УДК 621.618

В.Д. Карлов[1], О.В. Лукашук[1], С.М. Шолохов[2]

[1] *Харківський університет Повітряних Сил України імені Івана Кожедуба, Харків*
[2] *Військова частина А1906*

ДО ПИТАННЯ ПРО СУТЬ ТА ВИДИ ІНФОРМАЦІЙНОЇ ЗБРОЇ В СУЧАСНИХ ІНФОРМАЦІЙНИХ КОНФЛІКТАХ

У статті проаналізовано особливості розвитку інформаційної зброї, яка застосовується в сучасних конфліктах. На підставі проведеного аналізу виділено та проаналізовано основні види інформаційної зброї, а також визначена суть цієї зброї в загальній концепції ведення силових інформаційних конфліктів.

Ключові слова: *інформаційна зброя, радіоелектронна боротьба, безпілотні літальні апарати, автоматизовані системи управління, високоточна зброя.*

Постановка проблеми

Аналіз відомої літератури [1, 2] свідчить про те, що останнім часом в розвинених країнах світу широко опрацьовуються теоретичні основи вироблення системних концепцій і ведення силового інформаційного протиборства. При цьому, як випливає з [3, 4], початком зародження форм і способів ведення інформаційного протиборства була поява інформаційної зброї та інформаційних ударних систем і засобів, що забезпечують їх застосування. В даний час в світовій практиці чітко намітилася тенденція різкого підвищення ролі інформаційної зброї (ІЗ) при плануванні і веденні операцій та бойових дій.

Це в черговий раз було підтверджено в ході проведення операцій ОВС НАТО в Іраку "Буря в пустелі" (1991 рік), "Шок і трепет" (2003 рік), в Югославії "Союзницька сила".

Разом з тим питанню створення теоретичної бази для вирішення проблем інформаційної боротьби в Україні, планування наступальних і оборонних інформаційних операцій, для підвищення ефективності досягнення цілей силових інформаційних конфліктів у відомій літературі приділено недостатньо уваги.

Ліквідації цього недоліку, зокрема і присвячена дана стаття, а саме питанню визначення суті, видів, об'єктів застосування і особливостей розвитку ІЗ в загальній концепції ведення силових інформаційних конфліктів.

Основна частина

Під інформаційною зброєю при проведенні наступальних інформаційних операцій в рамках забезпечення ведення бойових дій і операцій військами (силами), миротворчих і антитерористичних операцій зазвичай розуміють [3 – 5] сукупність спеціальних інформаційно-програмних ударних систем і засобів, комплексів і засобів радіоелектронної боротьби (РЕБ), електромагнітної поразки, технологій, інформації та дезінформації, вживаних для деструктивних дій на особовий склад і організацію автоматизованих систем управління (АСУ) державними структурами, військами (силами) і зброєю евентуального супротивника.

Розглянемо ряд з цих складових інформаційної зброї.

Інформаційна зброя електромагнітної поразки елементів АСУ

Системи і засоби електромагнітної поразки (ядерної і неядерної природи) об'єктів інформаційної боротьби за показниками бойової ефективності, як випливає з [2], можуть бути аналогами тактичної ядерної зброї. Це електромагнітні боєприпаси неядерної природи з радіусом дії від 0,2 до 10 кілометрів [2]. Як випливає з даних, приведених в [3], на шлях революційних змін в області РЕБ вже стали такі розвинені країни світу, як США, Китай, Франція і Англія. Зокрема, одна з основних тенденцій розвитку озброєння США – повномасштабні наукові експерименти по створенню і впровадженню в практику військ електромагнітної поразки. У операціях „Буря в пустелі", „Непохитна свобода" вперше для вирішення завдань дезорганізації управління військами (силами) супротивника була застосована електромагнітна зброя (ЕМЗ) [3].

Застосування цього виду інформаційної зброї приводить до вигорання елементів АСУ, наприклад, модемів, ліній зв'язку, високочутливої елементної бази персональних електронно-обчислювальних машин. Засобами доставки електромагнітних боєприпасів можуть бути літаки, безпілотні літальні апарати (БПЛА), артилерійські снаряди, крилаті і оперативно-тактичні ракети.

Зараз йде процес активного впровадження ЕМЗ для вирішення завдань дії на особовий склад і населення супротивника.

