УДК 004.056

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ОЦЕНИВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ КОМПАНИИ

А.А.ЗАМУЛА, В.И.ЧЕРНЫШ, Ю.В.ЗЕМЛЯНКО

Проводится сравнительный анализ методов оценивания рисков. Рассматривается перспективный математический метод оценивания информационных рисков корпоративной сети.

Ключевые слова: методы, информационные риски, аудит информационной безопасности.

ВВЕДЕНИЕ

В настоящее время на практике используются различные методы оценки и управления информационными рисками. Процедуры оценивания информационных рисков компании разделяют на следующие этапы :

- идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса;
- оценивание возможных угроз;
- оценивание существующих уязвимостей;
- оценивание эффективности средств обеспечения информационной безопасности.

Под риском понимают фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности. Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. При этом показатели ресурсов, значимость угроз и уязвимостей, эффективность средств защиты могут быть определены количественными и качественными методами.

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса компании. При этом вероятность того, что угроза реализуется, определяется следующим основными показателями:

- привлекательностью ресурса;
- возможностью использования ресурса для получения дохода;
- техническими возможностями реализации угрозы;
- степенью легкости, с которой уязвимость может быть использована.

Оценивание рисков относится к классу слабоструктурированных задач, в описании которых присутствуют не только числовые (количественные), но нечисловые (качественные) характеристики.

В настоящее время невозможно получить исчерпывающее количественное описание состоянии информационной безопасности прежде всего потому, что, во-первых за время, необходимое для его получения, обстановка внутри и вне корпоративной системы может сильно изменяться. А во-вторых, если и возможно получить подобное описание, то воспользоваться им будет нецелесообразно ввиду его сложности и потребности значительных вычислительных ресурсов, необходимых для его реализации. Поэтому на практике анализ состояния информационной безопасности корпоративной системы и оценка ее характеристик почти всегда выполняется аудитором непосредственно во время аудита информационной безопасности компании [1].

На современном этапе развития информационных технологий оценивание информационных рисков может быть автоматизировано при помощи соответствующих программно-технических систем.

В последнее время широко распространены многочисленные методы обработки нечисловой информации, среди которых наибольшую известность получили методы экспертных оценок [2]. При использовании этих методов основным источником информации служит эксперт в области безопасности корпоративных систем. Важнейшей идеей, лежащей в основе использования методов экспертных оценок, является декомпозиция сложной трудноформализуемой задачи на последовательность более простых задач, соответствующих определенному виду элементарных экспертиз.

В настоящее время хорошо известен ряд программных методов оценки рисков: CRAMM, RiskWatch, ГРИФ и др.

В основе метода CRAMM лежит комплексный подход к оценке рисков, который сочетает количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций как правительственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний (profiles). Для коммерческих организаций имеется Коммерческий профиль (Commercial Profile), для правительственных организаций – Правительственный профиль (Government profile).

К достоинствам метода CRAMM относят следующее:

- CRAMM является хорошо структурированным и широко опробованным методом ана-

лиза рисков, позволяющим получать реальные практические результаты;

• в основе программного продукта лежит достаточно объемная база знаний по контрмерам в области информационной безопасности, базирующаяся на рекомендациях стандарта BS 7799;

• CRAMM можно использовать в качестве инструмента для разработки плана непрерывности бизнеса;

• данная методика позволяет экономически обосновывать расходы организации на обеспечение информационной безопасности.

К недостаткам метода CRAMM можно отнести следующее:

• использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора;

• CRAMM в большей степени подходит для аудита уже существующих информационных систем, находящихся на стадии эксплуатации, нежели чем находящихся на стадии разработки;

• аудит по методу CRAMM – процесс достаточно трудоемкий и может потребовать значительного времени непрерывной работы аудитора;

• программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются «предсказание годовых потерь» и оценка «возврата от инвестиций. Программа RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. В этом продукте риски в сфере информационной и физической безопасности компьютерной сети предприятия рассматриваются совместно [3].

Основными достоинствами RiskWatch являются:

• точная количественная оценка соотношения потерь от угроз безопасности и затрат на создание системы защиты;

• возможность программной реализации;

• обеспечение соответствия требованиям стандартов.

К недостаткам RiskWatch можно отнести:

• такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов;

• полученные оценки рисков далеко не исчерпывает понимание риска с системных позиций – метод не учитывает комплексный подход к информационной безопасности.

Для проведения полного анализа информационных рисков необходимо построить полную модель информационной системы с точки зрения информационной безопасности. Для решения этой задачи метод ГРИФ, в отличие от представленных на рынке западных систем анализа рисков, которые громоздки, сложны в использовании и часто не предполагают самостоятельного применения ИТ-менеджерами и системными администраторами, обладает простым и интуитивно понятным для пользователя интерфейсом. Основная задача системы ГРИФ - дать возможность ИТ менеджеру самостоятельно оценить уровень рисков в информационной системе, оценить эффективность существующей практики по обеспечению безопасности компании.

В программном инструментарии ГРИФ создается наиболее полная классификация угроз, можно сделать вывод которая описывает все существующие угрозы. Оценивая вероятность реализации актуальных для ценного ресурса угроз, можно сделать выводы о уровне информационные риски предприятия.

К достоинствам метода ГРИФ относят следующее:

• простота в использовании;

• позволяет ИТ-менеджеру самостоятельно проводить оценивание информационных рисков;

• относительно невысокая стоимость продукта;

• интерфейс на русском языке.

