УДК 005.5-049.5:004.056

Н. А. Королева, В. М. Тютюнник

Формализация процесса обеспечения информационной безопасности организации

Предложен алгоритм решения задачи обеспечения информационной безопасности организации, который заключается в формировании множества угроз, направленных на ресурсы организации, генерации вариантов мероприятий по защите от этих угроз и формулировке задач оптимизации выбора мероприятий по информационной безопасности. Алгоритм использован в экспертной автоматизированной информационной системе поддержки принятия решений.

Задача формализации процесса обеспечения информационной безопасности (ОИБ) организации сводится к последовательной формализации угроз информационной безопасности, ресурсов организации, оценки уровня ОИБ, генерации вариантов мероприятий по ОИБ и выбору его оптимального варианта.

Угрозы информационной безопасности (ИБ) в организации разделим по трем признакам: источник угрозы, объект угрозы, методы и средства реализации угрозы. Каждый из выделенных признаков содержит свои характеристики, отражающие его особенности и влияющие на характер угрозы. Источник угрозы имеет две важные характеристики — тип и расположение; объект угрозы характеризуется типом и целью угрозы; методы и средства реализации угрозы обусловлены особенностями источника и объекта угрозы (рис. 1).

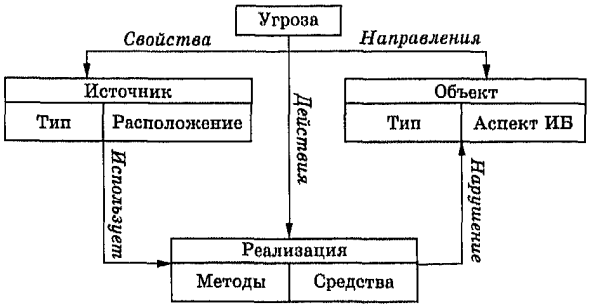

Рис. 1. *Признаки угроз информационной безопасности*

Пусть I — множество источников угрозы, характеризующихся типом и расположением относительно системы, на которую они направлены; тогда $I = \{I_A, I_T, I_C\}$, где: I_A - множество антропогенных источников угрозы; I_T множество техногенных источников угрозы; I_C множество стихийных источников угрозы.

Обозначим I^{in} -- множество внутренних источников угрозы, I^{out} — множество внешних источников угрозы. Тогда множество источников угрозы представим в виде матрицы:

$$I = \begin{pmatrix} I_A^{in} & I_A^{out} \\ I_T^{in} & I_T^{out} \\ I_C^{in} & I_C^{out} \end{pmatrix}, \text{ размерностью } 3 \times 2.$$

Или $I = \{I_j^k\}$, где j индекс типа источника угрозы, $j = \{A, T, C\}$; k — индекс расположения источника угрозы, $k = \{in, out\}$.

Пусть O множество объектов, на которые направлена угроза. В качестве объекта угрозы выступают все ресурсы организации: человеческие, информационные, физические. Тогда $O = \{O_1, O_2, O_3, \ldots, O_i, \ldots O_n\}$, где O_i — объект угрозы; n — общее количество объектов угрозы.

В соответствии с целью нарушения аспекта ИБ, обозначим: O_i^K объект с нарушенной конфиденциальностью, O_i^Q -- объект с нарушенной целостностью, O_i^D — объект с нарушенной доступностью; i -- индекс объекта угрозы; K - нарушенная конфиденциальность; Q нарушенная целостность; D -- нарушенная доступность.

Тогда множество объектов угроз представляется в виде матрицы:

$$O = \begin{pmatrix} O_1^K & O_1^Q & O_1^D \\ O_2^K & O_2^Q & O_2^D \\ O_3^K & O_3^Q & O_3^D \\ \ldots & \ldots & \ldots \\ O_n^K & O_n^Q & O_n^D \end{pmatrix}, \text{ размерностью } n \times 3,$$

где n - количество объектов угрозы; $n = \overline{1, i}$.

Или $O = \{O_i^n\}$.

