УДК 351.86

А.М. Ткачов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

АНАЛІЗ ТЕХНОЛОГІЙ БОРОТЬБИ У ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Розглядається процес проведення інформаційних операцій, які представляють собою комплекс заходів, що мають на меті вплинути на інформаційно-управляючі системи противника при одночасного захисті своєї інформації та інформаційних систем. Проведено аналіз технологій боротьбі у інформаційному просторі.

Ключові слова: *інформаційна операція , інформаційна війна, інформаційний простір.*

Вступ

Зі зростанням народонаселення людина виявилася як би відокремленим від реальності, для неї все більшу роль набуває загальний соціально-інформаційний простір. Засоби масової інформації (ЗМІ) формують погляди людини, вона живе в інформаційному просторі, що створений масовими комуні-

каціями (МК). Будь-які події у світі існують для людини тільки тому, що вони представлені в ЗМІ. В даний час увійшло в повсякденний побут поняття віртуальної реальності, відповідне "уявної реальності, квазі-існуванню, коли світ сприймається як справжній, але насправді не існує "[1].

Метою даної статті є аналіз технологій боротьби у інформаційному просторі.

Основний матеріал

Предметом аналізу у даній статті є технології боротьби соціальних систем в інформаційної сфері з приводу впливу на ті чи інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, в результаті якого одні учасники суперництва отримують переваги, необхідні їм для подальшого розвитку, а інші їх втрачають [4]. Практична реалізація цього здійснюється шляхом проведення інформаційних операцій, які представляють собою комплекс заходів, що мають на меті вплинути на інформацію та інформаційно-управляючі системи (ІУС) противника при одночасному захисті своєї інформації та інформаційних систем [2]. Інформаційна війна(ІВ) являє собою відповідну операцію, проведену в період кризової ситуації або конфлікту (включаючи війну) для досягнення поставлених цілей над супротивником. Стосовно до інформаційних операцій (ІО) термін «супротивник» розглядається в більш широкому сенсі. Під ним маються на увазі організації, групи осіб чи окремі особи, які приймають рішення чи здійснюють дії, спрямовані на зрив виконання завдань, поставлених перед командуваннями Збройних Сил.

Підготовка та проведення інформаційних операцій (ІО) пов'язані з узгодженням і дозволом на рівні національного військово-політичного керівництва країни комплексу питань законодавчого та політичного характеру. ІО проводяться на всіх рівнях військових дій, межі між якими найчастіше носять умовний характер.

Наступальні і оборонні ІО можуть проводитися за єдиним задумом і планом і взаємно доповнювати один одного. Вони орієнтовані на одні й ті ж об'єкти впливу, в якості яких можуть виступати:

– органи управління держави та її Збройних Сил;

– ІУС цивільної інфраструктури (телекомунікаційні, включаючи засоби масової інформації, транспортні, енергетичного комплексу, фінансового та промислового секторів);

– керуючі елементи військової інфраструктури (системи зв'язку, розвідки, бойового управління, тилового забезпечення, управління зброєю);

– лінії, канали зв'язку і передачі даних;

– інформація, що циркулює або зберігається у системах управління;

– суспільство в цілому (як цивільне населення, так і особовий склад Збройних Сил), його державні, економічні та соціальні інститути;

– керівний склад і персонал автоматизованих систем управління, який бере участь у процесі прийняття рішень.

У технічних системах під управлінням розуміється «процес організації такого цілеспрямованого впливу на об'єкт, у результаті якого цей об'єкт переводиться в необхідний (цільовий) стан» [6]. В якості об'єкта управління будемо розглядати масову й індивідуальну свідомість людини в системі управління. Стан об'єкта змінюється під дією середовища, в якій він знаходиться.

Нехай X – стан середовища, якій взаємодіє з об'єктом, а Y – стан об'єкта (1). Тоді об'єкт можна представити як перетворювач F^0 стану середовища у стан об'єкта [7]:

$$Y = F^0(X) \qquad (1)$$

де F^0 – поки невідомий оператор зв'язку входу X і виходу Y об'єкта, що характеризує специфіку його роботи.