Інформаційна зброя дії на програмно-математичне забезпечення АСУ

Відповідно до [3] це:
спеціальне програмне забезпечення,
комп'ютерні віруси,
закладки,
логічні бомби,
“троянські програми”,
“черв'яки”.

Вірус по своїй структурі складається з двох частин – розмноження (цілірозподілу та доставки) і дій (бойовій, ударній частині). При цьому перша частина вірусу є “головкою наведення” і служить для вибору мети (цілей) і доставляє його до об'єкту поразки. Інформація про мету надається “системами комп'ютерної розвідки”.

При цьому системи і засоби дії на програмне забезпечення можуть розглядатися як аналог високоточної зброї (ВТЗ) в інформаційному просторі. Згідно [3], деструктивна дія вірусу як інформаційна ВТЗ спрямована на нанесення шкоди об'єкту, зокрема, або системі в цілому.

Ця частина вірусу може бути “міною сповільненої дії” і спрацьовувати при виконанні необхідних умов. Дуже часто “бойова” частина вірусу виявляється касетним зарядом, здатним вражати декілька об'єктів за один запуск.

Як обґрунтовано в [3], автоматизована система управління супротивника може не знищуватися в ході інформаційної атаки. Тоді метою інформаційної атаки є захоплення управління АСУ супротивника.

Прикладом таких засобів можуть служити “троянські програми” ВО (Backdoor.BO, aka Back Orifice Trojan) і NetBus. Ці програми є могутніми утилітами видаленого адміністрування комп'ютерів в мережі і надають користувачеві більше можливостей, чим має авторизований користувач цього комп'ютера.

Структурно вони складаються [2] з двох частин: видаленого “клієнта-розвідника (диверсійної групи)” і “серверної” частини (командування, штабу). Видалений “клієнт” діє по командах з центру і служить засобом (плацдармом) для ведення інформаційних дій.

Одним із засобів створення і розповсюдження вірусів і “троянов” є автоматизовані “конструктори вірусів” (наприклад, VLC, NRLG, PS-MPC, G2), за допомогою яких можна вибрати тип вірусу, об'єкти, що вражаються, наявність або відсутність самокодування, протидію відгадчику, внутрішні текстові рядки, вибрати ефекти, супроводжуючі роботу вірусу, і тому подібне На їх базі в мінімальні терміни (1-6 ч) може бути створене більше тисячі вірусів [3].

По відомих відомостях [1], армією США оголошений конкурс на розробку комп'ютерного “вірусу”, призначеного для виведення з ладу електронних систем супротивника, військових ліній зв'язку, систем управління озброєними силами і передачі помилковій інформації.

Інформаційна зброя дії на мережі і телекомунікаційні засоби обміну даними АСУ

Відповідно до [1 – 3] це засоби перехоплення, руйнування або викривлення інформаційних масивів (масивів програм і даних), які використовуються в автоматизованих інформаційно-ударних системах супротивника).

Найбільш популярними атаками на мережі і телекомунікаційні засоби обміну даними вважаються [1 – 3]:

- установка вірусу на комп'ютер жертви за допомогою передачі файлу по ICO;
- застосування програм видаленого адміністрування;
- переповнювання робочого телекомунікаційного каналу користувача (атаки “відмова в обслуговуванні”) шляхом відправлення йому величезної кількості TCP-пакетів з позначкою “терміново” (наприклад, за допомогою WINNUKE).

На рівні мережевого програмного забезпечення можливі:
прослуховування каналу;
перехоплення пакетів на маршрутизаторі;
викривлення помилкового маршрутизатора;
нав'язування помилковій інформації (пакетів).

Особливістю даного виду інформаційної зброї є висока прихованість та масштабність організації дії. Одним з прикладів масштабності дії на телекомунікаційні мережі служить атака, проведена 11 вересня 2000 року на сервер Western Union. Внаслідок цього були вкрадені кредитові і дебітні карти 15700 онлайнових клієнтів.

Активно схильні до програмно-комп'ютерного подавлення системи управління енергетикою, банками і подібні до них установи. Вже давно зрозуміли, що неможливо говорити про комп'ютерну безпеку незакритих комп'ютерних систем в Україні до тих пір, поки не буде розроблена “своя” операційна система.

Застосування операційних систем, що купуються за кордоном, неминуче ставить важливі системи життєзабезпечення держави в стан очікування команди на виключення ззовні.

