УДК 002.6:004.056

Н. А. Королева, В. М. Тютюнник

Методика оценки уровня обеспечения информационной безопасности организации

Предложена методика оценки важности ресурсов организации с точки зрения информационной безопасности (ИБ), опасности угроз, оценки рисков, основанная на концепции нечетких множеств (НМ). Методика опробована в экспертной автоматизированной информационной системе поддержки принятия решений по обеспечению информационной безопасности (ОИБ) организации.

Задачи оценки важности ресурсов и опасности угроз им из-за их многокритериальности и неопределенности удобно решать с использованием концепции нечетких множеств (НМ) [1–4].

Для оценки ресурсов и угроз воспользуемся правилом Заде задания лингвистических переменных (ЛП):

$$\Omega = \{\omega, T(\omega), A, G, Q\},$$

где ω — название переменной; T — терм-множество значений; т. е. совокупность ее лингвистических значений; A — носитель; G — синтаксическое правило, порождающее термы множества T; Q — семантическое правило, которое каждому лингвистическому значению ω ставит в соответствие его смысл $Q(\omega)$, причем $Q(\omega)$ обозначает нечеткое подмножество носителя U.

Для оценки угрозы зададим ЛП Ω_U = "Опасность угрозы", которая принимает нечеткие значения $T = \{T_1, T_2, T_3, T_4, T_5\}$, где T_1 = "Незначимая", T_2 = "Значимая", T_3 = "Опасная", T_4 = "Очень опасная", T_5 = "Критическая".

Для определения носителя множества Ω_U, содержащего терм-значения T, в рамках решаемой задачи проведем балльный метод экспертной оценки. В качестве факторов, обусловливающих опасность угрозы, будем использовать параметры, из которых первые пять – $Б_1$, $Б_2$, $Б_3$, $Б_4$, $Б_5$ характеризуют источник и цель угрозы, остальные — $Б_6$, $Б_7$, $Б_8$, $Б_9$, $Б_{10}$, $Б_{11}$, $Б_{12}$, $Б_{13}$ – степень опасности угрозы: $Б_1$ — источник угрозы; $Б_2$ — расположение источника угрозы; $Б_3$ – преднамеренность воздействия; $Б_4$ — цель угрозы нарушения аспекта ИБ; $Б_5$ — объект угрозы; $Б_6$ – уровень нарушителя; $Б_7$ — возможность предотвращения/нейтрализации угрозы; $Б_8$ – возможность обнаружения реализации угрозы; $Б_9$ – возможность восстановления объекта после реализации угрозы; $Б_{10}$ — частота появления угрозы за год; $Б_{11}$ — опасность реализации угрозы для объекта с точки зрения ущерба; $Б_{12}$ — затраты на реализацию угрозы; $Б_{13}$ — простота реализации угрозы. Количественная оценка каждого параметра определяется в баллах — от 1 до 4. Для вычисления носителя множества Ω_U данные сводятся по показателям $Б_6 - Б_{13}$ в таблицу и рассчитываются интервалы для каждого терм-значения.

Для каждого НМ введем значения функции принадлежности $\mu_{T_j}(x_i)$, обозначаемые терм-величинами T_1, T_2, T_3, T_4, T_5. Для оценки опасности каждой угрозы, заполним табл. 1.

Таблица 1

Матрица показателей степени опасности угрозы

№	Угрозы ИБ	Показатели													
		$Б_1$	$Б_2$	$Б_3$	$Б_4$	$Б_5$	$Б_6$	$Б_7$	$Б_8$	$Б_9$	$Б_{10}$	$Б_{11}$	$Б_{12}$	$Б_{13}$	K_1
1	u_1														$K_1(u_1)$
2	u_2														$K_1(u_2)$
3	u_3														$K_1(u_3)$
...	...														...
n	u_n														$K_1(u_n)$

Примечание: $K_1 = \sum_{i=6}^{13} Б_i$.

Функции принадлежности i-й угрозы одному из терм-значений T_1, T_2, T_3, T_4, T_5 сводим в табл. 2, на основании данных которой выбираем максимальное значение по каждой строке, характеризующее опасность угрозы.

Таблица 2

Матрица оценки угроз

№	$K_1(u_i)$	Функции принадлежности				
		μ_{T_1}	μ_{T_2}	μ_{T_3}	μ_{T_4}	μ_{T_5}
1	$K_1(u_1)$					
2	$K_1(u_2)$					
3	$K_1(u_3)$					
...	...					
n	$K_1(u_n)$					

При обследовании организации, угрозы информационной безопасности важно рассматривать с точки зрения существующих в организации механизмов обеспечения информационной безопасности. Так, например, показатель угрозы "Вирусы" при отсутствии в организации антивирусного обеспечения, оперативного обновления антивирусных баз, запрета на установку постороннего программного обеспечения, при наличии неограниченных и неконтролируемых возможностей работы в сети Интернет и т. д., изменяется и переходит из категории "Опасная" в "Очень опасную" или "Критическую". Поэтому, помимо вычисления общих показателей степени опасности угроз ИБ, важно оценить потенциальные угрозы для организации. Кроме этого, показатели $Б_1 - Б_2$ характеризуют источник угрозы и объект угрозы и позволяют в дальнейшем осуществить связь "ресурс-угроза".

