УДК 621.391

Г.В. Пєвцов, С.В. Залкин, А.О. Феклістов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

КОНЦЕПТУАЛЬНІ ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ВОЄННІЙ СФЕРІ

Розглядаються концептуальні положення щодо забезпечення інформаційної безпеки у воєнній сфері: визначення та правові основи Концепції інформаційної безпеки у воєнній сфері, принципи, основні цілі, завдання, об'єкти, суб'єкти, реальні та потенційні загрози, напрями, методи та заходи забезпечення інформаційної безпеки у воєнній сфері.

Ключові слова: *інформаційна безпека, концепція інформаційної безпеки, воєнна сфера.*

Вступ

Постановка проблеми у загальному вигляді. Сучасні зміни міжнародної обстановки, що відбуваються у світі, значно впливають на погляди у галузі управління державними системами безпеки та оборони щодо характеру загроз безпеці, шляхів їх своєчасного виявлення, запобігання та нейтралізації [1].

На даний час інформаційний вплив, розглядається розвиненими країнами як найбільш ефективний засіб забезпечення своїх національних інтересів. Україна у сучасних умовах є одночасно об'єктом і суб'єктом інформаційного впливу, який обумовлений її геополітичним положенням і наявністю політичних, економічних та інших інтересів щодо нашої держави з боку розвинених країн та сусідніх держав.

Таким чином, проблеми забезпечення інформаційної безпеки національних інтересів у будь-якій сфері набувають великої значущості [1 - 20].

Одним з актуальним напрямків вирішення даних проблем є визначення концептуальних підходів щодо забезпечення інформаційної безпеки у воєнній сфері.

Мета статті – визначення концептуальних підходів щодо забезпечення інформаційної безпеки у воєнній сфері.

Викладення матеріалів досліджень

Основним офіційним документом, в якому повинні бути сформульовані концептуальні підходи щодо забезпечення інформаційної безпеки у воєнній сфері, є Концепція інформаційної безпеки у воєнній сфері (далі – Концепція), яка представляє собою систему офіційно прийнятих державою поглядів на цілі, завдання і принципи забезпечення інформаційної безпеки у воєнній сфері. В ній повинні бути визначені об'єкти та суб'єкти інформаційної безпеки у воєнній сфері, загрози та можливі їх джерела , напрями і методи запобігання и нейтралізації цих загроз, а також заходи забезпечення інформаційної безпеки у воєнній сфері.

Правовою основою Концепції повинні бути Закони України "Про основи національної безпеки України", "Про інформацію" та Указ Президента України "Про Доктрину інформаційної безпеки України" [20].

Концепція повинна бути складовою Концепції національної безпеки України і основою для: формування і проведення державної інформаційної політики, розробки і проведення заходів щодо забезпечення інформаційної безпеки у воєнній сфері; гармонізації законодавства щодо забезпечення інформаційної безпеки у воєнній сфері; підготовки пропозицій для формування й удосконалення інформаційних відносин суб'єктів інформаційної безпеки у воєнній сфері; розробки державних цільових програм створення і розвитку інформаційних технологій, інформаційних ресурсів й інформаційної інфраструктури у воєнній сфері.

Забезпечення інформаційної безпеки у воєнній сфері має здійснюватися за наступними принципами: конфіденційності, цілісності та доступності інформації; обмеження доступу до інформації виключно на підставі нормативно-правових актів; запобігання правопорушенням в інформаційній сфері; своєчасності й адекватності заходів захисту інформаційних ресурсів реальним і потенційним загрозам; чіткого розмежування повноважень та взаємодії органів управління різних ланок у забезпеченні інформаційної безпеки; пріоритетності національних інформаційних систем та технологій.

Основними цілями забезпечення інформаційної безпеки у воєнній сфері мають бути:

захист інформаційного середовища, інформаційного потенціалу та інформаційних технологій, що складають державну таємницю або конференційну інформацію;

запобігання, локалізація і нейтралізація реальних та потенційних загроз інформаційній безпеці у воєнній сфері;

протидія від негативного інформаційно-психологічного впливу для захисту здоров'я і психіки особового складу.