Предположим, что любой источник угрозы может быть направлен на любой ресурс организации с целью нарушения любого аспекта ИБ. Это предположение описывается декартовым произведением

$$IxO = \{(I_j^k, O_i^m) \mid I_j^k \in I,\ O_i^m \in O\},$$

которое включает бесконечное множество упорядоченных пар. Поэтому зададим бинарное отношение $\rho_1 = (I_j^k, O_i^m)$ реальных пар "источник угрозы - объект угрозы". Общее количество пар (I_j^k, O_i^m),

принадлежащих декартову произведению IxO, равно $18n$, где n — общее количество объектов угроз ИБ.

Любой источник угрозы, направленный на конкретный объект и имеющий определенную цель нарушения аспекта ИБ, использует для реализации методы и связанные с ними средства. Зададим множество методов реализации угроз $Z = \{z_1, z_2, z_3, \ldots, z_e, \ldots, z_n\}$ и множество средств реализации угроз $L = \{l_1, l_2, l_3, \ldots, l_q, \ldots, l_s\}$. Пусть с любым z_e связано подмножество $L_q \subset L$, т. е.: $\forall z_e \exists L_q \subset L : z_e \xrightarrow{\tau} L_q$, где τ — отображение, задающее множество соответствий z_e и L_q. Зададим на множестве $ZxL = \{(z_e, l_q) \mid z_e \in Z,\ l_q \in L\}$ бинарное отношение $\rho_2 = (z_e, l_q)$ реальных пар "метод реализации — средства реализации".

Таким образом, можно записать, что, если на множестве IxO задано бинарное отношение $\rho_1 = (I_j^k, O_i^m)$, и на множестве ZxL задано бинарное отношение $\rho_2 = (z_e, l_q)$, то возможно отображение f, задающее соответствие $(I_j^k, O_i^m) \xrightarrow{f} (z_r, L_n)$ и имеющее следующие особенности: значения функции зависят от переменных I_j^k и O_i^m; условия биекции не выполняются, так как не выполняются условия инъекции (область определения задается парами (I_j^k, O_i^m) на множестве IxO, а значения функции из множества ZxL для различных элементов могут совпадать). Отображение f является сюръективным, а задание множества пар (z_e, l_q) выполняется экспертными процедурами.

Таким образом, формализованное описание угроз ИБ организации примет вид:

$$U = (I_j^k, O_i^m, z_r, L_n),$$

где I_j^k — идентификатор источника угрозы, характеризующийся типом и расположением; O_i^m — идентификатор объекта угрозы, характеризующийся типом ресурса организации и целью нарушения ИБ; z_r — идентификатор r-го метода реализации угрозы; L_n — идентификатор n-го подмножества средств реализации угрозы.

Обозначим множество ресурсов организации $R = \{R_H, R_F, R_S\}$, где R_H — человеческие ресурсы, R_F — физические ресурсы, R_S — информационные ресурсы. В свою очередь, каждый из типов ресурса является множеством, содержащим элементы: $R_j = \{r_{ji}\}$, где j — идентификатор типа ресурса, i — номер j-го типа ресурса. Предполагается, что множество угроз ИБ направлены на все ресурсы организации, т. е. $\exists \tau_1 \in R \times U = \{(r_{ji}; u_i)\}$.

Так как, $U = (I_j^k, O_i^m, z_r, L_n)$, то бинарное отношение τ_1 определяется однозначно по объекту угрозы, т. е. $r_{ji} = O_i^m$.

Для множества угроз ИБ организации существует множество мероприятий по их нейтрализации, которые обозначим $V = \{v_i\}$. Это утверждение описывается декартовым произведением $UxV = \{(v_i; u_i)\}$. Зададим бинарное отношение $\tau_2 \in UxV = \{(u_i; v_i)\}$ реальных пар "угроза — методы нейтрализации". Кроме этого, ОИБ организации предполагает защиту всех ресурсов, т. е. с каждым ресурсом организации связано множество мероприятий по ОИБ. Это утверждение представим в виде бинарного отношения $\tau_3 \in RxW = \{(r_{ji}; w_i)\}$, где R — множество ресурсов организации; W — множество мероприятий по ОИБ, направленных на защиту ресурсов. Процесс определения мероприятий по ОИБ организации представим композицией бинарных отношений $\tau_2 \circ \tau_1$, где $\tau_2 = \{(u_i; v_i)\}$, $\tau_1 = \{(r_{ji}; u_i)\}$; $\tau_3 = \{(r_{ji}; v_i)\}$.

