А. С. Лысов
Тюменский государственный университет

ЗАДАЧА АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ В ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЯХ

В данной работе обозначена задача анализа информационных рисков в учреждениях госсектора. Для определения путей решения задачи выполнено сравнение существующих методик анализа рисков. Описана созданная автором данной статьи методика анализа информационных рисков, позволяющая повысить точность оценок параметров угроз, даваемых экспертами.

Задачи обеспечения информационной безопасности (ИБ) становятся актуальными для все более широкого круга организаций благодаря повсеместному внедрению информационных технологий (ИТ) в жизни общества. Для обеспечения режима ИБ в организациях в России приняты стандарт по ИБ [2] и ряд руководящих документов [3], где описаны обязательные требования по обеспечению режима ИБ. Выполнение этих требований позволит организации обеспечить «базовый» уровень безопасности, так как требования не рассматривают структуру организации и специфику ее деятельности. Для определения дополнительных мер защиты информации с учетом особенностей работы организации используются специализированные стандарты в каждой из областей. К сожалению, в России на данный момент принят только один специализированный стандарт по ИБ — это стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» [6].

Рассмотрим возможность определения необходимых дополнительных мер по обеспечению режима ИБ для государственных учреждений. Так как стандарт по ИБ в данной области отсутствует, необходимо проанализировать особенности работы организации и на базе этой информации произвести выбор дополнительных средств обеспечения безопасности, для этого используются методики анализа информационных рисков.

Выполним обзор методик анализа рисков для определения возможности их применения в государственных учреждениях. Методики будем отбирать по следующим принципам: опубликованные в открытой печати; имеющие программную реализацию для автоматизации процесса анализа; учитывающие особенности организации.

Для учреждений госсектора наиболее важны следующие характеристики методик: простота использования; возможность проверки точности ответов экспертов, выполняющих оценку рисков; учет информационных ресурсов и служб; возможность подстройки методики под специфику организации. Поэтому выполним сравнение характеристик работы методик по следующим критериям:

· простота использования (субъективная характеристика);

· метод получения данных о параметрах угроз;

· возможность изменения (подстройки) методики 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.

Обзор методик сделан на базе информации с официальных сайтов методик и их программных комплексов и на базе [1, 4]. В данном обзоре мы не будем рассматривать: справочные и методические материалы, например SOS — Interactive Online Security Polices and Support; программный комплекс Cobra, относящийся к базовому уровню безопасности, и разделы стандартов по ИБ, связанные с анализом рисков (например, NIST 800-30), так как они не удовлетворяют принципам отбора методик, выдвинутым выше.

В рамках данной статьи не представляется возможным детально описать работу всех изученных методик анализа рисков. Поэтому мы рассмотрим только общую информацию о методиках и выполним сравнение по обозначенным критериям.

RA2 art of risk. Система RA2 art of risk базируется на британском стандарте ISO 17799, на методических материалах Британского института стандартов (BSI) PD 3002, PD 3003, PD 3005, а также на стандарте ISO 13335, части 3 и 4. Этот инструмент позволяет выполнять оценку рисков как в соответствии с требованиями базового уровня, так и в соответствии с более детальными спецификациями PD 3002 Британского института стандартов.

Risk Advisor. Компания «MethodWare» выпускает ряд продуктов, которые могут быть полезными для аналитиков в области ИБ, для нас имеет актуальность ПО анализа и управления рисками Risk Advisor. Методология отвечает австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999). Имеется версия, соответствующая ISO 17799.

RiskWatch. Компания RiskWatch предлагает ПО, предназначенное для идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в области компьютерной и физической безопасности предприятия. В продукте учитываются требования стандартов США. Кроме того, выпущена версия продукта RiskWatch для стандарта ISO 17799.

CRAMM. Метод CRAMM разработан в центральном агентстве по компьютерам и телекоммуникациям Великобритании (ССТА) для анализа и контроля рисков. Сейчас существует несколько версий метода, ориентированных на требования министерства обороны, гражданских государственных учреждений, финансовых структур, частных организаций. В настоящее время продается версия CRAMM 5, соответствующая стандарту BS 7799 (ISO 17799).

