УДК 681.5.01 к.т.н. **Литвиненко Н.І.** (ВІКНУ)

ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ЯК СКЛАДОВА ЧАСТИНА КОМПЛЕКСНОГО ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПРОВЕДЕННЯ СУЧАСНИХ БОЙОВИХ ДІЙ

У статті проаналізовані принципи та завдання застосування інформаційних операцій за досвідом армій розвинутих країн. В сучасних умовах ведеться активна підготовка до ведення інформаційних воєн, в яких знищення противника буде можливим за допомогою принципово нового типу зброї - інформаційного, здатного руйнувати мережі і комп'ютерні системи управління військових та інших життєво важливих об'єктів держави. Бурхливий розвиток в даному питанні викликав багато проблем, пов'язаних із забезпечення власної кібербезпеки. Тому на сьогоднішній день більшість потужних держав світу приділяє належну увагу питанням кіберзахисту.

Ключові слова: інформаційні операції, кіберзахист, кіберзагроза, кібербезпека.

Вступ. За думкою зарубіжних фахівців сьогодні в більшості країн світу, і в першу чергу в США, ведеться активна підготовка до ведення інформаційних воєн. Знищення противника в нових умовах буде можливим за допомогою принципово нового типу зброї - інформаційного, здатного руйнувати мережі і комп'ютерні системи управління військових та інших життєво важливих об'єктів держави. Багато експертів вважають, що по ефективності його можна зарахувати до зброї масового ураження.

Постановка завдання. Згідно поглядів вищого воєнно-політичного керівництва США, стратегії національної безпеки США, інших нормативних документів, інформаційна боротьба може проводитись у формі інформаційних операцій (дій) стратегічного, оперативного та тактичного рівнів.

Досвід з досягнення інформаційної переваги на полі бою, отриманий в ході операції «Буря в пустелі» (1991), що стала останньою «класичної» і першою великою інформаційною війною в сучасній військовій історії збройних сил США, став символічною точкою відліку революційних перетворень у галузі нових інформаційних технологій. Колишній командувач командуванням навчальним та наукових досліджень з будівництва СВ генерал-майор Гленс Отіс ретельно проаналізував даний досвід і в матеріалах своєї роботи вказав наступне: «З операції« Буря в пустелі »можна отримати багато уроків. Деякі з них - нові, деякі - старі. Один урок, тим не менш, є воістину фундаментальним. Природа війни докорінно змінилася. Та сторона, яка виграє інформаційну кампанію, переможе. Ми продемонстрували цей урок всьому світу: інформація є ключем до сучасної війні в стратегічному, оперативному, тактичному та технічному відношенні». Дані висновки доводять, що інформаційні операції стануть невід'ємною частиною ведення бойових дій у майбутньому.

Результати дослідження. Інформаційні операції (дії) – комплекс заходів ЗС США щодо впливу на людські і матеріальні ресурси противника з метою ускладнити чи зробити неможливим прийняття ним правильних рішень з одночасним захистом своїх інформаційних систем.

Інформаційна операція (дія) є інтегруючою формою застосування різних складових, які в свою чергу поділяються на основні, підтримуючі та пов'язані з проведенням інформаційних операцій.

Основними складовими інформаційних операцій (дій) є:

- психологічні операції (Psychological Operations, PSYOP);
- введення противника в оману (Military Deception, MILDEC);
- забезпечення інформаційної безпеки операцій (Operational Security, OPSEC);
- радіоелектронна боротьба (Electronic Warfare, EW);
- операції в комп'ютерних мережах (Computer Network Operations, CNO).

Підтримуючими складовими інформаційних операцій (дій) є:

- інформаційне забезпечення (Information Assurance, IA);

−фізичний захист власних об'єктів інформаційної інфраструктури (Physical Security);

−вогневе ураження об'єктів інформаційної інфраструктури противника (Physical Attack);

−контррозвідка (Counterintelligence, CI);

−фото, відеозйомка та документування бойових дій (Combat Camera, COMCAM).

Безпосередньо пов'язаними з проведенням інформаційних операцій складовими є:

−громадські заходи (Public Affairs, PA);

−цивільно-військові операції (Civil-Military Operations, CMO);

−оборонна підтримка публічної дипломатії (Defense Support to Public Diplomacy, DSPD).

