УДК 681.3.004

О.С. Петров[1], А.В. Бородулін[2], А.В. Мінін[1]

[1]*Східноукраїнський національний університет ім. Володимира Даля, Луганськ*
[2]*Служба безпеки України, Ялта*

МОДЕЛЬ АНАЛІЗУ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОМП'ЮТЕРНІЙ МЕРЕЖІ

Запропонована математична модель аналізу загроз інформаційної безпеки комп'ютерних мереж організацій. Описані основні математичні множини даної моделі, приведені основні задачі та ознаки, використовувані при моделюванні живучості комп'ютерних мереж.

Ключові слова: *живучість комп'ютерної мережі, множина, аспекти ІБ, методи і засоби реалізації загрози, оцінка ризиків.*

Постановка проблеми

Сучасні комп'ютерні мережі (КМ) будуються, як правило, з використанням персональних комп'ютерів (ПК) і обчислювальних локальних мереж (ОЛМ), побудованих на базі стандартних мережевих технологій. Задача забезпечення живучості КМ розділяється на дві підзадачі:

– забезпечення структурної живучості;

– забезпечення функціональної живучості.

Під забезпеченням структурної живучості мається на увазі установка додаткової апаратури і ліній зв'язку або модернізація існуючих компонентів надійнішими. Забезпечення функціональної живучості може бути досягнуте за рахунок нових моделей і процедур організації обчислювального процесу. Якщо мінімізація вартості КМ переважає (що характерно для середніх і малих організацій), то рішення другої підзадачі є переважним.

У сучасній науці теорія живучості складних технічних систем, у тому числі і обчислювальних, переживає етап становлення в самостійну наукову дисципліну. Спостерігається явний недолік моделей і алгоритмів синтезу живучих КМ, особливо у задачах побудови систем управління і передачі даних на базі ПК із застосуванням стандартних мережевих технологій, що функціонують в умовах можливої загрози витоку інформації.

Погрози інформаційної безпеки в КМ розділені за трьома ознаками:

– джерело загрози,

– об'єкт загрози,

– методи і засоби реалізації загрози.

Кожна з виділених ознак містить свої характеристики, які відображають її особливості та характерні погрози. Джерело загрози має дві важливі характеристики – тип і розташування; об'єкт загрози характеризується типом і метою загрози; методи і засоби реалізації загрози обумовлені особливостями джерела і об'єкту загрози.

Виклад основного матеріалу

Множина джерел загрози можна представити у вигляді матриці:

$$Y = \begin{pmatrix} Y_A^{int}\ Y_A^{ext} \\ Y_T^{int}\ Y_T^{ext} \\ Y_C^{int}\ Y_C^{ext} \end{pmatrix} \text{ або } Y=\{ Y_j^k \}, \qquad (1)$$

де j – індекс типу джерела загрози, j = {A, T, C}; Y_A – множина антропогенних джерел загрози; Y_T – множина техногенних джерел загрози; Y_C – множина стихійних джерел загрози; k – індекс розташування джерела загрози; k = {int, ext}; Y_{int} – множина внутрішніх джерел загрози; Y_{ext} – множина зовнішніх джерел загрози.

Множина об'єктів погроз представлена у вигляді матриці розмірністю n × 3:

$$U = \begin{pmatrix} U_1^{конф} & U_1^{ціл} & U_1^{дост} \\ U_2^{конф} & U_2^{ціл} & U_2^{дост} \\ U_3^{конф} & U_3^{ціл} & U_3^{дост} \\ -- & -- & -- \\ U_n^{конф} & U_n^{ціл} & U_n^{дост} \end{pmatrix} \text{ або } U = \{ U_i^m \}, \quad (2)$$

де i – індекс об'єкту загрози; m – визначник мети порушення аспекту інформаційної безпеки (ІБ), $U_i^{конф}$ – елемент з порушеною конфіденційністю, $U_i^{цел}$ – елемент з порушеною цілісністю, $U_i^{дост}$ – елемент з порушеною доступністю; конф – визначник порушеної конфіденційності; ціл – визначник порушеної цілісності; дост – визначник порушеної доступності.

