© Khoroshko V., Khokhlacheva Yu. Information war protection from destructive informational and psychological influences. Part 2 // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 1, pp. 18-23.

DOI: 10.18372/2225-5036.25.13666

ІНФОРМАЦІЙНА ВІЙНА. ЗАХИСТ ВІД ДЕСТРУКТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ. ЧАСТИНА 2.

Володимир Хорошко, Юлія Хохлачова

Національний авіаційний університет, Україна

ХОРОШКО Володимир Олексійович, д.т.н., професор

Рік та місце народження: 1945 рік, м. Харків, Україна.
Освіта: Київський інститут інженерів цивільної авіації, 1968 рік.
Посада: професор кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, технічні системи захисту інформації, аналіз функіонування складних систем.
Публикации: більше 500 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

ХОХЛАЧОВА Юлія Євгеніївна, к.т.н., доцент

Рік та місце народження: 1981 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2004 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, оцінювання уразливостей, оптимізація інформаційних систем.
Публикации: більше 70 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: hohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Анотація: *У ході проведеного дослідження було сформовано рекомендації щодо протистояння інформаційній війні. Проведено аналіз факторів інформаційних впливів та протидія інформаційній зброї, в результаті якого зазначено ряд можливих дій для здійснення протидії російській інформаційній ескалації в Україні з метою створення гідної і адекватної відповіді на інформаційні виклики сучасності. Запропоновано підхід, який дозволяє відстоювати власні інтереси та інтереси держави в умовах глобальних інформаційних впливів. Як показує досвід останніх збройних конфліктів одними з найважливіших механізмів війни є не тільки зміни у військовій справі, але й інформаційна революція, яка зараз переживає стадію формування. Прикладом масштабного використання інформаційної зброї є інформаційна війна, яка ведеться Росією проти України. Визначень терміну інформаційної війни на сьогодні є безліч, але в даній статті розглядається саме визначення, яке є у роботах Мартіна Лібікі «Що таке інформаційна війна?». М. Лібікі також визначив сім різновидів інформаційної війни (командно-управлінська, хакерська, економічна, психологічна, розвідувальна, електронна та кібервійна) та чотири складові психологічної війни (підрив громадського духу, деморалізація збройних сил, війна культур, дезорієнтація командування). Забезпечення інформаційної безпеки в сфері державного та муніципального управління ґрунтується на детальному аналізі структури та змісту управління, а також інформаційних процесів і використання при управлінні відповідних технологій. При цьому визначальними факторами при розробці засобів інформаційної зброї стають саме індивідуальні особливості людини та соціуму. Для того, щоб змоделювати поведінку людини (або суспільства), необхідно знати саме її (його) індивідуальні особливості та переваги. Зараз уже зрозуміло, що інформаційна боротьба стає тим фактором, що впливає на саму війну, її початок, хід і результат. Це підтверджується агресією Росії проти України. Тому, досить актуальною проблемою безпеки України є розробка концепції захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби. У ході проведеного дослідження було сформовано рекомендації щодо протистояння у інформаційній війні. А також проведено аналіз факторів інформаційних впливів та протидії інформаційній зброї, який дозволяє зазначити що потрібно, на нашу думку, для того, щоб протидіяти російській інформаційній ескалації в Україні.*

Ключові слова: *інформаційна війна, інформаційний вплив, інформаційно-психологічний вплив, інформаційна зброя, протидія.*

Вступ

Досвід останніх збройних конфліктів показує, що одними з найважливіших механізмів війни стають не тільки зміни у військовій справі, але й інформаційна революція, яка зараз переживає стадію формування. Перший досвід ведення інформаційної боротьби в оперативному масштабі, як однією із складних військових протиборств, був започаткований у війні в зоні Перської затоки у 1991 році. Успіх застосування інформаційної зброї не тільки окрилив США в розумінні ролі інформаційної боротьби, але надав приклад іншим державам, як її застосовувати та вести. Прикладом масштабного використання інформаційної зброї є інформаційна війна, яка ведеться Росією проти України.

На сьогодні є безліч визначень інформаційної війни. Визначення цього терміну є і у роботах Мартіна Лібікі «Що таке інформаційна війна?» [1]. У ній автор визначив сім різновидів інформаційної війни: командно-управлінська, хакерська, економічна, психологічна, розвідувальна, електронна та кібервійна.

Найбільш важливими, на наш погляд, є електронна та психологічна війни. Електронна війна об'єктом свого впливу має засоби електронних комунікацій – радіозв'язку, телевізійних і комп'ютерних мереж.