Говорячи про управління як про цілеспрямоване процесі, не можна обійти того, чиї цілі реалізуються в процесі управління. Для цього необхідно ввести поняття «суб'єкта», який є джерелом цілей, що реалізуються управлінням. У «ідеалі» суб'єктом має бути держава, проте в якості нього можуть виступати будь-які суб'єкти, або їх сукупність.

Об'єктом боротьби у інформаційному просторі є будь-який об'єкт, до якого можливе здійснення інформаційного впливу (в тому числі - застосування інформаційної зброї) або іншого впливу (силового, політичного, економічного і т.д.), результатом якого буде модифікація його властивостей як інформаційної системи [4].

Якщо стан Y об'єкта задовольняє потребам суб'єкта, що взаємодіє з цим об'єктом і його експлуатує, то ніякого управління не потрібно. Якщо ж стан об'єкта чому-небудь не задовольняє потреб суб'єкта, то останній повинен організувати такий вплив на об'єкт, який б перевів об'єкт в новий стан, що задовольняє суб'єкта [7].

Інформація <X', Y'> утворює сенсорну середу суб'єкта, тобто ту частину середовища <X, Y>, яку він здатний сприйняти своїми сенсорами. Зручно вважати, що суб'єкт завжди з приводу будь-якого об'єкта формулює свою мету (цілі) Z *, реалізація якої в об'єкті призведе, на думку суб'єкта, до задоволення його потреб. Ця мета являє собою набір вимог, що пред'являються суб'єктом до стану Y об'єкта. Виконання цільових вимог Z * в об'єкті визначається рівністю

$$Y = Z^*, \qquad (2)$$

а невиконання – нерівністю

$$Y \neq Z^*. \qquad (3)$$

При відсутності управління цілі суб'єкта не реалізуються. У результаті суб'єкту доводиться вирішувати дилему:

1) або змиритися з існуючим станом, вираженим нерівністю (3), і тим самим терпіти певний збиток, пов'язаний з незадоволенням своїх потреб;

2) або створити систему управління, яка реалізувала б його мети Z * в об'єкті, тобто добитися виконання рівності (2), але при цьому затратити певні ресурсі на її створення та експлуатацію.

У всякому разі, для реалізації управління необхідно створити канал управління U, за допомогою якого можна впливати на стан об'єкта управління:

$$Y = F^0(X, U), \qquad (4)$$

де F^0 – як і раніше оператор роботи об'єкта, але враховує наявність чинника управління U.

Блок-схема системи управління у інформаційному просторі показана на рис. 1.

Тут D_X і D_Y – датчики, що вимірюють стан середовища та об'єкта відповідно. Результати вимірювань

$$\begin{cases} X' = D_X(X) \\ Y' = D_Y(Y) \end{cases} \qquad (5)$$

надходять на керуючий пристрій (КП) – орган управління, який виробляє команди управління U. Ці команди повинні бути оброблені виконавчими механізмами, з тим щоб змінити стан керованого входу U' об'єкту.

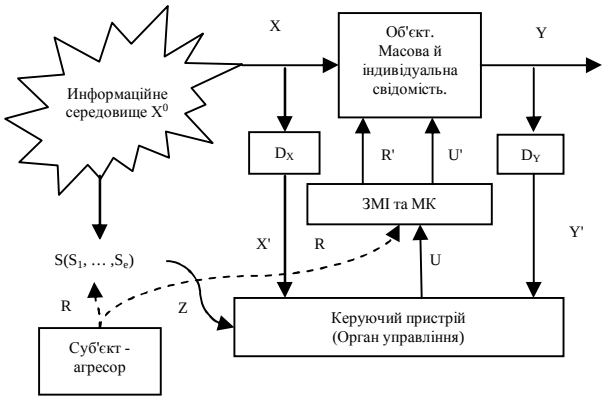

Рис. 1. Блок-схема системи управління у інформаційному просторі

Для функціонування керуючого пристрою йому потрібно повідомити мету Z* управління, а також алгоритм управління φ – вказівку, як добиватися поставленої мети, володіючи інформацією про стани середовища, об'єкта і мети:

$$U = \varphi(X', Y', Z^*). \qquad (6)$$

Як видно з рис. 1, управління пов'язано перш за все з цілями {Z *}, які надходять ззовні в систему управління. Ці цілі утворює (генерує) суб'єкт, який і є споживачем майбутньої системи управління об'єктом. Суб'єкт виступає в якості замовника і споживача створюваної системи управління. [7]

Таким чином, КП сприймає навколишнє середовище як кінцевий або нескінченний набір її параметрів

$$S = (s_1 \dots s_e) \qquad (7)$$

кожен з яких цікавить суб'єкта і може бути ним змінено. Сприйнята суб'єктом ситуація завжди керована:

$$S(U, R) = (s_1(U, R), \dots, S_e(U, R)), \qquad (8)$$

де U, R – управління суб'єктів.

Проте свої цілі УУ формулює не в термінах середовища S: суб'єкту зручніше оперувати іншими, властивими йому поняттями (назвемо їх цільовими).

Нехай ці цільові поняття описуються вектором

$$Z = (z_1 \dots z_e), \qquad (9)$$

де кожен цільовий параметр z_i однозначно визначається ситуацією S, тобто

$$z_i = \psi_i(S)(i = 1, \dots, k) \Rightarrow Z = \psi(S), \qquad (10)$$

где $\psi(S) = (\psi_i(S), \dots, \psi_k(S))$, а функції $\psi_i(S)$ визначають зв'язок стану середовища та цільового параметра z_i. Якщо розглядати k-мірний простір цілей {Z}, то в ньому суб'єкт може сформулювати свою мету як $Z^* \in \{Z\}$.

Виходячи з описаної інформаційної системи та визначення захищеності, всі загрози можна розділити на два види:

I. Загрози неадекватної оцінки керуючим пристроєм дійсності (X ', Y', S).

До цього типу загроз відносяться:

1) Неадекватне сприйняття суб'єктом навколишнього середовища при формуванні простору ситуацій {S}, тобто $X'' \neq X^0$.

2) Формування простору ситуацій {S} на основі неправдивої інформації R, що надається суб'єктом-агресором.

3) Некоректна робота датчика D_X і видача їм необ'єктивної інформації, тобто $X' \neq X$.

4) Некоректна робота датчика D_Y та видача їм необ'єктивної інформації, тобто $Y' \neq Y$.

II. Загрози порушення процесу управління над об'єктом (U, R);

До цього типу загроз відносяться:

1. Несприятливі умови навколишнього середовища X^0, негативно сприймаються об'єктом управління.

2. Існування власної інформаційної інфраструктури суб'єкта-агресора, здатної донести інформацію R до об'єкта управління.

3. Генерування інформаційних потоків R суб'єктом-агресором у ЗМІ та МК керуючого пристрою.

4. Порушення цілісності інформації U' суб'єктом-агресором.

5. Вихід з ладу або порушення роботи системи адміністративно-організаційного управління.

Суб'єкт-агресор може здійснювати наступні види атак:

I. Підготовчий етап. Атаки, орієнтовані на збір інформації про роботу системи, стратегії управління, за допомогою перехоплення і аналізу інформа-

ційних потоків, а також іншими технічними та організаційними методами.