Если $\tau_2 \circ \tau_1 \leq \tau_3$, $(u_i; v_i) \circ (r_{ji}; u_i) \leq (r_{ji}; w_i)$, то можно утверждать, что уровень ОИБ достаточен для защиты ресурса, полагая, что множество мероприятий по ОИБ, направленных на ресурсы, больше множества мероприятий по нейтрализации угроз либо совпадает с ним, т. е. $v_i \leq w_i$.

Если $\tau_2 \circ \tau_1 > \tau_3$, $(u_i; v_i) \circ (r_{ji}; u_i) > (r_{ji}; w_i)$, т. е. $v_i > w_i$, то можно утверждать, что уровень ОИБ недостаточен для защиты ресурса, и существуют уязвимости, через которые может быть реализована угроза. Тогда необходимо доопределить множество w_i до v_i, таким образом, чтобы, по крайней мере, выполнялось тождество $v_i \equiv w_i$.

Для определения мероприятий по ОИБ зададим нечеткое соответствие множеств U и W: $\Gamma = \{U, W, F\}$, где F — функция принадлежности UxW. Нечеткое соответствие Γ зададим в виде ориентированного графа с множеством вершин $U \cup W$, каждая дуга которого обозначает функцию принадлежности $\mu_F(u_i, w_j)$. В матричном виде нечеткое соответствие $\Gamma = \{U, W, F\}$ зададим с помощью матрицы инциденций R_Γ, строки которой помечены элементами u_i, а столбцы — w_j, на пересечении строк и столбцов расположен элемент $k_h = \mu_F(u_i, w_j)$, где μ_F — функция принадлежности элементов нечеткому графику [1].

Пусть

$$\Gamma = \{U, W, F\}, \quad h = \overline{1,6};$$

$$F = \{\langle k_1/((u_1, w_1))\rangle, \langle k_2/((u_1, w_4))\rangle, \langle k_3/((u_2, w_1))\rangle, \langle k_4((u_3, w_2))\rangle, \langle k_5/((u_4, w_1))\rangle, \langle k_6/((u_4, w_3))\rangle\}.$$

Матрица инциденций R_Γ и граф нечеткого соответствия позволяют выбрать мероприятия по ОИБ путем селекции максимальных значений k_h (рис. 2).

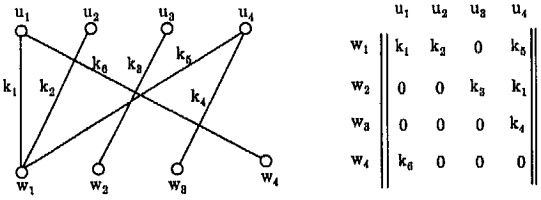

Рис. 2. Графическое и матричное задание нечеткого соответствия $\Gamma = \{U, W, F\}$

Для генерации вариантов мероприятий по ОИБ задачу оптимизации (в зависимости от требований пользователя) сформулируем в двух вариантах.

Первый вариант. Известны стоимости ресурсов организации, угроз, методов и средств защиты ресурсов от угроз: $c(r_{ji})$, $c(u_i)$, $c(w_i)$. Следует определить при заданных значениях рисков с учетом проведенной селекции минимальные затраты на ОИБ. При этом введем ограничения: стоимость ресурса больше или равна стоимости угрозы, направленной на него, в противном случае, средства, затраченные на реализацию угрозы, экономически не оправданы. По той же причине стоимость ресурса меньше или равна стоимости мероприятий по его защите. Тогда имеем:

$$\left.\begin{aligned} C_{ОИБ} &= \sum_{i=1}^{n} c(w_i) \to min \\ C_{риск} &= \sum_{i=1}^{m} f(r_{ji}, u_i) \leq C_{зад} \\ c(u_i) &\leq c(r_{ji}) \leq c(w_i) \\ c(u_i);\ c(r_{ji});\ c(w_i);\ j &= \overline{1,m} \end{aligned}\right\}.$$