Психологічна війна – здійснюється шляхом пропаганди, «промивання мозку» і іншими методами інформаційної обробки населення.

Мартін Лібікі виділяє чотири складові психологічної війни: підрив громадського духу, деморалізація збройних сил, війна культур, дезорієнтація командування.

Безліч визначень інформаційної війни пов'язано, мабуть, із складністю і багатогранністю такого явища, труднощами побудови аналогій з традиційними війнами. Якщо спробувати трансформувати визначення в поняття «інформаційна війна», то навряд вийде щось конструктивне. Це пов'язано з рядом особливостей цієї війни [2].

Для інформаційної війни зазвичай чітко визначена оборона, поняття початку і закінчення можна застосувати лише для окремих операцій інформаційної війни, лінія фронту не визначена, а наступ описується різними моделями. Успіх проведених інформаційних операцій не має прямого зв'язку з співвідношенням військових потенціалів сторін. Забезпечення інформаційної безпеки в сфері державного та муніципального управління ґрунтується на детальному аналізі структури та змісту управління, а також інформаційних процесів і використання при управлінні відповідних технологій.

При цьому визначальними факторами при розробці засобів інформаційної зброї [2] стають саме індивідуальні особливості людини та соціуму. Для того, щоб змоделювати поведінку людини (або суспільства), необхідно знати саме її (його) індивідуальні особливості та переваги.

Зараз уже зрозуміло, що інформаційна боротьба стає тим фактором, що впливає на саму війну, її початок, хід і результат. Це підтверджується агресією Росії проти України. Тому, розробка концепції захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби є актуальною проблемою безпеки України.

Метою роботи є аналіз загальнотеоретичної суті протидії інформаційним впливам.

Новизна полягає в тому, що на сьогодні не існує у повному обсязі достатніх чинників захисту особистості від загроз, пов'язаних з поширенням інформаційних та інформаційно-психологічних впливів. Тому, враховуючи важливість цієї проблеми у теперішній час, представлена спроба вирішення її у даній роботі.

Основна частина

Задача виявлення дезінформації або інформаційного впливу є складною і багатоаспектною задачею [3, 4], розв'язання якої потребує урахування наступних параметрів:

– визначення якісних показників, які характеризують інформаційний вплив, який несе у собі дезінформацію;

– визначення особливостей організаційної структури проходження інформаційного впливу від джерела до кінцевого користувача (створення маршрутної моделі);

– дослідження кількісних та якісних показників, які характеризують знання про навколишній світ (проблемну область) і є необхідними для залучення при аналізі інформації на достовірність;

– визначення показників зовнішньої характеристики інформаційних впливів (Звідки? Куди? Кому? Від кого? Коли надійшов певний інформаційний вплив) та методик їх використання при оцінці достовірності інформації;

– дослідження інформаційних моделей суб'єкта, об'єкта та створювача інформації тощо.

В книзі [5] можна прочитати: «В руках сучасних держав є велика сила, яка створює рух думки в народі – це преса. Жодне сповіщення не буде проникати в суспільство без нашого контролю. Це і тепер уже нами досягається тим, що всі новини виходять кількома агентствами, в яких вони централізуються з усіх кінців світу. Ці агентства будуть тоді вже повністю нашими установами і будуть оголошувати тільки те, що ми їм предпишемо».

Тобто вплив засобів масової інформації (ЗМІ) є дуже різноманітним та виражається в [6]:

– поінформованості суспільства;

– настановах суспільству, поведінці суспільства.

Результатами впливу засобів масової інформації можуть бути [7]:

– зміни в поведінці суспільства;

– зміни в настановах суспільству (бо поведінка і настанови не можуть бути ототожнені);

– зміни у знаннях суспільства, як наслідок зростання поінформованості.

Слід відзначити, що ЗМІ мають дуже великий вплив на суспільство в цілому та на окрему людину.

При аналізі інформаційних джерел можна визначити такі характерні впливові прийоми:

1. Читання думок. Журналіст ніби читає думки пересічних людей, але насправді нав'язує їм свої міркування.

2. Анонімність. Цей прийом ближче до першого типу. Він полягає у використанні анонімного

або фактично анонімного джерела повідомлень. Улюблений прийом для введення в оману активно використовується усіма ЗМІ, особливо російськими. Він відноситься до так званого «Сірого» впливу.