Основними завданнями забезпечення інформаційної безпеки у воєнній сфері мають бути: створення нормативно-правової бази щодо забезпечення інформаційної безпеки у воєнній сфері; створення системи інформаційної безпеки у воєнній сфері; забезпечення безпеки інформаційно-телекомунікаційних мереж та систем; виявлення, оцінка та прогнозування рівня загроз інформаційній безпеці у воєнній сфері; організація антивірусного захисту інформаційного потенціалу і сертифікація інформаційних процесів, програм та засобів, які використовуються в інтересах забезпечення інформаційної безпеки у воєнній сфері; ліцензування діяльності будь-яких органів з проведення робіт, пов'язаних із використанням таємної інформації та інформації з обмеженим доступом, а також з створенням засобів захисту інформації; захист інформації від витоку по каналам зв'язку; регламентація порядку і правил використання технічних засобів передачі та обробки інформації у воєнній сфері; захист інформаційних систем і засобів зв'язку від вогневого ураження противника; створення державної системи протидії внутрішнім і зовнішнім загрозам національної безпеки України кібернетичного характеру у воєнній сфері.

До об'єктів забезпечення інформаційної безпеки (об'єктів, на яких необхідно передбачати заходи запобігання або ліквідації загроз в інформаційній сфері) слід віднести: інформаційні системи та системи і засоби управління військами і зброєю; інформаційні процеси, ресурси та інфраструктура, що використовуються у воєнній сфері; система формування, розповсюдження і використання інформаційних процесів, що використовуються у воєнній сфері; інформаційні технології військового та подвійного призначення, системи і засоби захисту інформації, що використовуються у воєнній сфері; виробничі підприємства і науково-дослідні установи, які займаються оборонною проблематикою в інтересах України; озброєння, військова техніка і військові об'єкти, які мають параметри (характеристики), що охороняються; морально-психологічний стан особового складу військових формувань.

Суб'єктами інформаційної безпеки у воєнній сфері є військовослужбовці та працівники Збройних Сил (ЗС) України, підрозділи, військові частини та з'єднання ЗС України, органи державного і військового управління, підприємства оборонно-промислового і наукового комплексів.

На сучасному етапі основними реальними та потенційними загрозами інформаційній безпеці України у воєнній сфері є: порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України; несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони; реалізація програмно-математичних засобів з метою порушення функціонування інформаційних систем у сфері оборони України; перехоплення та знищення інформації в інформаційно-телекомунікаційних системах та мережах, радіоелектронне подавлення засобів зв'язку та управління; інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби.

Основними напрямами забезпечення інформаційної безпеки у воєнній сфері є:

концептуальні, що включають визначення цілей та практичних завдань забезпечення інформаційної безпеки у воєнній сфері;

організаційні, що пов'язані з необхідністю формування оптимальної структури і складу функціонуючих органів системи інформаційної безпеки у воєнній сфері та координацією їх взаємодії, удосконаленням прийомів і способів стратегічного та оперативного маскування й дезінформації, розвідки і радіоелектронної боротьби, методів і засобів активної протидії негативному інформаційно-психологічному впливу;

технічні, що характеризуються постійним удосконаленням засобів захисту інформаційних ресурсів від несанкціонованого доступу, розвитком захищеності систем зв'язку, у тому числі систем зв'язку і управління військами і зброєю, підвищенням надійності спеціального програмного забезпечення, а також підвищення ефективності захисту інформації про розробку, створення і технічні характеристики озброєння та військової техніки.

Для запобігання і нейтралізації загроз інформаційній безпеці слід використовувати правові, організаційні, програмно-технічні і економічні методи.

З метою забезпечення інформаційної безпеки у воєнній сфері необхідне проведення наступних заходів: проведення систематичного аналізу застосування засобів, форм та способів інформаційної боротьби у воєнній сфері, визначення напрямів забезпечення інформаційної безпеки держави; удосконалення законодавства з питань інформаційної безпеки, координації діяльності органів державної влади та органів військового управління під час вирішення завдань забезпечення інформаційної безпеки; удосконалення видів і засобів захисту інформації в інформаційно-телекомунікаційних мережах, що задіяні в управлінні військами і зброєю, від несанкціонованого доступу; удосконалення форм і способів про-

тидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності держави; підготовка спеціалістів з питань інформаційної безпеки у воєнній сфері.

Висновки

Визначені наступні концептуальні положення щодо забезпечення інформаційної безпеки у воєнній сфері: визначення та правові основи Концепції інформаційної безпеки у воєнній сфері, принципи, основні цілі, завдання, об'єкти, суб'єкти, основні реальні та потенційні загрози, напрями, методи та заходи забезпечення інформаційної безпеки у воєнній сфері.

Запропоновані концептуальні положення практично реалізовані під час розробки пропозицій до проекту Концепції забезпечення інформаційної безпеки у воєнній сфері.

Список літератури

1. Основи стратегії національної безпеки та оборони держави: підр. / В.Г.Радецький, О.П.Дузь-Крятченко, В.М.Воробйов та ін. – К.: НУОУ, 2009. – 596 с.

