УДК 355.40:356.35

Фролов В. С., к.військ.н., с.н.с.;
Колесніков В. О., к.військ.н., професор

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Інформаційна безпека у воєнній сфері

Резюме. Стаття присвячена сучасним проблемам інформаційної боротьби. Аналізуються можливі варіанти протидії загрозам національній безпеці держави у інформаційному просторі.

Ключові слова: інформаційна війна, інформаційне суспільство, мережецентрична війна.

Постановка проблеми. У XXI столітті інформація стала виконувати одну з основних функцій інструменту війни. Для вирішення різних міждержавних та воєнних конфліктів все частіше використовується інформаційна сфера, що породжує такі явища як міждержавне інформаційне протиборство та мережеві війни, що характеризуються активним впливом на інформаційну сферу противника та прийняттям комплексу заходів для виявлення загроз та захисту своєї інформаційної інфраструктури від деструктивного втручання та кібервпливу.

"Гібридна війна", що розгорнута Російською Федерацією проти України, ведеться під прикриттям широкомасштабної інформаційної війни у світовому інформаційному просторі, тому проблеми підготовки та ведення інформаційних операцій привертає увагу наукових фахівців у сфері інформатики, кібернетики та воєнної політики.

Актуальність проблеми дослідження полягає у необхідності обґрунтування не тільки організації захисту вітчизняного інформаційного простору від зовнішніх загроз, але й проведення попереджувальних заходів впливу на інформаційний простір держави-противника та активний захист національних інтересів України у світовому інформаційному просторі.

Огляд останніх досліджень та публікацій. Аналіз поглядів деяких вітчизняних вчених на проблеми підготовки та ведення сучасних інформаційних війн підтверджує їх зосередженість у значній мірі на захисті національного інформаційного простору від зовнішніх та внутрішніх загроз національним інтересам України. Автори та розробники законодавчих актів щодо ведення інформаційної боротьби розглядали тільки одну сторону проблеми – інформаційну безпеку України, яка є частиною інформаційної війни та організовується для захисту національних інтересів держави. Проблемам активного впливу на інформаційний простір із метою упередження інформаційних атак противника, на наш погляд, приділяється недостатньо уваги дослідників.

Метою статті є обґрунтування деяких напрямів розвитку активної фази ведення інформаційної війни Україною у світовому інформаційному просторі.

Виклад основного матеріалу. Інформація – абстрактне поняття, що має різні значення залежно від контексту та походить від латинського слова «*information*», яке має декілька значень:

роз'яснення;
виклад фактів, подій;
витлумачення;
представлення, поняття;
ознайомлення, просвіта.

Іншими словами, інформація – це нові знання, які отримує споживач (суб'єкт) у результаті сприймання і переробки певних відомостей [2].

Інформація, яка циркулює в АСУ державного управління, оборони, економіки та фінансів, стає важливим державним ресурсом та все більше впливає на національну безпеку. Революційний розвиток комп'ютерних технологій та комунікативних систем обміну інформативними потоками, відкрив додаткові можливості для деструктивних дій на них з боку вороже налаштованих сил. Для збереження інформаційних потоків недоступними для ворога, у державі створюється система інформаційної безпеки, яка включає нормативно-правові акти, технічні системи контролю засобів передачі інформації тощо.

Інформація, що функціонує у воєнній сфері, використовується для аналізу загроз територіальній цілісності та прийняття рішення на застосування збройних угруповань та силових структур для її захисту.

На початку XXI-го століття у США була розроблена та успішно поширюється теорія

мережецентричних війн (*Networkcentricwor fare*) як спроба адаптувати воєнне мистецтво і воєнну стратегію до умов життєдіяльності сучасного суспільства. До активних співучасників розроблення концепції мережецентричних війн відносять віце-адмірала ВМС США А.Сербовскі та професора Дж. Гарстка.