Вважаючи, що будь-яке джерело загрози направлене на будь-який елемент КМ з метою порушення будь-якого аспекту ІБ, задається бінарне відношення $\eta_l = \left(Y_j^k, U_i^m \right)$, реальних пар «джерело загрози – елемент загрози», де

$$\eta_l \in Y \times U = \left\{ \left(Y_j^k, U_i^m \right) \mid Y_j^k \in Y, U_i^m \in U \right\}.$$

Будь-яке джерело загрози, що направлене на конкретний елемент і має певну мету порушення аспекту ІБ КМ, використовує для реалізації методи і пов'язані з ними засоби, ці зв'язки можна описати наступним бінарним відношенням $\eta_2 = \left(z_e, l_q \right)$, $z_e \in Z$, $l_q \in L$, де Z – множина способів реалізації загрози; L – множина засобів реалізації загрози.

Таким чином, можна записати, що якщо у множині $Y \times U$ задано бінарне відношення $\eta_l = \left(Y_j^k, U_i^m \right)$, і у множині $Z \times L$ задано бінарне відношення $\eta_2 = \left(z_e, l_q \right)$, то можливе відображення f, відповідність $\left(Y_j^k, U_i^m \right) \xrightarrow{f} \left(z_e, l_q \right)$ яке має наступні особливості: значення функції залежать від змінних Y_j^k и U_i^m; умови бієкції не виконуються, оскільки не виконуються умови ін'єкції (область визначення задається парами $\left(Y_j^k, U_i^m \right)$ на множині $Y \times U$, а значення функції з множини $Z \times L$ для різних елементів можуть збігатися). Відображення f є сюр'єктивним, а завдання множини пар $\left(z_e, l_q \right)$ виконується експертними процедурами.

Таким чином, формалізований опис погроз КМ має вигляд:

$$S = \left(Y_j^k, U_i^m, z_e, L_n \right), \qquad (3)$$

де Y_j^k - визначник джерела загрози, що характеризується типом і розташуванням; U_i^m - визначник об'єкту загрози, що характеризується типом елементу КМ і метою порушення аспекту ІБ КМ; z_e - визначник e-го методу реалізації загрози; L_n - визначник n-ї підмножини засобів реалізації загрози.

Множина значущих чинників КМ представляється $R = \{R_H, R_F, R_S\}$, де R_H – множина людських чинників, R_F – множина фізичних ресурсів, R_S – множина інформаційних ресурсів. У свою чергу, кожен з типів чинників є множиною, що містить елементи: $R_j = \{r_{ji}\}$, де j – ідентифікатор типа ресурсу, i – номер j-го типа ресурсу. Вважаючи, що множина погроз ІБ направлена на всі елементи КМ, тобто $\exists \tau_1 \in R \times S = \left\{ \left(r_{JI}; u_i \right) \right\}$ має місце (3), то бінарне відношення τ_1 визначається однозначно по об'єкту загрози, тобто $r_{ji} \equiv U_i^m$.

Для множини погроз ІБ КМ існує множина заходів щодо їх нейтралізації: $V = \{v_i\}$. Бінарне відношення реальних пар «загроза – методи нейтралізації» має вигляд: $\tau_2 \in U \text{ x } V = \{(u_i; v_i)\}$. Окрім цього, відділ по ІБ КМ передбачає захист всіх ресурсів КМ, тобто з кожним ресурсом КМ пов'язана множина заходів щодо організації ІБ, що відбивається бінарним відношенням $\tau_3 \in R \text{ x } W = \{(r_{ji}; w_i\}$, де R – множина ресурсів організації; W – множина заходів щодо організації ІБ, направлених на захист КМ.

