

УДК 004.8

## Формалізація рівня загроз інформаційної безпеки підприємства

Савеленко О.К., викладач, kolodochkinaek@i.ua

Кіровоградський національний технічний університет, м. Кіровоград

Забезпечення інформаційної безпеки є важливим завданням для будь-якої організації, оскільки від збереження конфіденційності, цілісності і доступності інформаційних ресурсів багато в чому залежать якість і оперативність ухвалення управлінських рішень, ефективність їх реалізації.

Держава, регламентуючи стосунки в інформаційній сфері, не здатна виконати в повному об'ємі із завданнями забезпечення безпеки усіх суб'єктів інформаційних стосунків, однозначно відповідаючи лише за захист інформації, що становить державну таємницю. Тому в умовах різних форм власності ці завдання в повному об'ємі повинні вирішуватися керівниками організацій.

Це завдання може бути вирішене на базі експертних систем підтримки прийняття рішень, які реалізують спеціальні методики обстеження організацій і видачі рекомендацій по забезпеченню їх інформаційної безпеки [1].

При використанні апарату чітких і нечітких множин формалізований опис процесу забезпечення інформаційної безпеки організації в експертних системах підтримки прийняття рішень (СППР) можливо здійснити при послідовному визначенні наступних етапів:

- рівня загроз інформаційної безпеки;
- ресурсів організації, як об'єктів загроз;
- оцінки рівня забезпечення інформаційної безпеки організації;
- генерації рекомендацій по досягненню заданого рівня.

Розглянемо перший етап СППР, а саме, формалізацію рівня загроз інформаційної безпеки.

Загрози інформаційної безпеки в організації розділені за трьома ознаками: джерело загрози, об'єкт загрози, методи і засоби реалізації загрози. Кожна з виділених ознак містить свої характеристики, особливості, що відображають її, і загрози, що впливають на характер. 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.

Множина джерел загрози представлена у вигляді матриці розмірністю  $3 \times 2$  :

$$I = \begin{pmatrix} I_A^{in} & I_A^{out} \\ I_T^{in} & I_T^{out} \\ I_C^{in} & I_C^{out} \end{pmatrix}, \quad (1)$$

або

$$I = \{I_j^k\}, \quad (2)$$

де  $j$  - індекс типу джерела загрози,  $j = \{A, T, C\}$ ,  $I_A$  - множина антропогенних джерел загрози;  $I_T$  - множина техногенних джерел загрози;  $I_C$  - множина стихійних джерел загрози;  $k$  - індекс розташування джерела загрози,  $k = \{in, out\}$ ,  $I^{in}$  - множина внутрішніх джерел загрози,  $I^{out}$  - множина зовнішніх джерел загрози.

Множина об'єктів загроз представлена у вигляді матриці розмірністю  $n \times 3$  :

$$O = \begin{pmatrix} O_1^K & O_1^Q & O_1^D \\ O_2^K & O_2^Q & O_2^D \\ O_3^K & O_3^Q & O_3^D \\ \dots & \dots & \dots \\ O_t^K & O_t^Q & O_t^D \end{pmatrix}, \quad (3)$$

або

$$O = \{O_i^m\}, \quad (4)$$

де  $i$  – індекс об'єкта загрози;  $m$  – ідентифікатор цілі порушення аспекту інформаційної безпеки (ІБ);  $O_i^k$  – об'єкт з порушеною конфіденційністю;  $O_i^q$  – об'єкт з порушеною цілісністю;  $O_i^p$  – об'єкт з порушеною доступністю;  $K$  – ідентифікатор порушеної конфіденційності;  $Q$  – ідентифікатор порушеної цілісності;  $D$  – ідентифікатор порушеної доступності.

Вважаючи, що будь-яке джерело загрози спрямоване на будь-який ресурс організації з метою порушення будь-якого аспекту ІБ, задається бінарне відношення  $\rho_1 = (I_j^k, O_i^m)$  реальних пар «джерело загрози – об'єкт загрози», де  $\rho_1 \in I \times O = \{(I_j^k, O_i^m) \mid I_j^k \in I, O_i^m \in O\}$ .

Будь-яке джерело загрози, що спрямоване на конкретний об'єкт і має певну мету порушення аспекту ІБ, використовує для реалізації методи і пов'язані з ними засоби, що описується бінарним відношенням  $\rho_2 = (z_e, l_q)$ ,  $z_e \in Z$ ,  $l_q \in L$ , де  $Z$  – множина методів реалізації загрози;  $L$  – множина засобів реалізації загрози.

Таким чином, можна записати, що якщо на множині  $I \times O$  задано бінарне відношення  $\rho_1 = (I_j^k, O_i^m)$  і на множині  $Z \times L$  задане бінарне відношення  $\rho_2 = (z_e, l_q)$ , то можливе відображення  $f$ , задаюча відповідність  $(I_j^k, O_i^m) \xrightarrow{f} (z_e, l_q)$ , що має наступні особливості: значення функції, які залежать від змінних  $I_j^k$  і  $O_i^m$ ; умови бієкції не виконуються, оскільки не виконуються умови ін'єкції (область визначення задається парами  $(I_j^k, O_i^m)$  на множині  $I \times O$ , а значення функції із множини  $Z \times L$  для різних елементів можуть співпадати). Відображення  $f$  є сюр'єктивним, а задавання множини пар  $(z_e, l_q)$  виконується експертними процедурами.

Таким чином, формалізований опис загроз ІБ організації матиме наступний вигляд:

$$U = (I_j^k, O_i^m, z_e, L_n), \quad (5)$$

де  $I_j^k$  – ідентифікатор джерела загрози, що характеризується типом розташуванням;  $O_i^m$  – ідентифікатор об'єкта загрози, що характеризується типом ресурсу організації і ціллю порушення аспекту ІБ;  $z_e$  – ідентифікатор  $e$ -го методу реалізації загрози;  $L_n$  – ідентифікатор  $n$ -ї підмножини засобів реалізації загрози.

В подальшому визначається наступний етап, а саме, ресурси організації, як об'єкти загроз. Розгляд поточного і наступних етапів формалізованого опису процесу забезпечення інформаційної безпеки організації в експертних системах підтримки прийняття рішень (СППР) не розглядається, так як виходить за межі даної теми доповіді.

### Список літератури

1. Королева, Н.А. Экспертная система поддержки принятия решений по обеспечению информационной безопасности организации: моногр. / Н.А. Королева, В.М.Тютюнник. – Тамбов; М.; СПб.; Баку; Вена: Нобелистика, 2006. – 290 с.

2. Васильев В.И. Система поддержки принятия решений по обеспечению безопасности персональных данных /В. И. Васильев, Н. В. Белков. – Уфа. - Вестник УГАТУ: Методы и системы защиты и информации. – 2011. - Т. 15, № 5 (45). С. 54–65