На сьогоднішній день першочерговими завданнями для підтримки інформаційних операцій в США є:

−швидке розгортання формувань психологічних операцій в підтримку звичайних чи спеціальних операцій сухопутних військ і корпуса морської піхоти;

−розробка планів психологічних операцій на ТВД і узгодження їх з оперативними планами бойового застосування збройних сил та програмами бойової підготовки мирного часу;

−розробка і тиражування матеріалів інформаційно-психологічного впливу (листівок, плакатів, аудіовізуальної продукції, відеоматеріалів, програм радіо- і усного мовлення і т.д.);

−проведення психологічних операцій всіх рівнів;

−підготовка аналітичних, інформаційних, довідкових та інших матеріалів розвідувального характеру з питань психологічних операцій для вищого військово-політичного керівництва.

Військово-політичне керівництво США приділяє велику увагу розвитку сучасних зразків техніки психологічних операцій. Одним з прикладів цього є розробка, прийняття на озброєння та широке бойове застосування у воєнних конфліктах повітряних телерадіоцентрів на базі літаків EC-130J "Commando Solo". Літаки, загальна кількість яких становить сім одиниць, входять до складу 193 крила спеціальних операцій авіації національної гвардії, яке підпорядковується командуванню сил спеціальних операцій (місце дислокації – аеропорт м. Гарісберг, штат Пенсільванія). Жодна армія світу аналогічного літака не має. Обладнання літака дозволяє вести кольорові телевізійні передачі у всьому діапазоні телевізійного віщання, радіопропаганду на стандартних радіочастотах, здійснювати входження у бойові радіомережі військ противника, розповсюджувати листівки. В рамках проведення однієї операції, як правило, діють 2−3 літаки EC-130J. Оповіщення цільової аудиторії щодо конкретних радіо- та телевізійних частот, на яких працює літак, проводиться за допомогою гучномовних станцій та листівок.

Інформаційно-психологічний вплив, як відомо, був успішно «апробований» в останній військовій кампанії в Іраку. Тоді в ході військових дій ЗС США в рамках інформаційної операції через електронну пошту розіслали послання арабською мовою іракським генералам із закликом не виконувати накази С. Хусейна. Крім того, в електронних повідомленнях, складених спеціалістами служби, містилися звернення до цивільного населення країни з проханням про надання допомоги у виявленні баз і сховищ ядерного, хімічного і біологічної зброї тощо. Слід зазначити, що широкомасштабне адресне звернення до іракського військового керівництва - порівняно новий момент у практиці психологічних операцій, що проводяться в ЗС США. За задумом фахівців з Пентагону, найбільш перспективними напрямками використання глобальної мережі в інтересах психологічної боротьби при плануванні інформаційних операцій може стати прийом заміни інформаційного змісту сайтів, суть якого полягає в підміні сторінок або їх окремих елементів в результаті злому. Такі дії робляться, як правило, для залучення уваги до нападаючої сторони, демонстрації своїх можливостей або як спосіб вираження конкретної політичної позиції і тощо.

Серйозні надії американські військові фахівці в області теорії і практики планування психологічних операцій покладають на так звані семантичні атаки, в ході яких інформаційна система противника продовжує функціонувати, причому чисто зовні її робота не викликає жодних підозр. Однак вхідна інформація не відповідала реальності. Таким атакам, як правило, піддаються інформаційні сторінки, які часто відвідуються, та змісту яких користувачі повністю довіряють.

Нові інформаційні технології дозволяють більш ефективно надавати відповідне забезпечення в ході регіональних конфліктів. Це підтвердив досвід ведення війни проти Іраку навесні 2003 року. Тоді ЗС США вперше на практиці перевірили мережецентричну (Network-centric) концепцію бойових дій. У такій операції за рахунок абсолютного інформаційної переваги над противником забезпечується повна самосинхронізації бойових дій та акцій на полі бою, а також гарантується оперативність управління військами і високий рівень бойових можливостей. В результаті подібних дій противник позбавляється можливості проводити будь-який курс дій і впадає в шок. У ході бойової фази ведення кампанії, використовуючи переваги авіації, війська США вступили в бій без класичного тилового забезпечення і попередньої розвідки. При цьому всі комп'ютери штабу угруповання, працюючи з повним навантаженням, дозволяли відстежувати до 1 000 наземних цілей. Успішно, за висновком західних військових фахівців, спрацювала новітня система бойового управління майбутньої - TBMCS (Theater Battle Management Core System), що дозволила координувати вильоти літаків одночасно армійської і палубної авіації. У тактичному та оперативному ланці широке застосування нового комплексу бойового управління - FBCB (Force XXI Battle Command Brigade or Below), що представляє собою сучасну систему графічного відображення інформації на тактичному рівні аж до окремого військовослужбовця, дозволило повністю відмовитись від топографічних карт, приймати дані космічної й авіарозвідки в масштабі реального часу на екрани тактичних комп'ютерів командирів усіх ланок. Всього в зоні конфлікту було задіяно 4 тис. бортових комп'ютерів і 100 серверів, при цьому кожен користувач мав свій пароль. Застосування в ході бомбардувань Багдада дослідної електромагнітної бомби (Е-бомба) паралізувало іракське телебачення і роботу інших електронних засобів масової інформації, а скидання авіабомб GBU-37, вагою 2 000 кг кожна, в поєднанні з широкомасштабним використанням високоточної зброї певною мірою сприяло підриву морально - психологічного стану військ і населення Іраку.