Система «АванГард». Система создана в Институте системного анализа Российской академии наук. Комплексная экспертная система «АванГард» включает в себя два программных комплекса (ПК): «АванГард-Анализ» и «АванГард-Контроль». Для анализа рисков используется ПК «АванГард-Анализ», который позволяет построить структурную модель автоматизированной информационной системы (АИС), модель угроз и модель событий рисков, связанных с отдельными составляющими АИС; также этот ПК позволяет построить модель защиты — систему мер и требований, которые должны выполняться, чтобы обеспечить безопасность информационных систем организации. Система построена на базе стандарта ГОСТ Р ИСО/МЭК 15408: 2002 и собственной базы уязвимостей и контрмер.

Digital Security Office. Система Digital Security Office разделена на две программы «Гриф» и «Кондор». ГРИФ — комплексная система анализа и управления рисками информационной системы компании. ГРИФ строит картину защищенности информационных ресурсов в вашей системе и позволяет выбрать оптимальную стратегию защиты информации компании. Система построена на базе стандарта ISO 17799.

Оформим результаты сравнения методик анализа рисков в таблицу для наглядности. В ячейках таблицы присутствуют следующие значения: «+» означает полное соответствие критерию, «—» — несоответствие критерию, «+/—» — частичное соответствие критерию.

Таблица 1. Сравнение характеристик существующих методик анализа рисков.

	RA2 art of risk	Risk Advisor	RiskWatch	CRAMM	АванГард-Анализ	Гриф
Простота использ.	+	+	+	+/–	+/–	+
Метод получения данных	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн.	Прямая оценка вероятн. по 3 критериям
Возможность подстройки методики	–	–	–	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	ISO 17799
Учет угроз для ресурсов	+	+	+	+	+	+
Учет угроз для служб	+	–	+	+	+	+

Полученная в результате изучения методик анализа рисков таблица 1 позволяет сделать следующие выводы:

· на основе субъективной оценки простоты использования для нашей задачи могут быть применены все методики, кроме методик CRAMM и «АванГард-Анализ»;

· все рассмотренные методики для оценки значений угроз используют прямую оценку вероятностей, что не предоставляет методов для проверки точности ответов экспертов;

· для подстройки параметров методики под нужды организации можно использовать только методики CRAMM и «АванГард-Анализ»;

· характеристики учета угроз для ресурсов и служб для большинства методик равнозначны.

Таким образом, для выполнения процедуры анализа информационных рисков в государственных учреждениях с учетом описанных выше требований не может быть применима ни одна из рассмотренных методик.

Методика анализа рисков для государственных учреждений

Для выполнения процедуры анализа рисков автором данной статьи разработана методика, учитывающая ключевые требования для анализа рисков в государственных учреждениях. Методика имеет целью решение следующих задач:

· максимально упростить процесс оценки;

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

· обеспечить возможность подстройки методики под нужды конкретной организации, т. е. определения спектра учитываемых угроз.

Опишем подробнее задачу для анализа рисков в государственных учреждениях. Необходимо выполнить оценку рисков в органах государственной власти с распределенной инфраструктурой: региональные отделения, где должны производиться процедуры оценки рисков, и центральное отделение, выполняющее функции управления рисками. Специалисты, на которых возложены вопросы

защиты информации (эксперты), выполняющие оценку рисков, не всегда являются техническими специалистами, по этой причине требования простоты использования и проверки согласованности ответов экспертов очень важны.

Проанализировав существующие методы анализа рисков, можно выделить 4 этапа в нашей методике, на которые необходимо разделить процесс анализа рисков. Распишем этапы работы алгоритма методики подробнее:

Нулевой этап (вводный).

