УДК 004.02

А.С. Север, маг.;
Н.Н. Пустовалова, доц., канд. техн. наук (БГТУ, г. Минск)

ЭТАПЫ РЕШЕНИЯ ЗАДАЧИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ ПРЕДПРИЯТИЯ

Информационная система (ИС) предприятия − это совокупность технологических, аппаратных и программных средств, предназначенных для автоматизации процессов в повседневной работе предприятия. Отказ какого-либо из данных ресурсов приводит к невозможности выполнения предприятием одной или нескольких своих функций.

Проблема состоит в получении количественной (а именно, стоимостной) оценки информационных рисков системы − то есть рисков, связанных с нарушением конфиденциальности, доступности или целостности какого-либо ресурса.

Задачу управления информационными рисками можно разбить на четыре этапа.

Этап 1 − оценка текущего уровня риска ИС.

Этап 2 − построение рейтинга угроз с учетом силы их влияния на уровень риска ИС.

Этап 3 − формирование перечня наиболее эффективных контрмер для снижения текущего уровня риска ИС с учетом информации, полученной на предыдущем этапе.

Этап 4 − оценка достигнутого уровня риска ИС с учетом выбранных контрмер и оценка эффективности управления информационными рисками.

Рассмотрим оценку текущего уровня риска ИС, т. е. первый этап.

В качестве объекта управления возьмем информационную систему добровольного медицинского страхования страховой компании.

Под ***риском системы*** будем рассматривать сумму рисков ресурсов, из которых состоит система:

$$R = \sum_{i=1}^{n} R_i,$$

где R_i, − риск i-го ресурса; n − количество ресурсов.

С каждым ресурсом связано множество опасных состояний, реализация которых приводит к отказу, нарушению конфиденциальности, доступности или целостности данного ресурса.

Под ***риском i-го ресурса*** будем понимать сумму рисков, связанных с реализацией опасных состояний данного ресурса:

$$R_i = \sum_{j=1}^{M_i} \mathrm{r_{ij}},$$

где r_{ij} – риск реализации j-го опасного состояния i-го ресурса; j меняется от 1 до M_i; M_i – количество опасных состояний i-го ресурса.

Под ***риском реализации j-го опасного состояния i-го ресурса*** будем понимать произведение вероятности P_{ij} и стоимости потерь C_{ij} от реализации данного опасного состояния ресурса:

$$r_{ij} = P_{ij} C_{ij}.$$

Таким образом, задачу оценки риска ИС можно разбить на следующие этапы:

– описание структуры ресурсов ИС;

– описание множества опасных состояний ресурсов ИС;

– оценка вероятностей P_{ij} реализации опасных состояний, в том числе выявление меры влияния угроз на реализацию опасных состояний;

– оценка стоимости потерь C_{ij} от реализации опасных состояний.

Существует общепринятая классификация рисков по *частоте* возникновения ущерба и по *размеру* ущерба (потерь), выражаемому денежными единицами ущерба.

Если имеется полная информация об угрозах, уязвимостях и стоимости ресурсов, то определение размера ущерба не вызывает никаких проблем. Если же такой информации недостаточно, то соответствующие классы рисков можно установить на основе экспертного заключения.

Классификация представлена в таблице.

Таблица – Группировка рисков по частоте возникновения и размеру ущерба

По размеру	По частоте		
	редкие	средней частоты	частые
Малые риски	–	–	+
Средние риски	+	+	+
Высокие риски	+	+	–
Катастрофические риски	–	–	–

Такая классификация позволяет понять специфику различных рисков. Очевидно, что для рисков, выделенных в соответствии с данной классификацией, методы анализа и управления будут совершенно различными.

Для выявления опасных состояний, потери от которых наиболее существенны, предлагается использовать подход на основе нечеткой логики, а именно алгоритм Мамдани.

