УДК 354.42

О.М. Косогов

Військова частина А1906

ІНФОРМАЦІЙНА БЕЗПЕКА У СФЕРІ ОБОРОНИ ЯК СКЛАДОВА ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

На основі аналізу ролі та місця інформаційної безпеки держави визначено основні напрями забезпечення інформаційної складової воєнноїбезпеки. Зазначено, що активне розроблення інформаційної зброї і підготовка до інформаційних кампаній багато в чому визначаються поглядами розвинутих країн на цілі, умови, форми і наслідки застосування воєнної сили. Визначено інформаційну безпеку держави як невід'ємну складову воєнної безпеки.

Ключові слова: *інформаційна безпека, воєнна безпека, інформаційна зброя, державні органи.*

Вступ

Постановка проблеми. Аналіз літератури. На сьогодні інформаційна боротьба стає однією з важливих, а не рідко й основних форм вирішення суперечностей між державами, і в цій боротьбі шляхом проведення інформаційних операцій досягаються стратегічні цілі [1 – 4].

В умовах перманентного інформаційного протиборства у світі стрімко зростає рівень та значно розширюється спектр інформаційних загроз. Така ситуація становить серйозну небезпеку національній і міжнародній безпеці та призводить до важкопрогнозованих і часом непередбачуваних наслідків у воєнно-політичній, економічній, військово-технічній, екологічній та інформаційній сферах.

Не залишається осторонь світових тенденцій і Україна, яка, з огляду на своє геополітичне положення, існуючу навколо неї воєнно-політичну обстановку та наявність досить розвинутої інформаційної інфраструктури, перебуває під потужним іноземним інформаційним впливом. Маючи системний і цілеспрямований характер, у підсумку зовнішній негативний інформаційний вплив призводить до появи загроз національній безпеці України в інформаційній сфері, які завдають державі відчутних збитків.

Особливо це стосується виконання завдань оборони країни, оскільки ця діяльність безпосередньо спрямована на захист національних інтересів держави від зовнішніх загроз і пов'язана з підготовкою та веденням війни з можливим агресором.

Метою статті є визначення ролі та місця інформаційної безпеки в системі воєнної безпеки держави, виявити характерні особливості забезпечення інформаційної безпеки держави у воєнній сфері.

Основний матеріал

Активне розроблення інформаційної зброї і підготовка до інформаційних війн багато в чому визначаються поглядами розвинутих країн на цілі, умови, форми і наслідки застосування воєнної сили.

Становлення в розвинутих демократичних країнах громадянського суспільства як важливої соціально-політичної сили, яка здійснює суспільний контроль над владою, стимулювало формування нової системи цінностей, в якій ключове значення має життя людини, її права і безпека. Розвиток громадянського суспільства має стійку, незворотну тенденцію до поглиблення і розповсюдження на все більш широке коло країн. Для громадянського суспільства неприйнятний воєнний шлях розв'язання зовнішньополітичних проблем, якщо бойові дії пов'язані зі значними людськими втратами, якщо тільки не виникає загрози існуванню суспільства. Використовувати ж воєнну силу в ситуаціях, які не загрожують існуванню цих країн, стає все більш складніше по мірі розвитку громадянського суспільства.

Досвід воєнних конфліктів в останнє десятиріччя свідчить про те, що рівень допустимих для демократичних країн втрат становить сьогодні десятки, якщо не одиниці людських життів і це стає одним з найважливіших факторів стримування цих країн від застосування воєнної сили.

Подальша, глобалізація, і, особливо, зростаючий збіг економічних і політичних інтересів розвинених демократичних країн, виключають воєнні конфлікти між ними. Їхні загальні інтереси вимагають, крім усього іншого, надійного забезпечення безпеки кожного члена "клуба" і можливості спільного вирішення гострих світових проблем, у тому числі з застосуванням сили. Це завдання виконують воєнні союзи цих країн, у яких рішення приймаються за принципом консенсусу. У цих умовах без підтримки суспільної думки країн-учасниць союзу неможливе вирішення будь-яких проблем воєнним шляхом. Ця обставина різко знижує можливості воєнних організацій союзів розвинених демократичних країн в операціях, які не торкаються безпосере-

дньо їхньої безпеки. Тому основними засобами вирішення гострих політичних проблем стали економічна і культурна експансії, міжнародні економічні і політичні санкції, й у крайніх випадках – загроза застосування сили там, де це не загрожує серйозними людськими втратами по обидва боки. У цих умовах інформаційна зброя може стати дуже ефективним силовим засобом, що дозволяє вирішувати багато конфліктів без застосування традиційних засобів збройної боротьби.