Бурхливий розвиток інформаційної сфери став джерелом виникнення проблеми забезпечення власної кібербезпеки. На сьогоднішній день більшість потужних держав світу (США, Росія, ЄС, Китай, Індія та інші) знаходяться в процесі трансформації власних військових потенціалів з огляду на можливості використання мережі Інтернет. За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі у 2010 р., уже більше 20 країн планували здійснювати або реально здійснювали різноманітні інформаційні операції у 2009-2010 рр. Формуються спецпідрозділи, які мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і „обвал" структур супротивника. Згідно з офіційними заявами, такі підрозділи створено в США (U.S. Cyber Command), Великобританії (Cyber Security Operations Centre при уряді Великобританії), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence).

Дані про потенціал, чисельність чи завдання китайських кібервійськ практично відсутні. За даними ФБР, КНР на сьогоднішній день має армію у 180 000 хакерів, які займаються щоденними атаками на кібермережі США і лише в 2009 році здійснили 90 000 атак проти комп'ютерів Міністерства оборони США. З 180 тис. хакерів 30 тис. є військовими, а 150 тис. – комп'ютерними експертами з приватного сектору, місією яких є

отримання доступу до військових та комерційних секретів США та внесення розладу до урядових та фінансових служб.

Неменш активна політика в сфері кібербезпеки є і у США:

– 29 травня 2009 року оприлюднено „Огляд кібербезпеки" (Cyber Security Review) – комплексний документ, що визначає основні пріоритети нової команди у сфері кібербезпеки;

– створено посаду Керівника Кібербезпеки Ради національної та внутрішньої безпеки;

– створено Кіберкомандування США (U.S. Cyber Command) під головуванням генерала К. Александера, що одночасно очолюватиме і згаданий підрозділ і Агентство з національної безпеки;

– оприлюднено нову „Стратегію національної безпеки" (2010) в якій кіберзагрозам вперше відведено окреме місце в загальній структурі загроз США;

– оголошено про додаткові заходи із посилення внутрішньої кібербезпеки. З 1 жовтня 2009 року в США оголошено про набір додатково 1000 співробітників до спеціального кібербезпекового департаменту Управління національної безпеки (Department of Homeland Security), які будуть займатись виключно безпекою високотехнологічних систем США. Однак, навіть 1000 співробітників не повністю відповідає потребам США у фахівцях з кібербезпеки. У супровідному документі до спеціально організованих урядом США змагань „Кіберзмагання США" (U.S. Cyber Challenge) наводиться думка одного з експертів, що реальна потреба уряду в таких фахівцях складає від 10 000 до 30 000;

– збільшення держзамовлення на розробку нових засобів ведення війни і зокрема – кіберозброєнь та нових, більш захищених, військових мереж;

– створено проекти нормативних документів, що спрямовані на покращення взаємодії в сфері кібербезпеки союзниками США та убезпечення власного Інтернет простору в разі виникнення ситуацій, що загрожують національній безпеці.

Великобританія (потенціал якої в сфері кіберзахисту вважається одним з найпотужніших) все ще розбудовує власні сили безпеки у кіберпросторі. У 2010 році дана держава запустила у повноцінному режимі роботу Оперативного центру з кібербезпеки (20 співробітників) з метою координації вже існуючих різноманітних центрів із кібербезпеки різних відомств та створення майданчику для співпраці між урядом та приватним сектором із проблем кібербезпеки. Крім того у Великобританії ефективно працює Командування урядових комунікацій (Government Communications Headquarters), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів.

