$$M^* = \min\{M \in [0,1] : \mu_C(M) = 1\}.$$

Таким образом, в случае, когда $\mu_{B_k}(y_l) \geq M^*$ $(k,l = 1,2,...,n)$, можно считать установленным предпочтение исхода y_k над исходом y_l.

СПИСОК ЛИТЕРАТУРЫ

1. Черноруцкий И. Г. Методы принятия решений. СПб.: «БХВ-Петербург», 2005.
2. Корченко А. Г. Построение системы защиты информации на нечетких множествах. Киев: МК-Пресс, 2006.

Александр Сергеевич ЛЫСОВ —
старший преподаватель
кафедры информационной безопасности

УДК 004.056.53

ТЕХНОЛОГИЯ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ НА ОСНОВЕ МЕТОДА АНАЛИЗА ИЕРАРХИЙ

АННОТАЦИЯ. В статье обозначена актуальность задач анализа информационных рисков в организациях. Описана созданная автором данной статьи технология анализа информационных рисков, использующая метод анализа иерархий, который позволяет повысить точность оценок параметров угроз, даваемых экспертами.

This work shows the topical of tasks of informational risks in organizations analysis. The technology of informational risks analysis developed by the article author was described. This technology is based on method of hierarchy analysis which allows increasing the precision of threats parameters evaluation.

В современном мире эффективное и комплексное решение задач защиты информации в организации является ключевым фактором развития бизнеса. В соответствии с общепринятой международной практикой защиты информации [1] ключевое значение в процессе обеспечения информационной безопасности (ИБ) отводится процедуре анализа информационных рисков.

Отечественная нормативно-правовая база по ИБ в настоящий момент находится на этапе становления, уже приняты ряд руководящих документов [3] и стандарт в области защиты информации [2], но вопросы анализа информационных рисков остаются нерегламентированными. Поэтому организации должны самостоятельно выбирать средства анализа информационных рисков для комплексного обеспечения режима ИБ.

Для получения достоверной информации от анализа информационных рисков необходимо, чтобы специалист, выполняющий оценку рисков, предоставлял актуальные данные о состоянии ИБ в организации. При анализе информационных рисков силами собственных специалистов организации не всегда есть возможность обеспечить выполнение этого требования. Поэтому при выборе средств анализа рисков необходимо учитывать 2 ключевых требования: простота использования и возможность оценки качества вводимых данных.

Рассмотрим далее разработанную автором данной статьи технологию анализа информационных рисков, которая учитывает ключевые требования к про-

цессу анализа рисков в организациях. Технология преследует решение следующих задач:

• максимально упростить процесс оценки;

• обеспечить возможность оценки согласованности (правильности) ответов экспертов для определения необходимости повторения анализа рисков;

• возможность подстройки технологии анализа рисков под нужды конкретной организации, т.е. определения спектра учитываемых угроз.

Определим основные термины, используемые для описания технологии анализа рисков. *Экспертами* будем называть специалистов, которые выполняют оценку информационных рисков. *Ресурсы* — это любые материальные объекты, для которых мы хотим оценить риски ИБ. *Службы* — процедуры работы с данными или ресурсами, для которых мы оцениваем риски ИБ.

Проанализировав существующие средства анализа рисков [1], можно выделить 4 этапа для нашей технологии, на которые необходимо разделить процесс анализа рисков. Распишем этапы работы алгоритма технологии подробнее:

Нулевой этап (вводный). Здесь производится определение экспертов, принимающих участие в процессе оценки и задание значений коэффициентов для обобщения данных от нескольких экспертов. На данном этапе эксперт, выполняющий оценку рисков, должен заполнить данные о себе, чтобы сформировать *вес* Y_s *(степень доверия к эксперту)*. Этот параметр используется для минимизации дисперсии общего значения риска, при оценке параметров угроз несколькими экспертами в одном региональном отделе. Расчет веса s-го эксперта производится по следующей формуле:

$$Y_s = \left(\sum_{l=0}^{L} Y_s^l\right) / l, \qquad (1)$$

где Y_s^l — значение компонент веса, для всех компонентов используется шкала (от 0,1 до 1). Предполагается следующий набор компонент: Y_s^0 — учет опыта работы в области ИБ; Y_s^1 — учет повышений квалификации в области ИБ; Y_s^2 — учет связи работы эксперта с управлением инфраструктурой информационных систем; Y_s^3 — учет валидности оценок экспертов региональных отделений субъективно экспертами из центрального отдела.