3. Вилучення. Суть цього методу полягає у фільтрації думок членів суспільства. Текст журналіста проходить у повідомлення повністю, а текст інтерв'юера подається частинами. Як визначено у [7] виділяють чотири типи вилучень:

– відхилення;
– перспектива;
– підміна;
– останнє слово.

4. Звеличення. Цей тип прийомів спрямований на ідеалізацію, створення позитивного іміджу людини, спільноти або інституту. Визначають шість видів цього прийому:

– похвала;
– придушення негативу;
– найменування і звеличення негативів;
– ігнорування негативних характеристик;
– збільшення значущості;
– атака опонентів як аморальних осіб.

5. Приниження. Дослідження Е. Ефрона [5,7] доводять, що їх існує сім видів:

– пряма атака;
– непряма атака;
– атака за допомогою подвійного стандарту;
– гумор, сарказм, сатира, іронія;
– аргумент;
– звинувачення за асоціацією;
– код.

6. Підроблений інтелект. Суть цього типу прийомів у штучному створенні враження про нейтралітет комунікатора, який насправді заангажований однією зі сторін. Він поділяється Е. Ефроном [5] на шість прийомів:

– фальшивий комплімент;
– фальшива критика;
– фальшиві серії;
– фальшивий прототип;
– напівдебати;
– подвійна бесіда.

7. Повна фальсифікація. Досить активно використовуються прийоми, що є повною фальсифікацією. Найчастіше використовується така ситуація, як цитування вихопленого з контексту речення, фрази або висловлювання.

8. Редагування структури. Цей тип інформаційних прийомів активно використовує можливості психологічного впливу шляхом структуризації текстів:

– «отруйний сендвіч»;
– «цукровий сендвіч»;
– перебільшення деталей.

9. Інші техніки. Цей тип прийомів зазвичай використовують як додаток, як додатковий разом з іншими. Можна виділити його чотири основні види:

– суперузагальнення;
– недоведена теорія;
– навідне запитання;
– однослівна журналістика.

10. «Буденна розповідь». Цей прийом використовується для адаптації людини до негативної інформації, що викликає заперечення своїм змістом.

11. Голодування. Ефективний прийом емоційного впливу на суспільство та психологічного тиску на владу. Підбирається група добре оплачуваних молодих людей із міцним здоров'ям, які, нічим не ризикуючи, організовують «курс лікувального голодування» у якому-небудь публічному місці. Навколо цього ЗМІ підіймають неймовірний галас. Проти цього прийому встояти вкрай складно, тому що влада в будь-якому випадку змушена реагувати на висунуті «борцями» вимоги.

12. «Тримай злодія». Мета прийому – змішатися з переслідувачами.

Не має потреби детально зупинятися на досвіді Росії, інформаційний ресурс якої вже давно перетворено на потужну агітаційно-пропагандистську машину Кремля. Це, по-перше, «нацизм» – визначення просоюзних, прокомуністичних сил у колишньому СРСР протилежною стороною під гаслами: «Крим наш» та «Донбас наш». По-друге, представлення України та інших країн, як агресорів, які здійснюють геноцид російськомовного населення [8].

При цьому, слід враховувати, що характерною рисою сучасної цивілізації є її детермінованість інформаційним процесам. Потенційні можливості розвитку основних сфер життя сучасного суспільства, зокрема залежність від стану цих процесів. На сьогодні інформація вважається стратегічним національним ресурсом та засобом впливу на інші держави. Таку ситуацію важко було передбачити у попередні роки.

Впровадження сучасних засобів обробки і передачі інформації в різні сфери діяльності започаткувало новий еволюційний процес у розвитку суспільства – інформатизацію.

Під впливом інформатизації усі сфери життя суспільства набувають нових якостей – гнучкості, динамічності, але водночас зростає і потенційна вразливість суспільних процесів від інформаційного впливу [9].

Насамперед величезний потік інформації хлинув на людину, не даючи їй змоги сприйняти цю інформацію повною мірою. Внаслідок настає інформаційна криза або вибух, що має такі прояви:

– з'являються протиріччя між обмеженими можливостями людини щодо сприйняття та переробки інформації й існуючими потоками та чисельністю інформації, що зберігається. Наприклад, загальна кількість знань змінювалася спочатку дуже повільно, але вже з 1900 року вона подвоювалась вже кожні 50 років, з 1950 подвоєння відбувалося кожні 10 років, а з 1970 року – вже 5 років, з 1990 року – щорічно;

– існує чимало зайвої та шкідливої інформації, яка ускладнює сприйняття корисної для споживача інформації;

– виникають певні економічні, політичні й інші соціальні бар'єри, які перешкоджають поширенню інформації. Наприклад, через дотримання режиму таємності часто необхідною інформацією не можуть скористатися працівники інших відомств. Ці причини породили парадоксальну ситуацію: у світі накопичений великий інформаційний потенціал, але люди не можуть ним скористатися сповна через обмеження власних можливостей.