Фахівці, які вивчають сучасну теорію мережевих війн стверджують, що сучасні конфлікти розгортаються у чотирьох суміжних областях: фізичній, інформаційній, когнітивній (пізнавальна активність людини, що пов'язана з придбанням, організацією і використанням знання) та соціальній (історичні, культурні, релігійні цінності, етнічні особливості тощо). При цьому інформаційна область в епоху мережевих війн є пріоритетною. Усі чотири області інтегруються і, таким чином формується єдина мережа, що є основою ведення мережецентричних воєнних дій.

Мережецентричні війни – війни нового покоління, базуються на мережевих політтехнологіях – методиках оволодіння та використання інформації з метою підвищення швидкості управління.

Під швидкістю управління американські військові експерти розуміють три аспекти:

1. Війська досягають інформаційної переваги, під якою розуміється не отримання інформації у великій кількості, а більш висока ступінь усвідомлення та більш глибоке розуміння ситуації на полі бою. У технологічному плані усе це передбачає впровадження нових систем управління, розвідки, контролю, комп'ютерного моделювання тощо.

2. Війська, маючи інформаційну перевагу, впроваджують у життя принцип масованих результатів інформаційного впливу на особовий склад, а не масування засобів ураження для досягнення перемоги над противником.

3. Противник не має можливості проводити буду-яку активну протидію і впадає у стан шоку.

Мережецентричну війну можна представити у вигляді трьох підсистем, які переплітаються та тісно пов'язані між собою:

– інформаційної;

– сенсорної (розвідувальної);

– бойової.

Основу мережецентричної війни складає інформаційна підсистема, об'єктами якої є – політичне керівництво держави; персонал, який обслуговує систему життєзабезпечення та інфраструктуру; населення; збройні сили та система внутрішньої безпеки. Інформаційна підсистема мережецентричної війни є основним пріоритетом з усіх об'єктів ураження.

В інформаційній підсистемі мережецентричної війни поняття "інформація" розглядається як обсяг та зміст необхідних відомостей щодо противника, своїх військ, населення, інфраструктури населених пунктів, місцевості, погодних умов тощо та використовується військовим командуванням у ході розробки та прийняття рішень на застосування та всебічне забезпечення військ (сил). З метою введення противника в оману командири та штаби намагаються приховувати реальні відомості про стан своїх військ, систему управління та всебічного забезпечення, іншими словами – замаскувати реальний зміст інформації від противника.

На оперативному та стратегічному рівнях керівництвом Міністерства оборони та збройних сил плануються інформаційні операції, цілями яких ставиться порушення системи військового управління противника на всіх рівнях та підвищення ефективності застосування засобів ураження у "гарячій війні" з мінімальними збитками своїх військ.

Інформаційні операції у мережецентричних війнах відносяться до сфери оборони держави, плануються Міністерством оборони та керівництвом Генерального штабу в умовах ведення "гібридної" або "гарячої війни". Одночасно політтехнологи ведуть масовані та скоординовані заходи інформаційної війни, мета яких – деморалізація населення, паніка та шок, дезорганізація системи державного управління, компрометація влади держави-агресора тощо. Будь-які інші інформаційні заходи у сферах національної безпеки держави проводяться у відповідності до мети, змісту та завдань інформаційної війни, що ведеться проти держави-противника.

За словами французького генерала Пінателя, із приходом інформаційної ери область застосування стратегії еволюціонує від реального до віртуального: «Мова не йде більше про те, щоб готуватись вести війну, а про те, щоб готуватись її уникати, безперервно відновлюючи глобальний ефект залякування» [1].

Інформаційна війна – це війна з метою захоплення сировинних, енергетичних, людських ресурсів іншої держави, із використанням такого впливу на розум людей у сфері ідеології, релігії, політики, історії, філософії, науки, коли населенню держави – жертви агресії, цілеспрямовано впроваджуються такі неправдиві представлення про те, що відбувається у суспільстві, у житті людей, які дозволяють

агресору вільно маніпулювати як владою, так і народом цієї держави, практично без будь-якого спротиву та збройного вторгнення.