Застосування даного виду інформаційної зброї може мати місце при організації інформаційних атак на системи космічної розвідки і навігації.

Наприклад, в 2000 році командою “хакерів” були змінені параметри орбіти розвідувального супутника збройних сил Англії. Інформаційні ата-

ки на космічні системи розвідки і зв'язку проведені при організації терористичних актів 11 вересня 2001 року в США.

Інформаційна зброя радіоелектронної дії на системи радіозв'язку, передачі даних, радіонавігації і супутникового зв'язку, елементи систем радіоелектронної розвідки

До даного виду можуть відноситися існуючі, модернізовані та перспективні комплекси і засоби радіоелектронного подавлення (РЕП). Наприклад, в Збройних Силах України завдання по радіоелектронному подавленню засобів радіозв'язку можуть вирішувати станції:

– у короткохвильовому діапазоні – Р-378, Р-325 і їх модифікації (вид завадового сигналу – прицільний по частоті і загороджувальний за напрямком, дальність дії до 60 км.);

– у ультракороткохвильовому діапазоні – Р-934 Би, У (дальність дії до 400 км.), Р-330 П, У, Би (дальність дії до 30 км.), вид завади – прицільна по частоті і загороджувальна за напрямком;

– для інформаційної дії на навігаційні системи (навігаційна система "Такан") при проведенні наступальної інформаційної операції можуть застосовуватися станції Р-388 і їх модифікації (дальність дії до 400 км.).

Для дії на елементи перспективних систем супутникового зв'язку можуть застосовуватися перспективні засоби РЕП, розташовані на БПЛА.

Радіоелектронне подавлення багатофункціональних бортових станцій (МБРЛС) радіолокації може здійснюватися із застосуванням станцій СПН-30, СПН-40, СПО-8 (дальність дії 15... 150 км.).

Для впливу на процес управління озброєнням терористів (наприклад , радіокеровані фугаси, міни) можуть застосовуватися закидаючи передавачі завад (ЗПЗ).

Застосування таких засобів інформаційної боротьби особливо актуально при вирішенні завдань охорони VIP-персон, протидії дій різних видів розвідок.

Інформаційна зброя фізичного знищення елементів АСУ

До даного класу ІЗ віднесено [1, 5] системи та засоби, що приводять до фізичного руйнування елементів АСУ евентуального супротивника.

Наприклад:

системи і засоби вогняної поразки,

вибухові засоби, що доставляються розвідувально-диверсійними групами,

біологічні мікроби-руйнівники елементної бази [1, 5].

Інформаційна консцієнтальна зброя

Консцієнтальна зброя (КЗ) – інформаційна зброя, що руйнує свідомість особового складу [5]. У складі КЗ можуть застосовувати:

– засоби дії на свідомість і підсвідомість особового складу (психотропна інформаційна зброя). До даної групи можуть відноситися засоби масової інформації (радіо, преса, телебачення) і агітаційно-пропагандистські засоби (відеокасети, електронні підручники і енциклопедії). Цей різновид ІЗ може розглядатися як аналог зброї масового ураження і призначена для цілеспрямованого нанесення інформаційного збитку духовно-етичного життя особового складу протистоячого угрупування, його історичній пам'яті, світогляду, морально-етичним ідеалам з метою можливого управління його поведінкою, а також для створення перешкоди аналогічним діям супротивника;

– засоби дії на нейромозговий субстрат особового складу (психотропні засоби) – спеціальні лікарські препарати, психофармакологічні і психодіслептичні засоби, транквілізатори, антидепресанти, галюциногени, наркотики, алкоголь, призначені для дії на психіку особового складу на генному або хромосомному рівнях. Транквілізатори розривають зв'язок між інформаційно-психічними і фізичними процесами в організмі людини. Галюциногени викликають психічні розлади;

– засоби дії на організацію інформаційно-комунікативного середовища існування свідомості особового складу. Це спеціальні генератори, спеціальна відеографічна і телевізійна інформація, відео засоби, призначені для дистанційного зомбування особового складу протистоячого угрупування, а також для збудження психічних і психофізіологічних розладів операторів-користувачів підсистем на основі спеціальної контамінації ("змішення") колірної гамми, дискретності і інтенсивності випромінювання на екранах електронно-променевих трубок моніторів, ефекту "25 кадру" (сприйманого тільки на підсвідомому рівні) і ін. Наприклад, відомо, що 12 грудня 1997 р. в Японії по національному телебаченню демонструвався мультфільм, що містить контамінацію колірної гамми, звуку, мигання візуальної інформації і анімаційних кадрів, від перегляду якого десятки дітей отримали психофізіологічні розлади різної тяжкості;