Процес оцінки рівня організації ІБ КМ представляється композицією бінарних стосунків $\tau_2 \circ \tau_1$, де $\tau_1 = \{(r_{ji}; u_i\}$, $\tau_2 = \{(u_i; v_i)\}$, $\tau_3 = \{(r_{ji}; v_i\}$. Якщо $\tau_2 \circ \tau_1 \le \tau_3$, $\left(u_i; v_i \right) \circ \left(r_{ji}; u_i \right) \le \left(r_{ji}; w_i \right)$, то можна стверджувати, що рівень ІБ достатній для захисту ресурсу, вважаючи, що множина заходів щодо організації ІБ, направлених на ресурси, більше множини заходів щодо нейтралізації погроз або збігається з ним, тобто $v_i \le w_i$. Якщо $\tau_2 \circ \tau_1 > \tau_3$, $\left(u_i; v_i \right) \circ \left(r_{ji}; u_i \right) > \left(r_{ji}; w_i \right)$, тобто $v_i > w_i$, то можна стверджувати, що рівень ІБ недостатній для захисту КМ, і існують уразливості, через які може бути реалізована загроза. Тоді необхідно довизначити множину w_i до v_i, так, щоб принаймні, виконувалася тотожність $v_i \equiv w_i$.

Вибір заходів щодо ІБ визначається нечіткою відповідністю множини S и W: K = {S,W,F}, де F – функція приналежності S·W, яке задається у вигляді графа з множиною вершин S∪W, кожна дуга якого позначає функцію приналежності $\mu_F \left(s_i, w_j \right)$ або за допомогою матриці інциденції R_K, рядки якої помічені елементами w_j, а стовпці – s_i, на пересіченні рядків і стовпців розташований елемент $k_h = \mu_F \left(s_i, w_j \right)$, де μ_F - функція приналежності елементів нечіткому графіку.

Хай, наприклад K={S,W,F}, $h = \overline{1,6}$;

$$F = \left\{ \begin{matrix} \left\langle k_1 / (s_1, w_1) \right\rangle, \left\langle k_2 / (s_1, w_4) \right\rangle, \left\langle k_3 / (s_2, w_1) \right\rangle, \\ \left\langle k_4 / (s_3, w_2) \right\rangle, \left\langle k_5 / (s_4, w_1) \right\rangle, \left\langle k_6 / (s_4, w_3) \right\rangle \end{matrix} \right\}. \qquad (4)$$

Матриця інциденції R_K і граф нечіткої відповідності дозволяють вибрати для даного прикладу заходи щодо ІБ шляхом селекції максимальних значень k_h по кожному стовпцю (рис. 1).

Для генерації варіантів заходів щодо ІБ завдання оптимізації, залежно від вимог користувача, формулюється в двох варіантах.

Перший варіант. Відомі вартості ресурсів організації, погроз, методів і засобів захисту ресурсів від погроз: $c\left(r_{ji} \right), c\left(s_i \right), c\left(w_i \right)$. Слід визначити при заданих значеннях ризиків з врахуванням проведеної селекції мінімальні витрати на організацію ІБ. При цьому введені обмеження: вартість ресурсу більше або дорівнює вартості загрози, направленої

на нього, інакше засоби, витрачені на реалізацію загрози, економічно не виправдані. З тієї ж причини вартість ресурсу більше або дорівнює вартості заходів щодо його захисту. Тоді маємо (5).

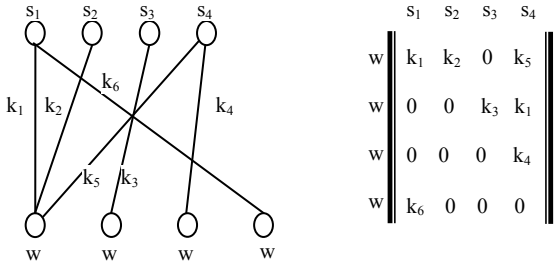

Рис. 1 Графічне і матричне завдання нечіткої відповідності K = {S,W,F}

Другий варіант. Відомі вартості ресурсів організації, погроз, методів і засобів захисту ресурсів від погроз: $c(r_{ji}), c(s_i), c(w_i)$. Необхідно визначити мінімальне значення ризиків при заданому значенні витрат на ІБ. При тих же обмеженнях маємо (6).

