

ОСОБЛИВОСТІ ВЕДЕННЯ БОЙОВИХ ДІЙ У ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

В статті на основі аналізу тенденцій розвитку збройної боротьби визначені особливості ведення бойових дій у інформаційному середовищі. Сучасне інформаційне середовище має значний вплив на процес управління військами у ході ведення бойових дій та ведення бойових дій в цілому. Проведений аналіз дозволив визначити вплив інформаційного середовища на ведення бойових дій і визначити шляхи підвищення ефективності ведення бойових дій у сучасному інформаційному середовищі. Визначені підходи дозволять офіцерам органів військового управління переглянути свої погляди на процес прийняття рішень під час управління військами у ході ведення бойових дій у інформаційному середовищі.

Ключові слова: інформаційне середовище ведення бойових дій; управління військами; бойові дії; прийняття рішень.

Вступ

Бурхливий розвиток наприкінці ХХ і початку ХХІ століття інформаційних технологій, широка інформатизація суспільства і безпосередньо збройних сил провідних країн світу значно змінили характер, методи і способи діяльності державних, урядових політичних і економічних структур, вплинули на соціальні взаємозв'язки, характер, форми і способи ведення бойових дій, сформувавши нові інформаційні загрози та виклики.

Постановка проблеми. Фундаментальна зміна характеру, форм і способів ведення бойових дій вимагає розробки більш гнучкої стратегії застосування, будівництва та організації управління збройними силами, розробки доктрини ведення інформаційного протиборства, інформаційних операцій забезпечення інформаційної безпеки України та її Збройних сил.

Аналіз останніх досліджень і публікацій.

У Першій світовій війні бойові дії велися в основному у двох середовищах - у наземному і морському. У Другій світовій війні [2] до них додалося третє середовище - повітряне. ХХ століття стало століттям радіо. Радіозв'язок став основою управління збройними силами. Він зробив управління військами (силами) більш гнучким і оперативним, а війська - маневренішими, але більш уразливими. Разом з тим виникла перша реальна інформаційна загроза. Можливість радіоперехоплення і придушення перешкодами засобів радіозв'язку, радіолокації і радіонавігації приводила до розкриття задумів і намірів командування.

Ведення радіо- і радіотехнічної розвідки (РРТР) дало можливість випереджати супротивника у прийнятті рішень. Але при цьому радіоелектронні засоби демаскували війська і їх пункти управління. По суті, боротьба у інформаційному середовищі у Другій світовій війні вже велася, але сама інформація, видобута РРТР, ще не носила характер стратегічного ресурсу. "Війна в ефірі", як її тоді

називали, ще не була всеосяжною і часто носила лише епізодичний характер.

У подальшому "війна в ефірі" набула більш масовий характер і проводилась протягом всього часу ведення бойових дій. Особливо це проявилось у ході війни у Перський затоці у 1991 році [1], після якої з'явилося нове поняття у військовій справі - інформаційне середовище.

Метою статті є розгляд основних особливостей ведення бойових дій у інформаційному середовищі.

Виклад основного матеріалу дослідження

У чому ж суть особливостей ведення бойових дій у інформаційному середовищі?

Щоб зрозуміти суть, характер, роль і значення ведення бойових дій у інформаційному середовищі, необхідно оцінити ступінь загрози, пов'язаної з їх появою, треба розглянути більш детально особливості, що відрізняють їх від інших бойових дій.

До таких особливостей інформаційного середовища та ведення у ньому бойових дій можна віднести, зокрема, відсутність чітких меж під час ведення бою (операції) (по території, часу, простору) [5, 7].

Інформаційне середовище ведення бойових дій (ІСБД) може одночасно охоплювати не лише локальні, а й глобальні райони ведення бойових дій (своїх і противника) і життєво важливі території та об'єкти державного значення протиборчих сторін про що свідчить досвід проведення анти терористичної операції на сході України.