Для оценки важности ресурсов организации с точки зрения информационной безопасности поступают аналогично: задается ЛП — Ω_R = "Важность ресурса с точки зрения ИБ организации", которая принимает нечеткие значения $D = \{D_1, D_2, D_3, D_4\}$, где D_1 = "Незначимый"; D_2 = "Значимый"; D_3 = "Важный"; D_4 = "Очень важный".

Для определения носителя множества Ω_R, содержащего терм-значения D, воспользуемся балльным методом экспертной оценки. В качестве факторов, влияющих на оценку ресурса, используются следующие: A_1 — стоимость ресурса; A_2 — важность ресурса в процессе функционирования всей ИС организации; A_3 — стоимость восстановления ресурса в случае его частичного разрушения в результате реализации угрозы или комбинации угроз; A_4 — время восстановления ресурса в случае его частичного разрушения в результате реализации угрозы или комбинации угроз; A_5 — стоимость восстановления ресурса в случае его полного разрушения в результате реализации угрозы или комбинации угроз; A_6 — время восстановления ресурса в случае его полного разрушения в результате реализации угрозы или комбинации угроз; A_7 — возможность восстановления ресурса в случае его утраты, частичного или полного разрушения; A_8 — критичность ресурса по аспектам ИБ: $A_{8к}$ — нарушение конфиденциальности; $A_{8ц}$ — нарушение целостности; $A_{8д}$ — нарушение доступности. По каждому ресурсу выставляются баллы экспертом или группой экспертов, и заполняется табл. 3, по которой определяется значение носителя множества Ω_R.

Таблица 3

Матрица показателей степени важности ресурсов организации

№	Ресурс	Показатели										
		A_1	A_2	A_3	A_4	A_5	A_6	A_7	$A_{8К}$	$A_{8Ц}$	$A_{8Д}$	K_2
1	r_1											$K_2(r_1)$
2	r_2											$K_2(r_2)$
3	r_3											$K_2(r_3)$
...	...											...
n	r_n											$K_2(r_n)$

Примечание: $K_2 = \sum_{i=1}^{8} A_i$.

Функции принадлежности i-го ресурса одному из терм-значений D_1, D_2, D_3, D_4 сведем в табл. 4.

Таблица 4

Матрица оценки ресурсов организации

№	$K_2(r_i)$	Функции принадлежности			
		μ_{D_1}	μ_{D_2}	μ_{D_3}	μ_{D_4}
1	$K_2(r_1)$				
2	$K_2(r_2)$				
3	$K_2(r_3)$				
...	...				
n	$K_2(r_n)$				

Комплексная оценка показывает критичность i-го ресурса во всей системе обеспечения информационной безопасности (ОИБ) организации, а также общий уровень защищенности ресурса. Такая методика оценки ресурса в системе ОИБ позволяет добавлять и оценивать любой ресурс. Кроме того, каждая графа в таблице характеризует некоторый параметр, существенный с точки зрения ОИБ организации. Так, например, графа $A_{8к}$ характеризует критичность ресурса по такому аспекту ИБ, как нарушение конфиденциальности. Если уровень критичности i-го ресурса по конфиденциальности высокий, то необходимо предусмотреть мероприятия по защите ресурса от раскрытия, ознакомления.

Таким образом, помимо комплексной оценки ресурса, отражающей критичность ресурса во всей системе ОИБ и уязвимость ресурса, данные в ячейках таблицы являются параметрами, на основании которых строятся правила сопоставления каждому ресурсу множества связанных с ним угроз и вариантов мероприятий по ОИБ.

Если угрозу невозможно предотвратить, то риск можно свести к минимуму, создав адекватные меры защиты. Методика оценки рисков основана на полученных оценках ресурсов и связан-

ных с ними угроз. Риск характеризует ущерб, который может наступить в результате реализации угрозы или нескольких угроз, и зависит от: показателей ценности ресурсов, вероятности реализации угроз, степени легкости, с которой уязвимости могут быть использованы при возникновении угроз, методов и средств обеспечения ИБ [5]. Процесс управления рисками направлен на достижение величины риска в допустимых пределах [6, 7].