Первый этап (ввод данных об инфраструктуре). Эксперт указывает существующие классы компонентов, присутствующих в инфраструктуре организации.

В соответствии с классификацией перечисляются все существующие *ресурсы* в организации и эксперт указывает оценки стоимости C, D, K. В соответствии с этими характеристиками рассчитывается стоимость ресурсов $H_р$ по следующей формуле:

$$H_р = (U_1 \times C + U_2 \times D + U_3 \times K) / (U_1 + U_2 + U_3), \qquad (2)$$

где U_1, U_2, U_3 — значения весовых коэффициентов, подстраиваемых для каждой организации (от 0,1 до 1); C — оценка стоимости ущерба для организации при разрушении ресурса; D — оценка стоимости ущерба для организации при недоступности ресурса в течение, например, месяца; K — оценка стоимости ущерба для организации при НСД к ресурсу. Все значения стоимостей эксперт оценивает в рублях.

Для оценки стоимости *служб* эксперт должен будет сравнить, насколько значение стоимости данной службы (например, электронной почты) больше или меньше, чем стоимость уже учтенных им ресурсов. Таким образом, значение стоимости для каждой службы H_c будет:

$$H_c = \begin{cases} H_p \times g, \text{ если } H_c > H_p \\ \dfrac{H_p}{g}, \quad \text{если } H_c < H_p \end{cases}, \qquad (3)$$

где g — значение коэффициента, насколько стоимость службы больше (меньше) стоимости ресурса.

Второй этап (оценка угроз экспертами).

На данном этапе необходимо рассчитать вероятности и ущерб от реализации каждой из угроз для всех ресурсов и служб. С учетом задач разработки данной технологии получение данных о вероятностях будет производиться не прямыми методами оценки вероятности, а будет использоваться *метод анализа иерархий* для определения суждений эксперта о значении вероятности одной угрозы относительно другой.

Значения вероятностей и ущерба от реализации угроз для данного ресурса могут быть представлены векторами $\vec{P}$ для вероятности и $\vec{V}$ для ущерба. При наличии *M* угроз для данного ресурса эксперту необходимо оценить отношения p_i/p_j для вероятностей угроз, по шкале значимости от 1 до 9 (1 — вероятность событий p_i и p_j одинаковы; 9 — вероятность p_i угрозы *i* «намного выше», чем вероятность p_j угрозы *j*), где *i*, *j* — меняются от *1* до *M*. После оценки всех пар отношений можно сформировать матрицу парных сравнений $A = (a_{ij}) = \left(p_i / p_j \right)$ для значений отношений вероятностей угроз.

Для матрицы парных сравнений *A* вектор значений вероятностей $\vec{P}$ можно найти, решив следующее векторное уравнение:

$$A \times \vec{P} = \lambda_{max} \times \vec{P}, \qquad (4)$$

где λ_{max} — наибольшее собственное значение матрицы, $\vec{P}$ — собственный вектор матрицы.

Для вычисления значений вектора $\vec{P}$ сначала необходимо найти λ_{max}, наибольшее собственное значение матрицы A. Для этого необходимо получить ненулевое решение уравнения: $(A - \lambda E) \times \vec{P} = 0$, где *E* — диагональная единичная матрица. А для этого $\det(A - \lambda E)$ должен быть равен нулю. Так как определитель матрицы $A - \lambda E$ равен нулю, то для нахождения λ_{max} необходимо решить характеристическое уравнение данной матрицы. Это может быть сделано с использованием численных методов.

