical confrontations. However, the unsolved public administration problem science remains the justification for the emergence of the hybrid threat phenomenon in an armed conflict in the East of Ukraine.

In addition to the fact that the scope of information security must comply with the requirements of the current legislation within the boundaries of the national state, the focus is also on the international safety and life standards developed and implemented by the advanced countries at their level of economic and technological development. The growing need for reliable data protection when processed in the information environment places unprecedented challenges for the IT industry in ensuring the protection of national interests. Violations of the functionality of digital systems, including violations of the established mode of protection of information, can lead to serious consequences. This is especially important for critical asset administration systems – digital administration systems.

Information protection is a complex of measures aimed at ensuring information security. Accordingly, the understanding essence the threats, especially the hybrid nature, lies, first of all, in the fact that the threats to information security – this is the reverse side of the digital technologies usage. It is advisable, from a methodological point of view, approach to information security problems begins with the identification of subjects of information relations and the interests of these entities associated with the information systems usage.

The main environment for communication in the field of information protection and security is the cybernetic environment or the virtual space (Internet). Cyberspace is a complex environment that does not exist in physical form, but occurs as a result of the interaction, software, Internet services with the help of technological devices and network communications. The growth of the role of information in the modern world has led to an increase in the possibilities of information confrontation. The widespread information and information resources usage for any kind of influence has led to the emergence of new concepts in the information warfare sector, one of which is related to the phenomenon of "hybridization" and derivative concepts of the "hybrid" war and "hybrid" threat.

The terms "hybrid warfare" and "hybrid warfare threats" are already established in the official terminology of Western military policy. Scientists include in the notion of hybrid warfare threats all means that contribute to harming the enemy, both traditional (classical) and new as war in the information space, the use and development of low-intensity conflict scenarios on the enemy's territory, international terrorism, migration, fomentation of ethnic and religious conflicts, transnational crime, demographic risks, globalization challenges, etc.

Hybrid warfare is a complex phenomenon that accumulates all kinds of modern warfare, rather, a comprehensive application of the traditional tools for conducting operational and strategic (military and special) operations to objectives of financial and economic pressure and resources redistribution in the another state territory, and as well as receiving moral and psychological benefits, the dissemination and validation of value priorities for "reloading" models and stereotypes of behavior of citizens of another country, initiated by diplomacy, various humanitarian events organized at the regional and international levels.

It was noted that comprehensive information security should be a priority mechanism for national interests protecting, especially in a situation where the desire for information dominance, in particular in geopolitical space, has a hybrid character, objectively requiring the introduction of methods of systemic counteraction to hybrid risks and threats to hybrid wars. Hybrid threats and hybrid wars are the product of modern, latest digital and manipulative technologies and fully justify its name. These phenomena are generated by the global terrorist threat, reflecting the new information and technological capabilities of modern times in terms of destructive socio-psychological, political and military activities. Hybrid threats are associated with the formation of a single virtual world and media space, globalization and the confrontation of states and civilizations in the digital reality. Such confrontations are new in terms of content, scope, purpose and ways to achieve it, including both known and potentially possible methods of struggle and influence on the mass consciousness.