Ці тенденції розвиваються на фоні зростання уразливості промислової, інформаційної, соціальної і воєнної інфраструктури розвинених країн. Руйнування в результаті бойових дій атомних електростанцій, хімічних підприємств й інших критичних об'єктів може призвести до регіональних і навіть глобальних катастроф, чреватих колосальними людськими і матеріальними втратами, що ставить під загрозу саме існування цих країн. Порушення їхньої інформаційної інфраструктури також призведе до техногенних і економічних катастроф, оскільки управління всіма найважливішими об'єктами народного господарства, соціальної і воєнної сфери розвинених країн засновано на широкому використанні інформаційно-комунікаційних технологій. Подальший розвиток інформаційно-комунікаційної сфери і поглиблення глобалізації робить світ ще більш уразливим.

Нарешті, інформаційно-технічний прогрес у воєнній справі створює умови для прискореного удосконалювання озброєння і військової техніки на основі широкого впровадження нових інформаційних технологій і створення зброї на нових фізичних принципах, інформаційної і нелетальної зброї. Основними особливостями нового покоління озброєнь стають кардинальне збільшення точності, дальності і потужності дії, різке збільшення можливостей розвідки, систем збору й обробки інформації і, як наслідок, зменшення часу прийняття оперативних рішень. Країни, які володіють такою зброєю і військовою технікою, одержують величезну воєнну перевагу перед супротивником, оснащеним традиційними типами озброєнь.

Наведені тенденції, по суті, і визначають припустимі межі й умови застосування сили розвиненими країнами і можливі типи конфліктів, що можуть бути для них прийнятні.

Безпосередньо у військовій справі рівень інформаційного потенціалу все більшою мірою обумовлює оперативність прийняття рішень, структуру і якість озброєнь, оцінку рівня їх достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в підсумку, результат збройного протистояння.

Значущість інформаційної безпеки як складової воєнної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз важливим національним інтересам України у воєнній сфері випливає, що реалізаційною основою більшості цих загроз є інформаційна [5].

З-поміж інших загроз стабілізації воєнно-політичної обстановки та недопущення збройних конфліктів в Центральній Європі розглядаються такі:

висунення територіальних претензій до України;

втручання у внутрішні справи України;

нестабільність воєнно-політичної обстановки навколо України;

активізація сепаратистських сил і підтримання їх ззовні; заяви та акції, що дискредитують внутрішню і зовнішню політику України;

войовничість політичного керівництва сусідніх країн;

загострення міжетнічних і міжконфесійних суперечностей;

нестабільність соціально-політичної обстановки в суміжних з Україною країн.

Не виникає сумніву в тому, що всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні, причому їх інформаційна складова досить вагома.

Крім того, за оцінками вітчизняних експертів з проблем інформаційної безпеки [611], що сформовані на основі аналізу іноземного впливу на інформаційний медіа – і кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції:

цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;

активізація критики вищого державного керівництва України;

здійснення рядом зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо- та зовнішньополітичній сферах;

посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі;

дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;

зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї.

Однією з істотних загроз підтримуванню боєздатності формувань Воєнної організації є втрата престижності воєнної служби і зниження морально-психологічного рівня особового складу. Ця загроза має інформаційний характер.

Такі загрози розвитку вітчизняної воєнної науки, як зниження вимог до неї, послаблення уваги до розвитку сучасного воєнного мистецтва, відставання в розробленні критичних технологій і технологій подвійного призначення та послаблення контролю за системою підготовки наукових кадрів мають суто інформаційний характер.

Слід зазначити, що йдеться не про абсолютизацію інформаційних факторів у реалізації наведених загроз, а про те, що вони, поряд з економічними, політичними, соціальними та іншими факторами, є домінуючими. Тому ефективність своєчасного виявлення та нейтралізації розглянутих загроз національній безпеці у воєнній сфері істотно залежить від виваженості й активності заходів щодо забезпечення воєнної безпеки на інформаційному рівні.