Далее при известном значении λ_{max} вектор вероятностей $\vec{P}$ следует искать, решая векторное уравнение (4). Для обеспечения единственности решения надо учитывать, что часто необходимо иметь нормализованное решение, и поэтому следует заменить одно из уравнений $p = \frac{1}{\lambda_{max}} \sum_{j=1}^{M} (a_{ij} p_j)$ системы (4) на уравнение $\sum_{k=1}^{n} p_k = 1$.

При необходимости расчета значений вектора $\vec{P}$ и наибольшего собственного значения λ_{max} без использования численных методов возможно определение приблизительных значений. Расчет приблизительных значений собственного вектора $\vec{P}$ матрицы парных сравнений и наибольшего собственного значение λ_{max} может быть произведен методами, предложенными Т. Саати [5].

Для проверки согласованности полученных результатов необходимо использовать индекс согласованности (ИС). ИС будет выражать «близость к согласованности», т.е. степень отклонения суждений эксперта друг от друга. Индекс согласованности рассчитывается по следующей формуле:

$$\text{ИС} = \frac{(\lambda_{max} - M)}{(M-1)}, \qquad (5)$$

где M — количество угроз для данного ресурса. Малое значение индекса согласованности (меньшее или равное 0,1) свидетельствует о приемлемой степени согласованности суждений эксперта. Значение ИС больше 0,1 служит основанием для пересмотра суждений эксперта. Для более точной оценки согласованности суждений экспертов, автором метода анализа иерархий рекомендуется значение *ИС* делить на случайный индекс (СИ), определенный экспериментально и зависящий от порядка матрицы парных сравнений.

Аналогичным образом происходит вычисление значений ущерба для всех ресурсов, служб и организации в целом.

Третий этап (генерация отчетов и рекомендаций).

На данном этапе подсчитываются результаты оценки угроз и определяются необходимые меры защиты. Для вычисления величины значения риска W_i для i-го ресурса, службы или организации в целом (i=0) следует воспользоваться методом взвешенной суммы для агрегирования данных субъективных оценок разных экспертов:

$$W_i = \sum_{s=1}^{s} \left(w_m^s \times Y_s \times H_i^s \right) / S, \qquad (6)$$

где S — количество экспертов, принимавших участие в оценке; Y_s — вес эксперта, определяемый на нулевом этапе; H_i^s — значение стоимости данного ресурса, указанное s-ым экспертом; w_m^s — значение риска для данного ресурса, определенное s-ым экспертом, рассчитываемое по следующей формуле:

$$w_m^s = \sum_{j=1}^{M} v_j^s \times p_j^s, \qquad (7)$$

где M — общее количество учтенных угроз для данного ресурса, v_j^s — величина ущерба, который может быть нанесен компоненту системы при реализации угрозы j, p_j^s — вероятность реализации угрозы j за месяц.

Значение риска возможного ущерба, рассчитанное по формуле (6), будет получено в рублях. Значения ущерба и вероятности осуществления угроз для каждого компонента системы эксперт определяет для периода времени (например, один месяц), таким образом, можно, говорить о риске W_i — величине возможного денежного ущерба для организации в течение месяца.

Для определения списка угроз был выбран стандарт BSI [4], поскольку он является единственным из открытых стандартов, затрагивающим широкий спектр вопросов защиты информации и описывающим контрмеры для угроз.

После расчета значений рисков для компонентов (ресурсов и служб) системы выводится информация об общем риске для компонента и рисках отдельных угроз и градация компонент по степени уязвимости в соответствии с этим значением.

Для наглядного представления информации о рисках для компонентов организации предлагается использовать уже широко применяемый метод градаций рисков по уровням. Например, в зависимости от полученных оценок риск компонента относится к одной из следующих групп относительно вычисленного максимального риска в организации W_{max}:

1. Высокий риск (значение риска в диапазоне (75-100)% от W_{max}). Предполагается, что без снижения таких рисков использование компонента может оказать отрицательное влияние на бизнес.

2. Существенный риск (значение риска в диапазоне (50-74)% от W_{max}). Здесь требуется эффективная стратегия управления рисками для данного компонента.