На величину потерь от реализации того или иного опасного состояния или на значимость опасного состояния влияют два фактора − собственно ущерб от реализации опасного состояния и вероятность реализации опасного состояния в течение рассматриваемого временного интервала. В качестве входных нечетких переменных в данном случае выступят «Ущерб от реализации опасного состояния, например, в течение года» и «Вероятность реализации опасного состояния в течение года». В качестве выходной переменной − «Значимость опасного состояния».

Если опасное состояние ИС связано с нарушением конфиденциальности информации, то вместо входной нечеткой переменной «Ущерб от реализации опасного состояния (в течение года)» используется нечеткая переменная «Ущерб от однократной реализации опасного состояния» и своя система правил вывода.

Под нечеткой переменной в общем случае понимается тройка <α, X, A>, где α − имя переменной, X − область определения α, A − нечеткое множество на X, описывающее ограничения на значения нечеткой переменной α с помощью набора функций принадлежности $\mu_A(x)$.

В качестве функции принадлежности. можно выбрать одну из функций: треугольная; трапециевидная; гауссова; сигмоидальная; двойная сигмоидальная.

Рассмотрим работу алгоритма нечеткого вывода Мамдани на следующем примере.

Пусть мы располагаем двумя правилами:

П1: если* есть $A1$ *и* y есть $B1$, то z есть $C1$,
П2: если x есть $A2$ и y есть $B2$, то z есть $C2$,

где x и y − имена входных переменных, z − имя переменной вывода; $A1$, $A2$, $B1$, $B2$ − значения входных переменных, $C1$, $C2$ − некоторые значения переменной z, определяемые заданными функциями принадлежности; при этом четкое значение переменной z_0 необходимо определить на основе указанных правил и некоторых исходных значений X_0 и y_0.

Алгоритм состоит из четырех этапов:

1. Введение нечеткости: находятся степени истинности для предпосылок каждого правила: $A1(X_0)$, $A2(X_0)$, $B1(y_0)$, $B2(y_0)$.

Например, $A1(X_0)$ − это значение функции принадлежности $A1$ переменной x в точке X_0.

2. Нечеткий вывод: находятся уровни «отсечения» для предпосылок каждого из правил [1]. При этом для логической операции «и» используется операция *min*, для логической операции «или» используется операция *max*. Поскольку в приведенных выше правилах используется операция «и», то:

$$\alpha 1 = min(A1(X_0), B1(y_0));$$
$$\alpha 2 = min(A2(X_0), B2(y_0)).$$

Затем находятся усеченные функции принадлежности для выходной переменной z:

$$C'1(z)=\alpha 1 \wedge C1(z);$$
$$C'2(z)=\alpha 2 \wedge C2(z);$$

где $C1(z)$, $C2(z)$ − функции принадлежности $C1$, $C2$ переменной z.

3. Композиция: с использованием операции max производится объединение найденных усеченных функций, что приводит к получению итоговой функции принадлежности для выходной переменной.

$$\mu_{\Sigma}(z) = C(z) = C_1' \vee C_2' = (\alpha 1 \wedge C1(z)) \vee (\alpha 2 \wedge C2(z)).$$

4. Дефаззификация: находится четкое значение выходной переменной z_0, например, центроидным методом (как координата центра тяжести для кривой $\mu\sum(z)$):

$$z_0 = \sum_{i=1}^{n} \alpha_i z_i \Big/ \sum_{i=1}^{n} \alpha_i,$$

где n − количество интервалов, на которые разбивается область значений выходной переменной z; z_i, − значения переменной z в i-ой точке с номером i; α_i − значение итоговой функции принадлежности $\mu_{\sum}(z)$ в точке z_i.

Таким образом, выходными данными алгоритма являются результирующие функции принадлежности для каждой выходной переменной и четкие значения, полученные путем дефаззификации этих функций.

ЛИТЕРАТУРА

1. Пегат А. Нечеткое моделирование и управление. − М.: Бином. Лаборатория знаний, 2009. – 798 с.