УДК 351.86

А.М. Ткачов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ

Розглянуто оцінку захищеності інформаційно-управляючих систем у процесі суперництва соціальних систем в інформаційному середовищі 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. Наведено вирази для оцінки ризиків. Зміну стану безпеки можна оцінити по швидкості зміни цих ризиків і тим самим визначити ефективність застосовуваної політики безпеки у інформаційно-управляючої системі.

***Ключові слова*:** *оцінка захищеності, інформаційна система, інформаційна операція.*

Вступ

Практична реалізація інформаційної боротьби здійснюється шляхом проведення інформаційних операцій (ІО), 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 [1]. Підготовка та проведення інформаційних операцій 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.

Метою даної статті є оцінка ризиків реалізації загроз безпеки інформаційно-управляючих систем у процесі інформаційної боротьби.

Основний матеріал

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

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

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

Тут D_X і D_Y – датчики, що вимірюють стан середовища та об'єкта відповідно. Результати вимірювань X', Y' надходять на керуючий пристрій (КП) – орган управління, який виробляє команди управління U. Для функціонування керуючого пристрою йому потрібно повідомити мету Z * управління, а та-

кож алгоритм управління φ – вказівку, як добиватися поставленої мети, володіючи інформацією про стани середовища, об'єкта і мети:

$$U = \varphi(X', Y', Z^*). \quad (2)$$

Ці параметри утворює (генерує) суб'єкт, який і є споживачем майбутньої системи управління об'єктом. Суб'єкт виступає в якості замовника і споживача створюваної системи управління [3].

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

$$S = (s_1 \dots s_e), \quad (3)$$

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

$$S(U, R) = (s_1(U, R), \dots, S_e(U, R)), \quad (4)$$

де U, R – управління суб'єктів. Проте свої цілі КП формулює не в термінах середовища S: суб'єкту зручніше оперувати іншими, властивими йому поняттями (назвемо їх цільовими).

Значення ризику будемо розглядати як сукупність потенційної ймовірності реалізації загрози і тяжкості можливих наслідків. У кожному конкретному випадку ризик можна визначити за сукупність декількох факторів:

1. Людський фактор.

Людський фактор порушує стан захищеності системи у зв'язку з «неадекватною» діяльністю персоналу, який є результатом:

– неможливості виконання людиною, покладеного на нього обсяг робіт;

– умисні дії співробітника, що порушують встановлені правила функціонування системи, які є результатом адаптації людини до умов середовища;

– некомпетентність співробітника.

Якщо один співробітник у середньому виконує певний обсяг роботи x, то N співробітників виконають обсяг роботи xN. Якщо для повного виконання роботи необхідно N_0 осіб, то обсяг невиконаної роботи буде пропорційний (N_0 – N). У результаті ризик з цього та інших двох показниками можна виразити наступною формулою:

$$R_ч \propto k(N_0 - N)\left[\sum_{n=1}^{N}(p_n \cdot \nu_n) + 1\right], \quad (5)$$

де k – коефіцієнт важливості даної організаційної структури; N_0 – мінімально необхідна кількість людей необхідних для реалізації організацією своїх функцій; N – кількість співробітників; ν_n – важливість займаної людиною посади, по можливості впливу на процеси в організації, а так само рівень його інформованості про процеси організації; p_n – ймовірність «неадекватного» поведінки співробітника. Вона характеризується якістю підбору персоналу та організаційно-правовими заходами. Величину p_n, окрім $n_j u_j$, можна оцінити й емпіричним шляхом за кількістю інцидентів.

2. Технічний (програмно-апаратний) фактор

$$R_T \propto k\sum_{n=1}^{N}(p_n \cdot \nu_n), \quad (6)$$

де k – як і в попередньому випадку, коефіцієнт важливості даної організаційної структури; N – загальна кількість комплексних засобах автоматизації (КЗА); ν_j – важливість КЗА в загальній організаційній структурі за кількістю оброблюваної інформації та її значущості; p_j – ймовірність реалізації несанкціонованих дій(НСД) у КЗА. Цю величину можна визначити в результаті зіставлення певної ймовірності реалізації загроз класами захищеності КЗА від НСД.

Знайти p_j можна на основі nfгих показників:

– міцність багаторівневого захисту;

– міцність багатоланкової захисту;

– ймовірність відмови обладнання.