Висновки

Таким чином, забезпечення інформаційної безпеки держави є проблемою високої складності та потребує комплексного підходу.

Тому для ефективного функціонування системи воєнної безпеки України сукупність зазначених організаційно-технологічних та організаційно-правових заходів слід поєднати в систему управління інформаційною безпекою в межах забезпечення воєнної безпеки України..

Відповідно до теоретичних розробок спеціалістів у галузі інформаційної безпеки, основними напрямами забезпечення інформаційної безпеки є правовий, організаційний, інженерно-технічний. Застосування всіх цих напрямів є необхідним для формування комплексної воєнної безпеки держави.

Список літератури

1. Киселев В.Д. Современные проблемы защиты в системах ее передачи и обработки / В.Д. Киселев, О.В. Есиков, А.С. Кислицын. Под ред. Е.М. Сухарева. – М.: Солид, 2000. – 200 с.

2. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф. Шаньгин, А.В. Соколов. – М.: ДМК, 2002. – 134 с.

3. Гарбарчук В. Кибернетический подход к проектированию систем защиты информации / В. Гарбарчук, З. Зинович, А. Свиц. Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки; Люблинский политехнический ун-т. – К.; Луцк; Люблин, 2003. – 658 с.

4. Маслова Н.А. Построение модели защиты информации с заданными характеристиками качества / Н.А. Маслова // Штучний інтелект. – Донецьк : ІШІ, 2007. – № 1. – С. 51-57.

5. Косогов О.М. Модель динаміки зміни рівня інформаційної безпеки системи / О.М. Косогов // Зб. наук. праць. – К.: ЦВСД НУО імені І. Черняховського, 2015. – №2 (54). – С. 76-79.

6. Пєвцов Г.В. Концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері / Г.В. Пєвцов, С.В. Залкін, А.О. Феклістов // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 2 (92). – С. 57-59.

7. Власюк О.С. Можливості застосування аналітичного планування для обґрунтування та підготовки рішень на вищих рівнях управління / О.С. Власюк. – К.: НІСД, вип. 47, серія наукові доповіді, 1996. – 71 с.

8. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: монографія / А.І. Семенченко. – К.:Вид-во НАДУ, 2008. – 428 с.

9. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О.М. Косогов // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: Харківський університет Повітряних Сил імені І. Кожедуба, 2014. – Вип. 3 (40). – С. 127-129

10. Асанович В.Я. Информационная безопасность: анализ и прогноз информационного воздействия / В.Я. Асанович, Г.Г. Маньшин. – Мн.: Амалфея, 2006. – 204 с.

11. Кормич Б.А. Інформаційна безпека: організаційно-правові основи / Б.А. Кормич. –К. : Кондор, 2003. – 384 с.

Надійшла до редколегії 29.04.2016

Рецензент: д-р техн. наук, проф. О.Б. Леонтьєв, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ОБОРОНЫ КАК СОСТАВЛЯЮЩАЯ ВОЕННОЙ БЕЗОПАСНОСТИ УКРАИНЫ

А.Н. Косогов

На основе анализа роли и места информационной безопасности государства определены основные направления обеспечения информационной составляющей военной безопасности. Отмечено, что активное разрабатывание информационного оружия и подготовка к информационным кампаниям во многом определяются взглядами развитых стран на цели, условия, формы и последствия применения военной силы. Определена информационная безопасность государства как неотъемлемая составляющая военной безопасности.

Ключевые слова: *информационная безопасность, военная безопасность, информационное оружие, государственные органы.*

INFORMATIVE SECURITY IN THE FIELD OF DEFENSIVE AS CONSTITUENT OF MILITARY SECURITY OF UKRAINE

O.M. Kosogov

On the basis of analysis of role and place of informative security of the state basic directions of providing the informative constituent of military security are certain. It is marked that active development of informative weapon and preparation to the informative campaigns are in a great deal determined by the looks of the developed countries to the aims, terms, forms and consequences of application of military force. Informative security of the state as inalienable constituent of military security is certain.

Keywords: *informative security, military security, informative weapon, public organs.*