Стрімке зростання обсягів інформації й об'єктивна зміна умов психологічної діяльності людини в сучасному світі привели до перерозділу ваги даних про оточуючий світ, що надходить до індивіда за допомогою різних інформаційних шляхів і в результаті безпосереднього сприйняття дійсності на користь даних, які отримуються ним із ЗМІ.

Розвиток ЗМІ, інформаційних технологій та техніки з інформаційної безпеки обумовлює масштабність і результативність проведення інформаційних виливів. Поява технічних засобів нового покоління, що здатні ефективно впливати не тільки на психіку і свідомість людей та на нове покоління людства, але й на інформаційно-технічну інфраструктуру держав-супротивників, дала змогу вести інформаційну війну на якісно новому рівні, основними завданнями якої є:

– здійснення деструктивного ідеологічного впливу;

– створення атмосфери бездуховності, негативного ставлення до культури та дискредитація фактів історичної, національної самобутності народу противника чи ворога;

– маніпулювання громадською думкою з метою створення політичного напруження та стану, близького до хаосу;

– формування негативного іміджу держави на міжнародній арені;

– дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою розпалення конфліктів, стимулювання недовіри, загострення ворожнечі, боротьби за владу;

– зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень;

– провокування соціальних, політичних, національно-етнічних і релігійних зіткнень;

– створення чи посилення опозиційних угруповань чи рухів;

– зміна системи цінностей, які визначають спосіб життя і світогляд людей;

– формування передумов до економічної, духовної чи військової поразки, втрати волі до боротьби та перемоги;

– підрив морального духу населення і, як наслідок, зниження обороноздатності та бойового потенціалу.

При цьому необхідно зменшити вплив ЗМІ супротивника (на сьогодні це Росія, на наше суспільство) на суспільство супротивника.

Чого лише варті численні російські фільми та серіали, якими заповнені були телеекрани України, і нав'язували кремлівський «правильний» погляд на життя. Слід ще враховувати, що сьогодні на протидію російським ЗМІ Україна нічого не протиставляє. На окупованих територіях Донбасу та Криму немає достатнього обсягу радіомовлення та телемовлення з України. Також дуже мало інформації отримують закордонні слухачі.

Відмітимо, що телеканал Russia Today, який охоплює супутниковим мовленням територію практично усіх континентів, доступний у мережах кабельного телебачення у більшості країн Європи.

Професійні журналісти цього каналу із сучасних телестудій доброю англійською мовою несуть у широкі маси новини, коментарі, аналітику, подані, звичайно, у вигідному для Росії світі.

Повідомлення про вбивства у Росії правозахисників та журналістів, розгін демонстрацій демократичної опозиції чи дебоші неонацистів на екрані там не показують.

Цій пропаганді піддаються в Росії та світі не тільки звичайні люди, а й чимало тих, хто творить громадську думку і впливає на неї: зірки естради та кінематографу, бізнесмени, чиновники та ін. Російська пропаганда має на меті посилити свої моральні позиції, принижуючи українців. Відтак, ситуація складається не на користь для України. Адже росіяни, як це ми вже відмічали, висвітлюють події в Україні на користь собі, щоб завоювати якомога більшу частину прихильників так званих «ДНР», «ЛНР» і Криму . А це шлях до розколу країни та пряма загроза нашому іміджу в очах демократичного світу. Росіяни вміло маніпулюють українською аудиторією за допомогою ЗМІ та дезорієнтують суспільство. Російські журналісти сьогодні висвітлюють інформацію про Україну, ігноруючи принципи та етичні засади журналістики, оскільки застосовують прийоми дезінформації та викривлення інформації [10].

Вразливість українського медіапростору до інформаційної війни з боку Росії породжена такими причинами:

1. В Україні не контролюється виникнення нових електронних ресурсів. Відтак, чи не щодня з'являються нові Інтернет-медіа, спрямування яких досить часто має антиукраїнський, пропагандистський характер.

2. Вільне і досить активне проникнення в супутникові ЗМІ, соціальні мережі та електронну пошту пропагандистських матеріалів.