2. Інформаційна безпека держави у контексті протидії інформаційним війнам: навчальний посібник / В.Б. Толубко та ін. – Київ, НАОУ, 2003. – 340 с.

3. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): монографія / В.Б. Толубко. – К.: НАОУ, 2003. – 315 с.

4. Руснак І.С. Розвиток форм і способів ведення інформаційної боротьби на сучасному етапі / І.С. Руснак, В.М. Телелим // Наука і оборона. – 2000. – № 2. – С. 18-23.

5. Рось А.О. Концептуальні засади моделювання інформаційної боротьби / А.О. Рось, І.В. Замаруєва, В.Л. Петров // Наука і оборона. – 2000. – № 2. – С. 46-53.

6. Замаруєва І.В. Державне та військове управління як об'єкт інформаційної боротьби / І.В. Замаруєва, С.В. Лєнков, А.О. Рось // Наука і оборона. – 2007. – № 3. – С. 28-34.

7. Толубко В.Б. Складові інформаційної боротьби / В.Б. Толубко, А.О. Рось // Наука і оборона. – 2002. – № 2. – С. 23-28.

8. Толубко В.Б. Концептуальні основи інформаційної безпеки України / В.Б. Толубко, С.Я. Жук, В.О. Косевцов // Наука і оборона. – 2004. –- № 2. – С. 19-25.

9. Жук С.Я. Тенденції та перспективи розвитку інформаційної боротьби й інформаційної зброї / С.Я. Жук, В.О. Чмельов, Т.М. Дзюба // Наука і оборона. – 2006. – № 2. – С. 35-41.

10. Фомін В.О. Інформаційна боротьба в підготовці воєнного конфлікту та запобіганні йому і стримуванні / В.О. Фомін, С.Я. Жук // Наука і оборона. – 2004. – № 4. – С. 12-17.

11. Певцов Г.В. Забезпечення інформаційної безпеки регіону: проблема, концепція та шляхи її реалізації / Г.В. Певцов, О.М. Черкасов. – Х.: Вид-во ХарРІ НАДУ "Магістр", 2008. – 138 с.

12. Joint Publication 3-13.2 Psychological Operations. – 07 January 2010. – 125 p.

13. Information Operations. Air Force Doctrine Document 2-5. – 11 January 2005. – 54 p.

14. Joint Publication 3-13 Information Operations. – 13 February 2006. – 136 p.

15. Information operations: warfare and the hard reality of soft power / Edited by Joint Doctrine for Information Operations. 9 October 1998 Leigh Armistead. – 1 st ed. – 2004. – 277 p.

16. UK Joint Warfare Publication 3-80. Information Operations. – 2002. – 55 p.

17. UK Joint Doctrine Publication 3-90. Civil-Military Co-operation (CIMIC). – 2006. – 47 p.

18. Neil Chuka. A Comparison of the Information Operations doctrine of Canada, the US, the UK, and NATO / Neil Chuka // Canadian Army Journal Vol.12.2 Summer 2009. – P. 91-99.

19. Феклістов А.О. Сучасні погляди на місце інформаційних операцій в системах інформаційної боротьби / А.О. Феклістов // Системи озброєння та військова техніка. – Х.: ХУПС, 2010. – 2'22. – С. 25-27.

20. Доктрина інформаційної безпеки України. Затверджена Указом Президента України від 8 липня 2009 року № 514/2009.

Надійшла до редколегії 11.02.2011

Рецензент: д-р техн. наук, проф. А.М. Сотніков, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВОЕННОЙ ОБЛАСТИ

Г.В. Певцов, С.В. Залкин, А.А. Феклистов

Рассматриваются концептуальные положения обеспечения информационной безопасности в военной области: определение и правовые основы Концепции информационной безопасности в военной области, принципы, основные цели, задания, объекты, субъекты, реальные и потенциальные угрозы, направления, методы и мероприятия по обеспечению информационной безопасности в военной области.

Ключевые слова: *информационная безопасность, концепция информационной безопасности, военная область.*

THE CONCEPTUAL APPROACHES FOR INFORMATION SECURITY MAINTENANCE IN DEFENCE SECTOR

G.V. Pevchov, S.V. Zalkin, A.O. Feklistov

The article considers the conceptual approaches for maintenance information security in defence sector: definition and legal framework for Information Security Concept in defence sector, principles, main aims, tasks, objects, subjects, real and potential threats, ways, methods and actions for information security maintenance in defence sector.

Keywords*: information security, concept of information security, defence sector.*