УДК 321:355

Нечхаєв С.М. к.військ.н., доцент[1];
Голда О.Л.[2]

[1] - Національний університет оборони України імені Івана Черняховського;
[2] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського

Удосконалений зміст інформаційних компаній США на Близькому Сході

Усовершенствованное содержание информационной компании США на Ближнем Востоке

The improvement sense of USA information companies on the Near East

Резюме. У статті розглянуто зміст складових інформаційної операції збройних сил.

Ключові слова: інформаційна компанія.

Резюме. В статье рассмотрено содержание составляющих информационной операции вооруженных сил.

Ключевые слова: информационная компанія.

Resume. In the article is examined the content of the elements of the Armed Forces informational operation.

Keywords: informational company.

Постановка проблеми. Символічною точкою відліку революційних перетворень у сфері новітніх інформаційних технологій став проведений військовим керівництвом США аналіз досвіду досягнення інформаційної переваги на полі бою під час операції "Буря в пустелі", проведеної у 1991 році. Ця операція стала останньою "класичною" і першою потужною інформаційною операцією в сучасній воєнній історії збройних сил США. На думку колишнього керівника командування навчальних і наукових досліджень будівництва сухопутних військ генерал-майора Глена Отіса, висловлену на сторінках американського військового виданя, "з операції "Буря в пустелі" можна отримати багато уроків. Деякі з них – нові, деякі – старі. У той же час один з уроків є, безумовно, фундаментальним. Природа війни докорінно змінилася. Та сторона, яка виграє інформаційну кампанію, переможе. Ми продемонстрували цей урок усьому світу: інформація є ключем в сучасній війні зі стратегічної, оперативної, тактичної і технічної точок зору" [1].

Аналіз основних досліджень і публікацій. Аналіз останніх досліджень і публікацій пов'язаних з інформаційними компаніями [2–7] свідчить, що загальні питання цих компаній розглядаються досить часто, переважно на прикладах їх проведення ЗС США. Тому, необхідність вивчення впливу інформаційних операцій на природу війни і кінцевий результат воєнних дій збройних сил США є актуальною проблемою і завданням для збройних сил інших держав.

Метою статті є розгляд змісту основних і допоміжних складових сучасної інформаційної операції за досвідом збройних сил США.

Викладення основного матеріалу. У збройних силах США термін "інформаційні операції" (далі – ІО) вже утвердився і широко використовується, у тому числі і в офіційних документах стратегічного планування застосування збройних сил. 13 лютого 2006 року комітет начальників штабів США затвердив нову редакцію доктрини "Інформаційні операції" (JP 3-13) [1]. У доктрині переглянуті погляди американського військового керівництва на підготовку і ведення збройними силами ІО, уточнені цілі, завдання й основні принципи інформаційної боротьби, а також обов'язки посадовців під час підготовки і ведення таких операцій у мирний і воєнний час.

Відповідно до нової доктрини ІО мають п'ять основних складових:

1. психологічна операція (Psychological Operations, PSYOPS);
2. оперативне маскування (Military Deception, MILDEC);
3. операція із забезпечення безпеки власних сил і засобів (Operations Security, OPSEC);
4. мережева операція (Computer Network Operations, CNO);
5. радіоелектронна боротьба (Electronic Warfare, EW).

До 2006 року вирішальну роль в ІО відігравали психологічні операції, оперативне маскування і забезпечення безпеки власних сил і засобів. У 2006 році до них додалися мережеві операції і радіоелектронна боротьба.

Мережевими операціями є: комп'ютерні мережеві атаки (Computer Network Attack, CNA) і мережевий захист (Computer Network Defense, CND), а також використання комп'ютерних мереж противника у своїх інтересах (Computer Network Exploitation, CNE).

CNA – це дія спеціально розробленими програмами на комп'ютери і комп'ютерні мережі противника для знищення наявної в них важливої інформації, а також для виведення з ладу самих комп'ютерів (мереж). Як CND розуміють заходи, які забезпечують моніторинг і аналіз мережевих атак на комп'ютерні об'єкти міністерства оборони США і захист від них. Під час використання CNE збирають важливу інформацію про самого противника, його автоматизовані системи управління і комп'ютерні мережі.