– засоби впливу на форми і способи ідентифікації особи;

– засоби "соціальної інженерії" – однієї з частин соціальної психології, спрямованої на маніпулювання людьми або породження в їх розумі нової моделі поведінки. Ці засоби вже апробовані при проведенні атак на "злом" фінансових комп'ютерних мереж (наприклад, атака на сервер Western Union).

Інформаційна зброя семантичної дії

Різновид інформаційної зброї, що впливає на якість і достовірність інтерпретації оператором (групою операторів) семантичної інформації.

До семантичної зброї відносяться:

– системи і засоби семантичного пошуку (виявлення), модифікації (фальсифікації) і знищення;

– системи і засоби семантичного і криптографічного аналізу;

– системи і засоби семантичної і криптографічної дії.

Наприклад, до засобів семантичної зброї можна віднести Macro-віруси, що заражають документи (інформацію, дані) з автоматичним виконанням макросів.

Спочатку цей клас вірусів заражає систему, в якій проводиться підготовка таких документів (наприклад, в Microsoft Word спочатку заражає основний шаблон системи – normal.dot), а потім виконує деструктивні дії над даними (знищуючи або модифікуючи).

Відомий випадок, коли застосування семантичної зброї привело до загибелі людини (дія здійснювалася на інформаційну систему медичної установи).

Висновки

У статті проаналізовано особливості розвитку інформаційної зброї, яка застосовується в сучасних конфліктах.

На підставі проведеного аналізу виділено та проаналізовано основні види інформаційної зброї в загальній концепції сучасного силового інформаційного конфлікту, а також визначена суть цієї зброї в загальній концепції ведення силових інформаційних конфліктів.

Список літератури

1. Батурин Ю.М.. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзинский. – М.: Юридическая литература, 1991.

2. Петраков А.В. Основы практической защиты информации. 2-е изд. Учеб. пособие / А.В. Петраков. – М.: Радио и связь, 2000. – 368 с.

3. Электромагнитная совместимость радиоэлектронных средств и непреднамеренные помехи; составитель Д.Р.Ж. Уайт; В 3-х выпусках. Вып. 2: Внутрисистемные помехи и методы их уменьшения / Сокр. пер. с англ.; Под ред. А.И. Сапгира. – М.: Сов. радио, 1978. – 272 с.

4. Барсуков В.С. Комплексная защита от электромагнитного терроризма / В.С. Барсуков // Системы безопасности связи и телекоммуникаций. – 2000. – № 32. – С. 94-98.

5. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: учебное пособие / В.А. Петров и др. – М., 1993.

Надійшла до редколегії 21.04.2016

Рецензент: д-р техн. наук, проф. Л.Ф. Купченко, Харківський університет Повітряних Сил імені Івана Кожедуба, Харків.

К ВОПРОСУ О СУЩНОСТИ И ВИДАХ ИНФОРМАЦИОННОГО ОРУЖИЯ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ КОНФЛИКТАХ

В.Д. Карлов, Е.В. Лукашук, С.Н. Шолохов

В статье проанализированы особенности развития информационного оружия, которое применяется в современных конфликтах. На основании проведенного анализа выделены и проанализированы основные виды информационного оружия, а также определена сущность этого оружия в общей концепции ведения силовых информационных конфликтов.

Ключевые слова: *информационное оружие, радиоэлектронная борьба, беспилотные летательные аппараты, автоматизированные системы управления, высокоточное оружие.*

TO A QUESTION ESSENCE AND TYPES OF INFORMATIVE WEAPON IN MODERN INFORMATIVE CONFLICTS

V.D. Karlov, E.V. Lukashuk, S.M. Sholokhov

The features of development of informative weapon that is used in modern conflicts are analysed in the article. On the basis of the conducted analysis the basic types of informative weapon are distinguished and analysed, and essence of this weapon is certain in general conception of conduct of power informative conflicts.

Keywords: *informative weapon, radio electronic fight, unmanned aerial vehicles, automated control the system, high-fidelity weapon.*