Згідно відкритих даних активно створюються відповідні підрозділи у Південній та Північній Кореї, Російській Федерації, Франції.

Така увага до забезпечення кібербезпеки та створення засобів ведення кібервійн, змушує уряди держав переглядати і свою внутрішню політику в кіберсфері. Це обумовлено, в тому числі, і зростанням кількості випадків використання розвідувальними службами та спеціалізованими військовими підрозділами можливостей та технічних потужностей транснаціональних кримінальних груп, що спеціалізуються у сфері кіберзлочиності.

Відповідних змін в різних країнах світу набуває і структура збройних сил. Практично в кожній провідній країні, на сьогоднішній день, створюються структури, призначені, як для забезпечення власної кібербезпеки, так і для активного впливу на кіберпростір можливого противника.

Висновки. Таким чином, інформаційні операції в умовах бурхливого розвитку комп'ютерних технологій будуть невід'ємною частиною ведення бойових дій у майбутньому, що викличе різке збільшення кількості кіберзагроз та зростанням їх ваги, поширенням комп'ютерної злочинності, використанням комп'ютерних мереж міжнародними терористичними організаціями. Тому необхідно вжити відповідні заходи щодо забезпечення інформаційної безпеки комп'ютерних мереж від проникнення, ушкодження або знищення противником.

ЛІТЕРАТУРА:
1. Joint Chiefs of Staff Joint Publication 3-13. Information operations. Washington. DC. 2006.
2. Headquarters Department of the Army. Field Manual 3 – 13 (FM 100 - 6). Information operations: Doctrine, Tactics, Techniques and Procedures. Washington. DC. 2003.
3. Joint Forces Staff College. Joint Information Operations Planning Handbook. 2003.
4. U.S. Army War College. Information Operations Primer. AY 11 Edition. 2010.
5. The United States Army operations concept 2016 – 2028. TRADOC Pam 525-3-1/ 2010.
6. Headquarters Department of the Army. Field Manual 3.05-30. Psychological operations/ Washington. DC. 2005.
7. target.vif2.ru Електронна версія журналу "Зарубежное военное обозрение ";
8. nvo.ng.ru Електронна версія журналу "Независимое военное обозрение ";
9. Офіційний сайт державного департаменту США, веб-сторінка http://www.state.gov;
10. Офіційний сайт збройних сил Великобританії, веб-сторінка http://www.army.mod.uk/21197.aspx;
11. Офіційний сайт кіберкомандування збройних сил США, веб сторінка https://www.cybercom.mil.
12. ЗВО. – 2007. – №5. – С. 7-12.

Рецензент: к.військ.н., доц. Пашков С.О., старший науковий співробітник науково-дослідного центру, Військовий інститут, Київський національний університет імені Тараса Шевченка

к.т.н. **Литвиненко Н.И.**

ИНФОРМАЦИОННЫЕ ОПЕРАЦИИ КАК СОСТАВНАЯ ЧАСТЬ КОМПЛЕКСНОГО ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПРОВЕДЕНИЯ СОВРЕМЕННЫХ БОЕВЫХ ДЕЙСТВИЙ

В статье проанализированы принципы и задачи применения информационных операций по опыту армий развитых стран. В современных условиях ведется активная подготовка к ведению информационных войн, в которых уничтожение противника будет возможным с помощью принципиально нового типа оружия – информационного, способного разрушать сети и компьютерные системы управления военных и других жизненно важных объектов государства. Бурное развитие в данном вопросе вызвало много проблем, связанных с обеспечением собственной кибербезопасности. Поэтому большинство мощных государств мира уделяет должное внимание вопросам киберзащиты.

Ключевые слова: информационные операции, киберзащита, киберугрозы, кибербезопасность.

Ph.D. **Litvinenko Nataliya**

INFORMATION OPERATIONS AS PART OF INTEGRATED INFORMATION TECHNOLOGY FOR THE MODERN COMBAT OPERATIONS

The article analyzes the principles and objectives of the use of information operations experience armies of developed countries. In modern conditions, is actively preparing for information war, in which the destruction of the enemy will be possible with the help of a new type of weapons - information that could destroy the network and computer control systems of military and other vital state. Rapid development in this matter has caused many problems to ensure its own cybersecurity. Therefore, by far the most powerful countries in the world pays due attention to cyberdefense.

Keywords: information operations, cyberdefense, cyberthreats, cybersecurity.