$$\begin{cases} C_{ИБ} = \sum_{i=1}^{n} c(w_i) \to \min; \\ C_{риск} = \sum_{i=1}^{m} f(r_{ji}, s_i) \le C_{зад}; \\ c(s_i) \le c(w_i) \le c(r_{ji}); \\ c(s_i); c(r_{ji}); c(w_i); j = \overline{1,m}; \end{cases} \quad (5)$$

$$\begin{cases} C_{риск} = \sum_{i=1}^{m} f(r_{ji}, u_i) \to \min; \\ C_{ИБ} = \sum_{i=1}^{n} c(w_i) \le C_{зад}; \\ c(s_i) \le c(w_i) \le c(r_{ji}); \\ c(s_i); c(r_{ji}); c(w_i); j = \overline{1,m}. \end{cases} \quad (6)$$

Вибір оптимального варіанту з множини, що згенерувала, ідентичний типовому завданню ухвалення рішення групою експертів з використанням теорії нечіткої множини.

Висновок

Розроблена модель аналізу загроз інформаційної безпеки організації включає декілька етапів. Перший етап – створення моделі об'єкту ІБ, яка формується шляхом внесення до системи повної інформації про всі ресурси організації, що входять в КС організації. Другий етап - оцінка важливості ресурсів з точки зору ІБ, визначення відповідності між існуючим і необхідним рівнями ІБ в організації. Третій етап - виявлення вразливостей і оцінка ризиків. Виконання дій з даних етапів формує на виході повну модель об'єкту ІБ з врахуванням реального виконання вимог. Побудована модель аналізується і генерується в звіт, який містить значення ризиків для кожного компонента КМ. Користувач задає критерії оптимізації, по яких генеруються оптимальні варіанти заходів щодо ІБ.

Список літератури

1. Модели принятия решений на основе лингвистического перемещения / А.Н. Борисов и др. – Рига: З, 1982. – 296 с.

2. Глушков В.М. О системной оптимизации / В.М. Глушков // Кибернетика. – 1980. – № 5. – С. 89-91.

3. Михалевич В.С. Вычислительные методы исследования и проектирования сложных систем / В.С. Михалевич, В.Л. Волкович. – М.: Наука, 1984. – 286 с.

4. Пятибратов А.П. Концептуальные положения оценки надежности и отказоустойчивости распределенной локальной компьютерной сети ВУЗа / А.П. Пятибратов, Мутаз Халед Абдель-Вахед // Открытое образование: журнал. – 2006. – № 5. – С. 37-41.

Надійшла до редколегії 26.03.2010

Рецензент: д-р техн. наук, проф. В.А. Лужецький, Вінницький національний технічний університет, Вінниця.

МОДЕЛЬ АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНОЙ СЕТИ

А.С. Петров, А.В. Бородулин, А.В. Минин

Предложена математическая модель анализа угроз информационной безопасности компьютерных сетей организаций. Описаны основные математические множественные числа данной модели, приведены основные задачи и признаки, используемые при моделировании живучести компьютерных сетей.

Ключевые слова: *живучесть компьютерной сети, множественное число, аспекты информационной безопасности, методы и средства реализации угрозы, оценка рисков.*

A MODEL OF ANALYSIS OF THREATS INFORMATIVE SAFETY IS IN COMPUTER NETWORK

A.S. Petrov, A.V. Borodulin, A.V. Minin

The mathematical model of analysis of threats informative safety of computer networks of organizations is offered. The basic mathematical plurals of this model are described, basic tasks and signs, used for the design of vitality of computer networks, are resulted.

Keywords: *vitality of computer network, plural, aspects of informative safety, methods and facilities of realization of threat, estimation of risks.*