3. Умеренный риск (значение риска в диапазоне (25-49)% от W_{max}). В отношении рисков, попавших в эту область, достаточно использовать основные процедуры управления рисками.

4. Незначительный риск (значение риска в диапазоне (1-24)% от W_{max}). Усилия по управлению рисками в данном случае не будут играть важной роли.

И завершающий шаг: на основании справочника стандарта BSI определяется рекомендованный список мер уменьшения рисков угроз информационной безопасности для каждого из компонентов системы и для системы в целом.

Для практического использования описанной выше технологии автором разработана информационная система, позволяющая автоматизировать процесс анализа информационных рисков.

Оценим степень применимости разработанной технологии, сравнив ее с существующими средствами анализа информационных рисков. Сравнение будем производить по следующим характеристикам:

- Простота использования (субъективная характеристика);
- Метод получения данных о параметрах угроз;
- Возможность изменения (подстройки) процедуры анализа рисков под организацию;
- Используемый стандарт по ИБ для определения списка угроз и контрмер;
- Возможность учета угроз для информационных ресурсов;
- Возможность учета угроз для служб в организации.

Информация о характеристиках существующих средств анализа рисков была получена с официальных сайтов и из источника [1].

Оформим результаты сравнения средств анализа рисков в таблицу для наглядности (табл. 1). В ячейках таблицы присутствуют следующие значения: «+» — означающее полное соответствие критерию, «−» — несоответствие критерию; и «+/−» — частичное соответствие критерию.

Таблица 1

Характеристики существующих средств анализа рисков

	RA2 art of risk	Risk Advisor	RiskWatch	CRAMM	АванГард-Анализ	Гриф	Технология анализа рисков
1	2	3	4	5	6	7	8
Простота использования	+	+	+	+/-	+/-	+	+

Продолжение табл. 1

1	2	3	4	5	6	7	8
Метод получения данных	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн. по 3-м критериям	Метод анализа иерархий
Возможность подстройки работы	-	-	-	Есть профили работы	Может выполнять эксперт	-	+
Использ. стандарт по ИБ	ISO 17799	AS/NZS 4360:2004 и ISO 17799	Стандарты США и ISO 17799	ISO 17799	ГОСТ Р ИСО/МЭК 15408	ISO 17799	BSI
Учет угроз для ресурсов	+	+	+	+	+	+	+
Учет угроз для служб	+	-	+	+	+	+	+

Таким образом, для выполнения процедуры анализа информационных рисков с учетом описанных выше требований простоты использования и возможности проверки согласованности оценок, даваемых экспертами, может быть применима только разработанная *технология анализа информационных рисков.*

СПИСОК ЛИТЕРАТУРЫ

1. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. М.: Компания АйТи; ДМК Пресс, 2004. 384 с.

2. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. М.: ИПК Издательство стандартов, 2002.

3. РД ФСТЭК России // www.fstec.ru

4. Сайт стандарта BSI // www.bsi.de/english/publications/index.htm

5. Саати Т. Принятие решений: Метод анализа иерархий / Пер. с англ. М.: Радио и связь, 1993. 278 с.

Ольга Андреевна НЕСТЕРОВА —
инженер-программист
научно-исследовательского института
информационных и коммуникационных технологий

Евгений Александрович ОЛЕННИКОВ —
зав. лабораторией информатизации
медицинских учреждений
научно-исследовательского института
информационных и коммуникационных технологий,
кандидат технических наук

УДК 004.9:61

НЕКОТОРЫЕ ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМЫ ИНТЕГРАЦИИ ДАННЫХ РЕЗУЛЬТАТОВ ОБСЛЕДОВАНИЙ НА РАЗЛИЧНОМ МЕДИЦИНСКОМ ОБОРУДОВАНИИ

АННОТАЦИЯ. В статье рассматриваются некоторые подходы к решению проблемы интеграции данных результатов медицинских обследований, проводимых на оборудовании функциональной диагностики Тюменского кардиологического центра, в рамках единой информационной системы.