3. Україна не повною мірою може протистояти вірусам та шкідливому програмному забезпеченню, що розповсюджується російськими хакерами.

4. У Росії на відміну від України з'явилося чимало різноманітних розробок, спрямованих на пропаганду та маніпулювання свідомістю. Розвиток цієї сфери у нас на початковому рівні і немає ефективних засобів протидії агресивним сигналам, які використовує Росія.

5. Неналежною є підготовка фахівців до ведення інформаційної війни в ЗМІ. Українські вищі навчальні заходи не готують фахівців з кіберзахисту, а якщо у них навіть і є поодинокі спецкурси з таких дисциплін, то вони викладаються дуже поверхнево і в них мало уваги поділяють підготовці фахівців з технічного і криптографічного захисту інформації.

6. Немає відповідної джерельної бази, яка б надавала доступ до інформації про стратегію і тактику ведення інформаційної війни. Адже якщо проаналізувати наявність відповідної літератури, яка вийшла після часів Незалежної України, то її обмаль, а кількість фахівців з цього питання мізерна.

У світі останніх подій Україна не має достатніх засобів та ресурсів для ведення у «сучасному форматі» інформаційної війни (протидіяти її впливам).

У ході проведеного дослідження було сформовано рекомендації щодо протистояння у інформаційній війні, а саме:

1) підсилити державний контроль за інформаційним простором України;

2) більш оперативно координувати інформаційний вплив на вразливі елементи інформаційної системи противника;

3) розробити методи і засоби протистояння інформаційним акціям ворога для зменшення сфери його впливу;

4) використовувати комплексний підхід при формуванні стратегії інформаційної війни, тобто поєднувати суто інформаційні методи впливу з економічними, військовими, політичними і тощо.

Висновки

Аналіз факторів інформаційних впливів та протидії інформаційній зброї дозволяє зазначити наступне:

1. Проблеми інформаційної війни впливів з боку Росії проти України – питання надзвичайно гостре. На нашу думку, для того, щоб протидіяти російській інформаційній ескалації в Україні слід:

– підвищити ефективність політики інформаційної безпеки в галузі оборони, а відтак вдосконалити і посилити відповідні структури держави;

– перешкоджати маніпулятивним технологіям супротивника, які застосовують для впливу на суспільну свідомість;

– вдосконалювати методи протидії інформаційним впливам та захисту державних інформаційних ресурсів.

2. Українці не мають іншої альтернативи, ніж гідно і адекватно відповідати на інформаційні виклики сучасності. Бо лише так в умовах глобальних інформаційних впливів можна відстоювати власні інтереси.

Література

[1]. M. Libicki, Conquest in cyberspace. National security and information warfare, Cambridge, 2007, 207 p.

[2]. І. Іванченко, В. Хорошко, Ю. Хохлачова, Д. Чирков, Забезпечення інформаційної безпеки держави, К.: ПВП «Задруга», 2013, 170 с.

[3]. В. Балабін, І. Замаруєва, І. Пампуха, "Концептуальні засади захисту системи інформаційно-аналітичного забезпечення завдань інформаційної боротьби як складової воєнної безпеки", *Вісник КНУ ім. Тараса Шевченка*, №22, С. 30-33, 2009.

[4]. А. Рось, І. Замаруєва, В. Петров, "Концептуальні засади моделювання інформаційної боротьби", *Наука і оборона*, №2, С. 47-53, 2000.

[5]. С. Расторгуев, *Философия информационной войны,* М.: МПСИ, 2003, 496 с.

[6]. В. Хорошко, М. Шелест, "Кибертерроризм и информационная безопасность", *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*, Вип. 1(27), С. 9-14, 2014.

[7]. В. Хорошко, Ю. Хохлачова, М. Прокофьєв, "Концепція застосування інформаційних впливів та протидії інформаційній зброї", *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні*, Вип. 1(31), 2016. – С. 9-24.

[8]. Агитация и пропаганда по-украински. [Электронный ресурс]. Режим доступу: https://www.pravda.com.ua/rus/articles/2009/12/17/4544755.

[9]. В. Петрик, А. Кузьменко, В. Остроухов, *Соціально-правові основи інформаційної безпеки: навч посіб.,* К.: Росава, 2007, 496 с.

[10]. Н. Еляшевська, "Вразливість україни до інформаційної війни", *Теле- та радіожурналістика*, Вип. 14, С. 165–169, 2015.