Для ІСБД не існує державних кордонів і закритих територій. ІСБД може мати локальний, глобальний характер, або той чи інший одночасно, що підтверджується веденням, так званої, гібридної війни проти України з боку Російської Федерації. ІСБД властиві висока анонімність і

скритність дій, труднощі виявлення автора і використуваних ним коштів.

Бойові дії у інформаційному середовищі можуть:

впливати (іноді вирішально) на ефективність та успішність ведення бойових дій в інших середовищах;

передувати бойовим діям у інших середовищах, вестися одночасно з бойовими діями у інших середовищах або після їх завершення, а також бути спонуканням до початку, продовження, припинення бойових дій або відмови противника від своїх намірів;

забезпечити досягнення і утримання інформаційної переваги над противником, підвищити їх ефективність, скорочувати втрати і забезпечувати успішність завершення бою (операції);

створювати сприятливі умови для досягнення як військових, так і політичних цілей своєю стороною, надаючи когнітивний вплив на особовий склад збройних сил та осіб, що беруть участь у підготовці та прийнятті рішень.

Бойові дії в інформаційному середовищі скорочують часовий цикл підготовки і прийняття рішень на ведення бойових дій і забезпечують можливість упередження противника у прийнятті рішень; підвищують оперативність виконання окремих бойових завдань та операції у цілому [3, 4]. Бойові дії в інформаційному середовищі не мають аналогій з історичним оперативно-стратегічним та оперативно-тактичним досвідом ведення бойових дій на землі, у повітрі і на морі.

За поглядами військових фахівців США і НАТО [8], бойові дії в інформаційному середовищі, що позбавляють можливості використання 50 і більше відсотків інформаційних

систем і комп'ютерних мереж під час ведення бою (операції), є умовою, що спонукає до початку або продовження ведення бойових дій.

Висновки й перспективи подальших досліджень

Таким чином, можна сказати, що особливості самого інформаційного середовища, бойових дій у ньому та їх вплив на всі інші середовища протиставлення сторін набувають все більшого впливу і масштабу, які надають глобального впливу не тільки на ефективність бою (операції) збройних сил, а й на військово-політичне керівництво сторін, стан економіки і політику, оскільки у проведенні інформаційних операцій можуть брати участь не тільки війська (сили) збройних сил, але і війська (сили) інших силових структур і цивільні засоби масової інформації протиставлених сторін.

Протиставлення в інформаційній сфері стало носити багатопрофільний характер суспільно-економічних, військово-політичних і державних відносин. Її метою стало не лише підвищення ефективності бойових дій шляхом завоювання інформаційної переваги, але і завоювання всебічної загальної переваги над потенційним противником, щоб забезпечити свої економічні, політичні, а якщо необхідно, то і військові цілі [9, 10]. Тому створення у Збройних Силах України спеціального органу військового управління, який буде здійснювати координацію дій підпорядкованих йому кібернетичних підрозділів, надасть можливість вдосконалити стратегію ведення бойових дій у інформаційному середовищі, що підвищить бойову ефективність Збройних Сил України.

Література

1. **Боевые действия** в Персидском заливе. Аналитический обзор. – М.: ИНФО-ТАСС, АСОНТИ, 1991. 2. **Нейл Грант**. Конфликты XX века. – М.: “Физкультура и спорт”. 1995. 3. **Дасс Р.** Зерно на мельнице. – Киев: “София”, 1993 г. 4. **Делаграмматик М.** Последний солдат суперимперии, или кому нужна “кибервойна” // “Литературная Россия” от 26.04.96, №17 (1733). 5. **Завадский И. И.** “Информационная война – что это такое?” // Защита информации. “Конфидент”. №4, 1996 г. 6. **Ларина Е., Овчинский В.** Кибервойны XXI века. О чем умолчал Эдвард Сноуден. Книжный мир, 2014 г.