В інформаційній війні під "інформацією" розуміється "результат відображення та обробки в людській свідомості різноманіття навколишнього світу, відомостей про предмети, що оточують людину, явища природи, діяльність інших людей тощо" [3].

За визначенням відомого російського експерта А. Іларіонова, інформаційна війна характеризується перш за все наявністю інформаційної агресії, інформаційних битв, інформаційних фронтів, використанням інформаційної зброї. У інформаційній війні апелюють такими поняттями, як інформаційний напад та інформаційна оборона, інформаційні атаки та інформаційний опір, інформаційний наступ та інформаційний супротив, інформаційні противники та інформаційні союзники, інформаційні перемоги та інформаційні поразки, інформаційні війська та жертви інформаційної війни, інформаційний тероризм, інформаційні спецоперації та інформаційний спецназ, інформаційні блокади та театри інформаційних бойових дій.

За метою та способами ведення інформаційні війни поділяються на два покоління.

До *першого* покоління інформаційних війн відносяться:

–вогневе придушення елементів військового управління;

– ведення радіоелектронної боротьби;

– добування розвідувальної інформації;

– здійснення несанкціонованого доступу до інформаційних ресурсів з метою їх викрадення чи фальсифікації;

– масове подання в інформаційних каналах дезінформації для впливу на осіб, що приймають рішення;

– отримання інформації від перехоплених джерел.

До *другого* покоління відносяться:

– створення атмосфери бездуховності і аморальності у суспільстві;

– маніпулювання суспільною свідомі-стю соціальних груп населення;

– дестабілізація політичних відносин між політичними силами з метою провокації конфліктів;

– зниження рівня інформаційного за без-печення влади;

– дезінформація населення та підрив авторитету влади;

– підрив міжнародного авторитету держави;

– нанесення збитку державі у політичній, економічній, оборонній та інших сферах національної безпеки.

Активні процеси інформатизації через масове впровадження нових інформаційних та телекомунікаційних технологій в усі сфери життя зумовило формування нової історичної фази розвитку цивілізації – *інформаційного суспільства*, у якому головним продуктом виробництва є інформація.

В інформаційному суспільстві найбільш ефективними стають *латентні* (скриті) форми ведення інформаційної війни, у яких використовуються різні форми маніпуляцій суспільною свідомістю.

Маніпуляція свідомістю стає основою технологій латентної інформаційної війни – війни нового типу, у якій використовується інформаційний вплив на людську свідомість на рівнях: індивідуальної свідомості (мікрорівень), суспільної свідомості нації (макрорівень) та у масштабах усього людства (мегарівень).

Інформаційні війни потребують нових методів та форм організації системи інформаційної безпеки держави. Відомчі вертикальні структури, що традиційно відповідають за безпеку держави, уже багаторазово підтвердили їх неефективність. Аналіз ведення сучасних інформаційних війн підтверджує невисоку ефективність планування та організацію інформаційних операцій (заходів протидії) у межах однієї сфери національної безпеки. Плануючи інформаційну операцію на визначеній території, звужується та обмежується обсяг інформації, що необхідний для впливу на всі верстви населення регіону, де ведуться бойові дії.

На наш погляд, інформаційну безпеку держави у воєнній сфері слід розглядати у контексті інформаційної війни, що ведеться в інформаційному просторі в усіх сферах національної безпеки держави.

У нових умовах ведення інформаційної війни важливо створювати міжвідомчі постійно діючі або тимчасові структури (*task team*) із широкими повноваженнями для формування системних інформаційних програм та блискавичного проведення інформаційних операцій або відбиття інформаційних атак.

Способи та методи ведення інформаційної війни швидко розвиваються та удосконалюються, тому затримка у створенні сучасної, адекватної системи протидії загрозам в інформаційній сфері дає противнику повну ініціативу та значні переваги в оволодінні свідомістю суспільства.

Загрози національним інтересам в інформаційному просторі виникають як ззовні (зовнішні), так і у середині держави (внутрішні).