II. Етап реалізації загроз безпеці

A. впровадження у комунікаційні засоби загальної схеми управління. Загрози (I.3), (I.4), (II.3), (II.5);

B. отримання суб'єктом-агресором ЗМІ та МК. Загрози (II.2);

C. радіоелектронне придушення суб'єктом-агресором інформаційних потоків. Загрози (II.4);

D. дезінформація, імітація і демонстративні дії, що вводять супротивника в оману. Загрози (I.1), (I.2);

E. диверсійні акції і спеціальні інформаційні операції. Загрози (II.5);

F. нав'язування противнику (КП) фіктивних наукових досліджень. Загрози (I.3);

G. застосування економічних і політичних санкцій проти противника. Загрози (II.1), (II.5);

H. порушення роботи апаратних і програмних засобів УУ. Загрози (II.4), (II.5);

I. підміна джерел мовлення. Загроза (II.4);

J. поширення інформації (а так само програм-спостерегачів, програм-вірусів) через загальну середу передачі (Internet). Загрози (II .2), (II .3);

III. Етап реалізації інформаційного впливу на об'єкт.

Враховуючи це, можна сформулювати основні принципи ведення боротьби у інформаційному просторі [4]:

1. Використання принципу інформаційної асиметрії, трансформація структури інформаційного простору супротивника з метою створення і маскування у його інформаційних об'єктів нових, асиметричних, властивостей, вразливих для асиметричного зброї.

2. Скритність і анонімність оперування інформаційно-психологічними впливами, можливість проведення їх з будь-якої точки інформаційного простору.

3. «Плавність» перемикання інформаційних впливів, регульована в широких межах інтенсивність і тривалість їх реалізації.

4. Багатоаспектність і многооб'ектность впливу з високим ступенем координації в часі і просторі.

5. Здатність «малими» інформаційними впливами отримати «великі» кінцеві результати.

6. Перенесення функцій стримування на інформаційну сферу.

7. Інформатизація як головний резерв підвищення ефективності силових (військових) акцій.

8. Наведення хаосу в інформаційному середовищі та подальше управління ним – як один з принципів отримання потрібних результатів [8].

Висновки

Таким чином, розглянуто технології боротьби в інформаційної сфері з приводу впливу на ті чи інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, в результаті якого одні учасники суперництва отримують переваги, необхідні їм для подальшого розвитку, а інші їх втрачають

Список літератури

1. Ортега-и-Гассет Х. Избранные труды: пер. с исп. / А.М. Руткевич (сост., предисл. и общ. ред.). – М.: Весь Мир, 1997. – 704 с.

2. Жуков В. Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. – 2001. – № 1, – С. 2-9.

3. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны: моногр. / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. – М.: Горячая линия-Телеком, 2003 г. – 541 с.

4. Манойло А.В. Объекты и субъекты информационного противоборства. [Електронний ресурс]. – Режим доступу до ресурсу: http: // www.psyfactor.org.

5. Растригин Л.А. Системы экстремального управления / Л.А. Растригин. – М.: Наука, 1974. – 632 с.

6. Растригин Л.А. Адаптация в сложных системах / Л.А. Растригин. – Рига: Зинатне, 1981. – 375 с.

7. Расторгуев С.П. Информационная война / С.П. Расторгуев. – М.: Радио и связь, 1999. – 416 с.

8. [Електронний ресурс]. – Режим доступу до ресурсу: http://www.psyfactor.org.

Надійшла до редколегії 28.10.2010

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

АНАЛИЗ ТЕХНОЛОГИЙ БОРЬБЫ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

А.М. Ткачев

Рассматривается процесс проведения информационных операций, которые представляют собой комплекс мероприятий, направленных на оказание воздействия на информационно-управляющие системы противника при одновременной защите своей информации и информационных систем. Проведен анализ технологий борьбы в информационном пространстве.

Ключевые слова: *информационная операция, информационная война, информационное пространство.*

ANALYSIS OF CONFRONTATION TECHNOLOGY IN THE INFORMATION SPACE

A.M. Tkachev

We consider the process of conducting information operations, which represent a set of activities aimed at influencing the information and control systems of the enemy while protecting its information and information systems. The analysis of confrontation technology in information space.

Keywords: *informational confrontation, information warfare, information space.*