УДК 355.405.1

Хорошко В., Хохлачева Ю. Информационная война. Защита от деструктивных информационно-психологических воздействий. Часть 2

Аннотация: *В ходе проведенного исследования были сформированы рекомендации по противостоянию информационной войне. Проведен анализ факторов информационных воздействий и противодействия информационному оружию, в результате которого указан ряд возможных действий для осуществления противодействия российской информационной эскалации в Украине с целью создания достойного и адекватного ответа на информационные вызовы современности. Предложен подход, который позволяет отстаивать собственные интересы и интересы государства в условиях глобальных информационных воздействий. Как показывает опыт последних вооруженных конфликтов одними из важнейших механизмов войны являются не только изменения в военном деле, но и информационная революция, которая находится в стадии формирования. Примером масштабного использования информационного оружия является информационная война, которая ведется Россией против Украины. Определений термина информационной войны сегодня есть множество, но в данной статье рассматривается определение, находящиеся в работах Мартина Либики «Что такое информационная война?». М. Либики также определил семь разновидностей информационной войны (командно-управленческая, хакерская, экономическая, психологическая, разведывательная, электронная и кибервойна) и четыре составляющие психологической войны (подрыв общественного духа, деморализация вооруженных сил, война культур, дезориентация командования). Обеспечение информационной безопасности в сфере государственного и муниципального управления основывается на детальном анализе структуры и содержания управления, а также информационных процессов и использования при управлении соответствующих технологий. При этом определяющими факторами при разработке средств информационного оружия становятся именно индивидуальные особенности человека и социума. Для того, чтобы смоделировать поведение человека (или общества), необходимо знать именно ее (его) индивидуальные особенности и преимущества. Сейчас уже понятно, что информационная борьба становится фактором, влияющим на саму войну, ее начало, ход и результат. Это подтверждается агрессией России против Украины. Поэтому, весьма актуальной проблемой безопасности Украины является разработка концепции защиты системы*

информационно-аналитического обеспечения задач информационной борьбы. В ходе проведенного исследования были сформированы рекомендации по противостоянию в информационной войне. А также проведен анализ факторов информационных воздействий и противодействия информационного оружия, который позволяет отметить, что нужно, по нашему мнению, для того, чтобы противодействовать российской информационной эскалации в Украине.
Ключевые слова: *информационная война, информационное воздействие, информационно-психологическое воздействие, информационное оружие, противодействие.*

Khoroshko V., Khokhlacheva Yu. Information war protection from destructive informational and psychological influences. Part 2

Abstract. *In the course of the research, recommendations were made on the confrontation with the information warfare. The analysis of the factors of informational influence and counteraction of information weapons was conducted, as a result of which a number of possible actions were taken to counter the Russian information escalation in Ukraine in order to create a decent and adequate response to the information challenges of our time. The approach, which allows to defend the interests and interests of the state in the conditions of global informational influences, is offered. As the experience of recent armed conflicts shows, one of the most important mechanisms of the war is not only changes in the military affair, but also the information revolution, which is now experiencing the stage of formation. An example of large-scale use of information weapons is the information warfare conducted by Russia against Ukraine. There are many definitions of the term of information warfare today, but this article deals with the definition that is contained in Martine Libiki's work «What is an information war?». M. Libiki also identified seven types of information warfare (command and control, hacking, economic, psychological, reconnaissance, electronic and cyberwar) and four components of psychological warfare (undermining of the public spirit, demoralization of the armed forces, war of cultures, disorientation of the command). The provision of information security in the field of state and municipal management is based on a detailed analysis of the structure and content of management, as well as information processes and use in the management of relevant technologies. At the same time, the defining factors in developing the means of information weapons are the individual characteristics of man and society. In order to simulate the behavior of a person (or society), it is necessary to know exactly its individual characteristics and advantages. It has now become clear that the information fight is becoming a factor affecting the very war itself, its beginning, course and outcome. This is confirmed by Russia's aggression against Ukraine. Therefore, a very urgent problem of Ukraine's security is the development of a concept for the protection of the information and analytical framework for information control tasks. In the course of the study, recommendations were drawn up on the confrontation in the information warfare. The analysis of the factors of informational influence and countermeasures of information weapons is also carried out, which allows us to indicate what we think in order to counter Russia's information escalation in Ukraine.*
Keywords: *information war, information influence, information and psychological influence, information weapon, counteraction.*

Отримано 25 *лютого 2019 року*, затверджено редколегією *19 березня 2019 року*