Радіоелектронна боротьба включає радіоелектронне придушення (Electronic Suppression, ES), радіоелектронний захист (Electronic Defence, ED) і радіоелектронне забезпечення (Electronic Security, ES).

ES призначене для дезорганізації і зниження можливостей використання противником радіоелектронних систем на усіх ієрархічних рівнях управління збройними силами.

ED призначене для захисту своїх радіоелектронних засобів від завад, які створює противник, а також для контролю за роботою радіоелектронних сил союзників для виключення взаємних завад.

ES призначене для виявлення, ідентифікації і визначення місцеперебування радіоелектронних засобів противника.

На думку військово-політичного керівництва США, до допоміжних складових ІО належать: забезпечення інформації (Information Assurance, IA), фізичне знищення критично важливих інформаційних об'єктів противника (Physical Attack, FA) і контррозвідка (Counterintelligence, CI).

Допоміжні складові є невід'ємною частиною основних складових ІО і безпосередньо або побічно впливають на вирішення завдань операції в цілому.

IA є системою заходів і дій, які дозволяють запобігти проникненню до інформаційних ресурсів і систем, визначити факт порушення, локалізувати об'єкт негативного впливу, нейтралізувати проникнення, відновити функції систем.

FA передбачає застосування засобів ураження для знищення і виведення із ладу ключових елементів системи управління і зв'язку противника.

CI призначена для визначення джерел загроз, припинення проникнення сил і засобів противника в державні і військові інформаційні мережі, а також для запобігання несанкціонованому втручанню в роботу цих мереж і несанкціонованому використанню банків даних своїх співробітників.

Для вирішення цих завдань командування збройних сил США передбачає ввести до складу сил і засобів інформаційної боротьби частини і підрозділи розвідки, РЕБ, психологічних операцій тощо. Випробування основних і допоміжних складових ІО в бойових умовах для вирішення завдань кампанії було успішно проведене в Іраку у 2003 році.

Висновок. Формою реалізації завдань сучасної інформаційної боротьби збройних сил США є інформаційна операція.

Кількість основних і допоміжних складових інформаційної операції поступово розширюється виходячи з необхідності ведення

активних дій в кіберпросторі, інформаційній і трьох фізичних сферах для фізичного знищення критично важливих інформаційних об'єктів противника, а також радіоелектронного придушення його мереж управління військами і зброєю, одночасного забезпечення безпеки власної інформаційної інфраструктури.

Залучення з цією метою космічних засобів дозволить за рахунок перенесення основної частини інформаційного потенціалу в навколоземний простір, результативно перетворити інформаційну перевагу на бойову. Тому, **перспективою подальшого розвитку в цьому напрямі** є об'єднання інтелектуальних об'єктів держави в єдиний інформаційний простір у межах ТВД (району або зони воєнних дій).

СПИСОК ЛІТЕРАТУРИ

1. Жуков В. Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. –2001. – № 1. 24–27с.
2. Комов С.А. О способах и формах ведения информационной борьбы / С.А. Комов // Военная мысль. – 1997. – № 4. – С. 18–22.
3. Воробеев К.Н. Прогноз характера и содержания операций (боевых действий) в войнах будущего / К.Н. Воробеев // Военная мысль. – 2005. – № 3. – С. 2–12.
4. Гриняев С.М. Концепции ведения информационной войны в некоторых странах мира / С.М. Гриняев // Зарубежное военное обозрение. – 2002. – № 2. – С. 11–15.
5. Поченцов Г.Г. Психологическая война / Г.Г. Поченцов. – К. : Ваклер, 2002. – С. 56–99.
6. Лисичкин В.А. Третья мировая информационно-психологическая война / В.А. Лисичкин, Л.А. Шелегин. – М., 1999. – С. 205–222.
7. Токов Е.Г. Психологические операции вооруженных сил США в войнах и конфликтах XX века / Е.Г. Токов, А.Л. Касюк // Зарубежное военное обозрение. – 1996. – № 6. – С. 22–24.