7. **Расторгуев С. П.** Информационная война как целенаправленное информационное воздействие информационных систем. // “Информационное общество”. №1. 1997. 8. **Строев В.** Системы с искусственным интеллектом в сухопутных войсках // “Зарубежное военное обозрение”. №3, 1997 г. С.: 27–30. 9. **Г. Смолян, В. Цыгичко, Д. Черешкин.** Новости информационной войны // Защита информации. “Конфидент”. №6. 1996 г. 10. **Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н.** Реалии информационной войны. // Защита информации. “Конфидент”. №4. 1996.

ОСОБЕННОСТИ ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ В ИНФОРМАЦИОННОЙ СРЕДЕ

Виктор Евгеньевич Бобылёв (канд. воен. наук, с.н.с.)

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

В статье на основе анализа тенденций развития вооруженной борьбы определены особенности ведения боевых действий в информационной среде. Современное информационное пространство может влиять на процесс управления войсками в ходе ведения боевых действий и ведения боевых действий в целом. Проведенный анализ позволил определить влияние информационной среды на ведение боевых действий и определить пути повышения эффективности ведения боевых действий в современной информационной среде. Определены подходы, позволяющие офицерам органов военного управления

пересмотреть свои взгляды на процесс принятия решений при управлении войсками в ходе ведения боевых действий в информационной среде.

Ключевые слова: информационная среда ведения боевых действий; управления войсками; боевые действия; принятие решений.

FEATURES OF WARFARE IN THE INFORMATION ENVIRONMENT

Viktor Y. Bobylov (Candidate of Military Sciences, Senior Research Fellow)

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The article is based on analysis of trends of the armed struggle by the features of warfare in the information environment of modern information environment has a significant impact on the control of troops in the course of combat and warfare in general. The analysis allowed to establish the impact of the information environment to conduct military operations and identify ways to improve the efficiency of warfare in the modern information environment. The approaches allow officers of the military authorities to reconsider their views on the decision-making process in the control of troops during warfare in the information environment.

Keywords: information environment of warfare; command and control; combat; making decisions.

References

- 1. The fighting in the Persian Gulf. Analytical overview** (1991), Modeling. [*Boevye dejstvija v Persidskom zalive. Analiticheskij obzor*], Moscow, INFO-TASS, ASONTI.
- 2. Neil Grant** (1995), The conflicts of the XX century. [*Konflikty XX veka*], Moscow, Fizkul'tura i sport.
- 3. Dass R.** (1993), Grain to the mill. [*Zerno na mel'nicu*], Kyiv, Sofija.
- 4. Delagrammatik M.** (1996), Last super soldier of the empire, or who need a "cyberwar". [*Poslednij soldat superimperii, ili komu nuzhna "kibervojna"*], Literaturnaja Rossija from 26.04.96, №17 (1733).
- 5. Zavadskij I.I.** (1996), Information War - what is it? [*Informacionnaja vojna – chto jeto takoe?*], Zashhita informacii, "Konfident", No.4.
- 6. Larina E., Ovchinskij V.** (2014), Cyber war of the XXI century. What silent Edward Snowden. [*Kibervojny XXI veka. O chem umolchal Jedvard Snouden*], Knizhnyj mir.
- 7. Rastorguev S.P.** (1997), Information warfare as purposeful information influence of information systems. [*Informacionnaja vojna kak celenapravlennoe informacionnoe vozdejstvie informacionnyh sistem*], Informacionnoe obshhestvo, No.1.
- 8. Stroev V.** (1997), Systems of artificial intelligence in the Army. [*Sistemy s iskusstvennym intellektom v suhoputnyh vojskakh*], Zarubezhnoe voennoe obozrenie, No.3, pp. 27-30.
- 9. Smoljan G., Cygichko V., Chereskin D.** (1996), News information war. [*Novosti informacionnoj vojny*], Zashhita informacii. "Konfident", No.6.
- 10. Chereskin D.S., Smoljan G.L., Cygichko V.N.** (1996), The realities of the information war. [*Realii informacionnoj vojny*], Zashhita informacii. "Konfident", No.4.

Отримано: 19.07.2016 року