Количественная оценка риска для каждого ресурса вычисляется по формуле:

$$C_i(риск) = [c(r_{ji}) \times q(r_{ji})] \times [c(u_i) \times p(u_i)],$$

где $C_i(риск)$ — количественная оценка риска; $c(r_{ji})$ — количественная оценка ресурса, характеризующая его важность для организации; $q(r_{ji})$ — вероятность защищенности ресурса; $c(u_i)$ — количественная оценка угрозы, направленной на ресурс и характеризующая ее опасность; $p(u_i)$ — вероятность реализации угрозы.

Величина риска в показателях и шкалах данной методики принадлежит интервалу $(0;b)$. Максимальное значение величины риска определяется как $C_i^{\max}(риск) \to b$, минимальное как $C_i^{\min}(риск) \to 0$.

Будем полагать приемлемой величину риска, равную 1% от максимальной величины ущерба, т. е. $C_i^{зад}(риск) \le \frac{b}{100}$. Если при оценке рисков величины оказались больше заданной, то необходимо предусмотреть стратегию управления рисками, которая базируется на подходах: 1) уменьшение или уклонение от риска; 2) переадресация риска; 3) принятие риска.

Уменьшение риска достигается использованием простых и дешевых контрмер. Например, грамотное управление паролями снижает риск несанкционированного доступа (НСД). Уклонение от риска основано на том, что от некоторых классов рисков возможно уклониться. Например, вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска НСД в локальную сеть со стороны Web-клиентов. Переадресация риска достигается за счет принятия мер страховки. Например, оборудование может быть застраховано от пожара или заключены договора с поставщиками средств вычислительной техники о сопровождении и компенсации ущерба, вызванного нештатными ситуациями [8–10].

Не всеми рисками можно управлять с помощью методики снижения значений рисков. Для каждой угрозы существует некое количественное значение стоимости контрмеры, после которой риск принимается. Процесс принятия рисков должен базироваться на реалистичных прогнозах относительно угроз. Оценка остаточных рисков подразумевает, что после проведения первичной оценки рисков и расчета стоимости контрмер, производится переоценка рисков с учетом наложенных контрмер, т. е. расчет остаточных рисков. После получения значений снижения рисков эти величины принимаются по соглашению с руководством организации.

Если стоимость реализации контрмер (включая передачу риска страховой компании) превышает стоимость самого ресурса или стоимость его восстановления, то риск принимается. Сценарий развития событий может включать вариант, при котором ресурс не подлежит восстановлению и потому требуется его полная замена. Простое принятие риска подразумевает принятие риска и в том случае, когда количественная оценка риска невозможна или она очевидна.

При оценке уязвимости ресурсов на основании исследования косвенных факторов, для каждой группы ресурсов и каждого типа угроз генерируется список вопросов, допускающих однозначный ответ. Уровень уязвимости оценивается, в зависимости от ответов, как: высокий, средний, низкий.

Оценка уязвимости в ОИБ ресурсов основана на соответствии механизмов защиты требованиям ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий" [11–13]. Проводится тестирование соответствия функциональных классов безопасности существующим в организации, в котором по каждому классу, в соответствие с требованиями [11–13], предлагается ответить на ряд вопросов. Вопросы предполагают однозначные ответы: да/нет. За ответ "да" назначается 0 баллов, за ответ "нет" — 1 балл. Таким образом, чем больше ответов "нет", тем ниже уровень ОИБ по данному классу. Вероятность защищенности по каждому функциональному классу рассчитывается по формуле:

$$p_i = \frac{n_i - s_i}{n_i},$$

где n_i – количество вопросов по i-му классу, s_i – количество набранных баллов, i — функциональный класс безопасности.

После вычисления вероятностей по каждому классу строится модель наиболее вероятных угроз. Так как события защищенности по каждому классу совместны и независимы, то общая вероятность защищенности по всем классам находится по формуле:

$$p = \prod_{i=1}^{k} p_i.$$

Данная формула отражает общую характеристику уровня организации информационной безопасности информационной системы организации в целом. Рассчитав стоимость мероприятий по уменьшению риска по каждому классу, генерируются рекомендации.

СПИСОК ЛИТЕРАТУРЫ

1. Кофман А. Введение в теорию нечетких множеств в управление предприятиями.- Минск : Выш. школа, 1992

2. Рыжов А. П. Элементы теории нечетких множеств и измерения нечеткости М.. Диалог МГУ, 1998.

3. Блюмин С. Л Введение в математические методы принятия решений. Липецк.: Липецкий гос пед. Институт, 1999. 100 с.

4 Розен В. В Цель оптимальность решение (математические модели принятия оптимальных решений).– М.: Радио и связь, 1982, 168 с.

5 Петренко С. А. Методика реорганизации корпоративной системы информационной безопасности // Информационное общество 2002. № 1. С 29–33.

6 Методика разработки системы оценки угроз и управления рисками Угрозы. Риски. Уязвимость.