Здесь производятся определение экспертов, принимающих участие в процессе оценки, и задание значений коэффициентов для обобщения данных от нескольких экспертов. На этом этапе эксперт, выполняющий оценку рисков, должен заполнить данные о себе, чтобы сформировать *вес* Y_s *(степень доверия к эксперту)*. Это 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:

$$Y_s = (\Sigma^{L}_{l=0} Y_s^l)/l, \quad (1)$$

где Y_s^l — значение компонентов веса, для всех компонентов используется шкала (от 0,1 до 1). Предполагается следующий набор компонентов: 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 — субъективный учет валидности оценок экспертов региональных отделений 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 в организации *ресурсы*, и эксперт указывает оценки стоимости C, D, K. По этим характеристикам рассчитывается стоимость ресурсов H_ρ по следующей формуле:

$$H_\rho = (U_1 \times C + U_2 \times D + U_3 \times K)/(U_1 + U_2 + U_3), \quad (2)$$

где U_1, U_2, U_3 — значения весовых коэффициентов 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* эксперту будет предлагаться 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:

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

где g — значение коэффициента, отражающего, 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 этой методики получение данных о вероятностях и ущербе мы будем производить не прямыми методами оценки вероятности, а *методом 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 $\vec{\rho}$ для вероятности и $\vec{V}$ для ущерба. При наличии M угроз для данного ресурса эксперту необходимо оценить отношения ρ_i/ρ_j для вероятностей угроз по шкале значимости от 1 до 10 (1 —

вероятности событий ρ_i и ρ_j одинаковы; 10 — вероятность ρ_i угрозы i «намного выше», чем вероятность ρ_j угрозы j), где i, j меняются от 1 до M. После оценки всех пар отношений можно сформировать матрицу парных сравнений $A = (a_{ij}) = (\rho_i / \rho_j)$ для значений отношений вероятностей угроз.

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

$$A \times \vec{\rho} = \lambda_{max} \times \vec{\rho}, \quad (4)$$

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

Для вычисления значений вектора $\vec{\rho}$ сначала необходимо найти λ_{max} — наибольшее собственное значение матрицы А. Для этого необходимо получить ненулевое решение уравнения: $(A - \lambda E) \times \vec{\rho} = 0$, 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, 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 $\vec{\rho}$ будем искать, решая векторное уравнение (4). Для обеспечения единственности решения учтем, что часто необходимо иметь нормализованное решение, и поэтому заменим одно из уравнений $\rho_i = \frac{1}{\lambda_{max}} \sum_{j=1}^{M} (a_{ij} \rho_j)$ системы (4) на уравнение $\sum_{k=1}^{n} \rho_k$.

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 [7]. Индекс согласованности рассчитывается по следующей формуле:

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

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 0,2 служит основанием для пересмотра суждений эксперта.

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)* воспользуемся методом взвешенной суммы для агрегирования данных субъективных оценок разных экспертов:

$$W_i = \sum_{s=1}^{S} (w^s_m \times Y_s \times H^s_i) / 10^4, \quad (6)$$

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

$$w^s_m = \sum_{m=1}^{M} v^s_m \times \rho^s_m, \quad (7)$$

где M — общее количество учтенных угроз для данного ресурса, v^k_m — величина ущерба, который может быть нанесен *i-му* компоненту системы, при реализации угрозы m, ρ^k_m — вероятность реализации угрозы m за месяц.

В формуле (6) мы делим значение риска на 10^4 для получения значения возможного ущерба в рублях. Значения ущерба и вероятности осуществления угроз для каждого компонента системы эксперт определяет для периода времени (например, один месяц), таким образом, мы можем говорить о риске W_i — величине возможного денежного ущерба для организации в течение месяца.

Для определения списка угроз был выбран стандарт BSI [5], 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 компонентов 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 попадает в одну 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.

В государственных учреждениях использование методик анализа рисков является еще, к сожалению, исключением из правил, но автор надеется, что в дальнейшем ситуация будет меняться в обратную сторону, об этом свидетельствует повышение интереса государства к вопросам информатизации и защиты информации.

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

СПИСОК ЛИТЕРАТУРЫ:

1. *Петренко С. А.* Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. М., 2004. — 384 с. илл.
2. ГОСТ Р ИСО/МЭК 15408—2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. М., 2002.
3. РД Гостехкомиссии России // Internet URL http://www.fstec.ru/.
4. *Медведовский И. Д.* Современные методы и средства анализа и контроля рисков информационных систем компаний // Internet URL http://www.dsec.ru/about/articles/.
5. Сайт стандарта BSI // Internet URL http://www.bsi.de/english/publications/index.htm.
6. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС - 1.0 — 2006.
7. *Саати Т.* Принятие решений: Метод анализа иерархий / Пер. с англ. М., 1993. — 278 с. илл.