Формуючи та організовуючи комплекс інформаційних заходів, вороже налаштовані держави намагаються максимально оволодіти сферою впливу на суспільство, захоплюючи вільний простір в інформаційному полі.

На підставі критеріїв інформаційної безпеки, з метою максимального ослаблення інформаційної агресії противника на сфери національної безпеки держави, створена система захисту інформаційного простору (рис. 1).

Стрімкий розвиток технічних засобів передачі інформації (Інтернет, супутникове телебачення, комп'ютерні системи тощо) ускладнює надійний захист інформаційного поля від агресивних дій противника. Досвід останніх років підтверджує, що без чітко спланованої, комплексної, активної боротьби в усіх видах інформаційної війни, неможливо досягти надійного функціонування системи інформаційної безпеки держави та оволодівати сферами впливу в інформаційному полі.

На рис.1 відображено принципову схему протидії загрозам в інформаційному просторі. Існуюча система інформаційної безпеки держави дещо стримує негативний вплив держави-агресора на інформаційне поле України.

У той же час відсутність системи активної боротьби за оволодіння сферами впливу в інформаційному просторі зводить нанівець усі зусилля системи інформаційної безпеки держави. Пасивна позиція, при якій використовуються тільки захисні механізми проти існуючих загроз в інформаційній сфері, не може бути ефективною та у повній мірі захистити національні інтереси держави. Як варіант, на схемі показано перелік заходів, що спрямовані на активний інформаційний вплив на свідомість суспільства держави-агресора та України з метою роз'яснення об'єктивних причин воєнного протистояння, упередження у наданні правдивої інформації про наслідки бойових дій, розкриття агресивних планів керівництва сусідньої держави щодо порушення територіальної цілісності України, обнародування фактів безпосередньої участі військових підрозділів держави-агресора у веденні бойових дій, надання озброєння та всебічного забезпечення терористичних бандформувань тощо. Слід підкреслити, що інформаційну боротьбу усіх сфер національної безпеки держави слід об'єднати під єдине керівництво з метою організації, планування та ефективного ведення інформаційних операцій.

Засоби та методи ведення інформаційної війни швидко розвиваються та удосконалюються, тому затримка у створенні сучасної, адекватної системи протидії загрозам в інформаційній сфері дає противнику повну ініціативу та значні переваги в оволодінні свідомістю суспільства.

Висновки

1.Запропонований варіант активних заходів держави в інформаційній сфері дасть змогу підвищити ефективність інформаційної безпеки України та суттєво знизити вплив держави-агресора на свідомість суспільства.

2. Практична реалізація запропонованої схеми інформаційної протидії противнику можлива після конкретизації заходів кожної сфери національної безпеки в інформаційному просторі, що є предметом **подальших досліджень**.