3. Фактор середовища

$$R_C \propto \frac{\left\langle f_э \cdot f_{инф} \right\rangle_{суб.агр.}}{\left\langle f_э \cdot f_{инф} \right\rangle_{уу}}. \quad (7)$$

– Якщо один з показників ($f_э$ або $f_{инф}$) дорівнює нулю, то в результаті ефективність інформаційного протиборства суб'єкта дорівнює нулю.

– Складання показників не має сенсу, через різні розмірності.

Однак у складних системах, що складаються з більшого числа елементів лінійні закони, як правило, не мають місце [3]. Найбільш часто тут спостерігаються показові закони.

Кінцевий результат реалізації будь-якої загрози – це генерація інформаційного потоку. Ризик генерації шкідливого потоку можна визначити як:

$$R \propto e^{\left[\sum_{i=1}^{N}(p_i D_i O_i)\right]}, \quad (8)$$

де N – кількість комунікаторів; p_i – імовірність генерації суб'єктом-агресором інформаційного потоку в даному комунікаційному пристрої. Ця величина утворюється сукупністю попередніх трьох факторів ($R_ч$, R_T, R_C), а так само законодавчих і організаційних заходів:

$$p_i = 1 - \frac{1}{e^{q(R_ч + R_T + R_c)}}. \quad (9)$$

Ця формула отримана виходячи з того, що ризики ($R_ч$, R_T, R_C) визначають інтенсивність успішних атак на систему; q – емпірично визначається коефіцієнт;

D_i – ступінь довіри до джерела. Лінійна залежність від цього показника обґрунтовується у багатьох роботах по психології масової поведінки; O_i – обсяг аудиторії (кількість людей), що сприймають цей комунікативний потік.

Експоненціальна форма даного закону (8) визначає швидкість розповсюдження збурень в хаотичних фрактальних системах. Експоненціальна

залежність зберігається лише до тих пір, поки ступінь досить мала. Чим більше стає ступінь, тим більше лінійної стає залежність. Це відображає «асиметричність», як основний принцип інформаційного протиборства. Всі ці формули не дають точних показників, а тільки показують залежність величин, тому замість рівності скрізь стоїть знак пропорційності [3].

Ризики, отримані за цими формулами, є безрозмірними, а їхні значення для оцінки безпеки системи управління якісними, але не кількісними. Безрозмірні величини набувають сенсу тільки при порівнянні їх один з одним. Порівнюючи показники цих ризиків у різні моменти часу, можна оцінити який стан системи більш безпечний. Зміну стану безпеки можна оцінити по швидкості зміни цих ризиків і тим самим визначити ефективність застосовуваної політики безпеки:

$$V_{эф} = V_{эф}\left(\frac{R_ч}{dt}, \frac{R_т}{dt}, \frac{R_с}{dt}\right). \qquad (10)$$

Без зниження цих показників будь-які заходи спрямовані на забезпечення інформаційної безпеки будуть безрезультатні.

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 багатооб'єктность 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.

Висновки

Таким чином, у статті розглянуто оцінку захищеності інформаційно-управляючих систем у процесі суперництва соціальних систем в інформаційному середовищі 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. Наведено вирази для оцінки ризиків. Зміну стану безпеки можна оцінити по швидкості зміни цих ризиків і тим самим визначити ефективність застосовуваної політики безпеки у інформаційно-управляючої системі.

Список літератури

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

2. [Електронний ресурс]. – Режим доступу до ресу: http: // www.cplire.ru / win / InformChaosLab / chaoscomputerra / Loskutov.html.

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

Надійшла до редколегії 14.12.2010

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

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

А.М. Ткачёв

Рассмотрена оценка защищенности информационно-управляющих систем в процессе соперничества социальных систем в информационной среде по поводу влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их теряют. Приведены выражения для оценки рисков. Изменение состояния безопасности можно оценить по скорости изменения этих рисков и тем самым определить эффективность применяемой политики безопасности в информационно-управляющей системе.

Ключевые слова: *оценка защищенности, информационная система, информационная операция.*

INFORMATION CONFRONTATION

A.M. Tkachev

We consider the evaluation of security information management systems in the rivalry of social systems in the information environment over the impact on those or other areas of social relations and to establish control over the sources of strategic resources, which resulted in some participants receive the benefits of competition, they need further development, while others they lose. The expressions obtained for the risk assessment. Changing the security status can be assessed by the rate of change of these risks and thereby determine the effectiveness of policies to be applied in the information management system.

Keywords**:** *assessment of security, information system, information operations.*