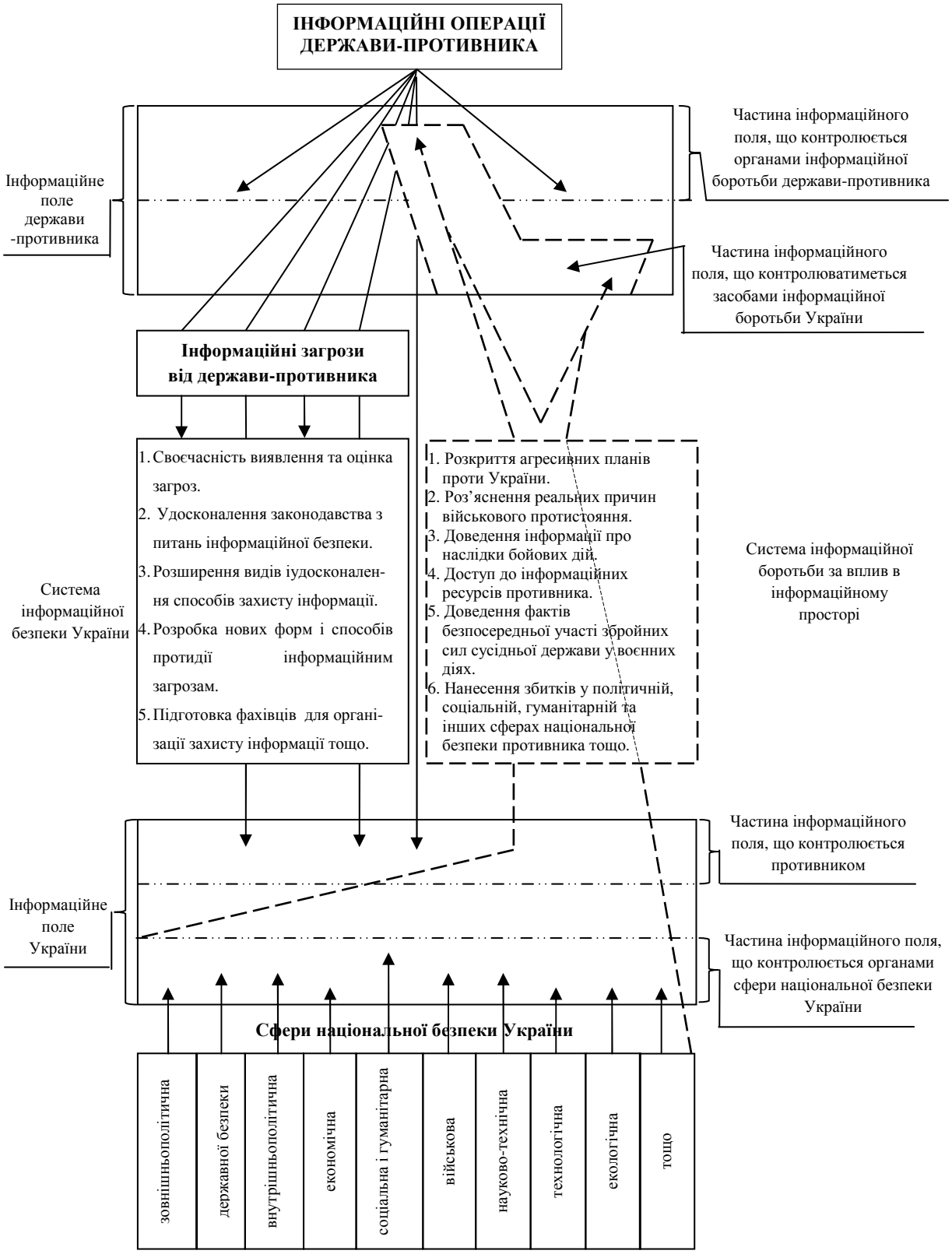

Рис. 1. Принципова схема протидії загрозам в інформаційному просторі

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Virieu F/ H/ La Madiacrafie. P.; Flammarion, 1990. – С. 109
2.Великий тлумачний словник сучасної української мови. www.lingvo.ua/uk-uk/інформація.
3.Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников– М.: Финансы и статистика, 1997.
4.Присяжнюк М., Жарков Я. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування // Центр воєнної політики та політики безпеки: http:// defpol. org. ua, (10 серпня 2009).
5.Почепцов Г.Г. Інформаційні війни. М.: ВЦ Гарант, 2008, – 453 с.
6.Афанасьєв В. Соціальна інформація та управління суспільством. – М.: Знание, 2005, – 119 с.

Стаття надійшла до редакції 12.02.2015

Фролов В. С.,
Колесников В. А.
Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Информационная безопасность в военной сфере

Резюме. Статья посвящена современным проблемам информационной борьбы. Анализируются возможные варианты противодействия угрозам национальной безопасности государства в информационном пространстве.

Ключевые слова:. информационная война, информационное общество, сетецентрическая война.

V. Frolov,
V. Kolesnikov
Center for Military and Strategic Studies National Defence University of Ukraine named Ivan Chernyhovskij

Information security in defense sector

Resume. This article is devoted to the contemporary problems of information warfare. We analyzed possible options for countering threats to national security in information space

Keywords: information warfare, information society, network-centric warfare.