К недостаткам ГРИФ можно отнести:

• отсутствие привязки к бизнесс-процессам (запланировано в следующей версии);

• нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности.

В Таблице 1 приводится сравнительный анализ представленных выше методов. Сравнение проводилось по следующим критериям: возможность обновлений, легкость работы для пользователя, стоимость лицензии за одно рабочее место, наличие сетевого решения, а также тип оценки.

Таблица 1

Критерии сравнения	CRAMM	RiskWatch	ГРИФ 2005
Поддержка	Обеспечивается		
Легкость работы для пользователя	Требует специальной подготовки и высокой квалификации аудитора		Не требует специальных знаний в области ИБ
Стоимость лицензии (1рабочее место, у.е)	От 2000 до 5000	От 10 000	От 1000
Тип оценки	Качественная	Количественная	Качественная и количественная
Сетевое решение	Отсутствует		Корпоративная версия Digital Security Office 2005

У эксперта всегда возникают трудности при анализе рисков, а если их число велико и они плохо структурированы, то линейное ранжирование рисков и выбор среди них наиболее значимого

превращается в сложную задачу. Лимит времени, отводимого на аудит информационной безопасности корпоративных систем, необходимость учета нечисловых характеристик системы защиты информации требуют разработки новых подходов к ее решению. Возможный выход из создавшегося положения заключается в использовании в качестве основной процедуры сравнения и оценки сценариев метода парных сравнений [1] .

Рассмотрим решение задачи:

Дано:

1. $R=(r_1,r_2,r_3,...,r_k)$ – множество рассматриваемых рисков информационной безопасности корпоративной системы.

2. Каждый из рассматриваемых r_g рисков информационной безопасности корпоративной системы характеризуется вектором характеристик

$$y^{(g)}=(y_1^{(g)}, y_2^{(g)},...y_p^{(g)}, y_{p+1}^{(g)},... y_n^{(g)}),$$

где $y_t^{(g)}, t=1,...,p$ – нечисловые характеристики анализируемого риска r_g, $y_j^{(g)}$, $j=p+1,..,n$ – числовые характеристики.

3. Предполагается, что в распоряжении аудитора имеются удовлетворяющие его весовые коэффициенты рисков k_m ,учитывающие числовые параметры $y_j^{(g)}$, $j=p+1,..,n$, $l=p+1,..,n$, $m=p=1,..,n$. Для числовых параметров это не является сложной задачей. Весовой коэффициент k_m, является целым положительным числом и несет информацию о сравнительной опасности риска r_l по отношению к риску r_m по рассматриваемой характеристике. Он используется только для того, чтобы упорядочить риски $R=(r_1,r_2,r_3,...,r_k)$ и определить первоочередные действия по предотвращению инцидентов.

Приведенная формализованная задача встречается в практике современного аудита информационной безопасности корпоративных систем. Один из вариантов ее решения основан на результатах математических методов теории квалиметрических шкал, модели линейного упорядочения альтернатив и парных сравнений [2, 4]. Каждый в отдельности из вышеназванных методов не позволяет решить поставленную задачу с приемлемыми для практических нужд точностью и затратами вычислительных ресурсов.

Ряд специальных работ в области защиты информационных технологий свидетельствует о том, что назначение весовых коэффициентов или назначение вероятностей наступления каких-либо событий является сложной операцией для аудитора [5]. В то же время сравнение двух значений по шкале измерения одного параметра является допустимой операцией в непрерывных и дискретных интервальных и порядковых шкалах, поскольку имеются результаты экспериментов, свидетельствующие о том, что аудитор может выполнять подобные операции с малыми противоречиями. Поэтому пусть варианты рисков корпоративной системы r_g попарно сравниваются с точки зрения их значимости для обеспечения безопасности системы по фиксированной нечисловой характеристике, а результаты сравнений записываются в виде матрицы парных сравнений $A=(a_{is})_{kxk}$ в вероятной калибровке [2]. При задании матрицы парных сравнений в вероятностной калибровке аудитору потребуется решить сложную задачу определения функции принадлежности рисков r_g к нечеткому бинарному отношению большей значимости одного из них над другим по рассматриваемой характеристике $\mu_R: RxR \rightarrow [0,1]$ $\mu_R(r_t, r_s)=P(r_t > r_s)$. $P(r_t > r_s)$ – вероятность того, что риск r_t, в случае его реализации, приводит к более тяжелым последствиям, чем реализация риска r_s. Элементы матрицы парных сравнений в вероятностной калибровке удовлетворяют следующим соотношениям $\forall i \; \forall j \; 0 \le a_{ij} \le 1 \; a_{ij}+a_{ji}=1$. Приведенная в табл. 2 шкала строго линейного порядка выполняет квантификацию качественных субъективных суждений эксперта об уровне риска r_g по фиксированной характеристике $y_i^{(g)}$, $t=1,..,p$, описываемой нечисловой величиной.

Таблица 2

Пункты квалиметричкой шкалы h_i	Определение значения	Комментарий относительно смысла значения
h_0	Значимость анализируемого риска практически низкая	Аудитор полагает, что риска практически нет
h_2	Значимость анализируемого риска умеренная	Аудитор полагает, что риск есть
h_4	Значимость анализируемого риска существенная	Аудитор полагает, что риск существенен
h_1, h_3, h_5	Промежуточные оценки между двумя соседними суждениями	Применяются в компромиссных случаях
h_6	Значимость анализируемого риска существенная – очень сильная	Аудитор полагает, что анализируемый риск – самый большой

Для построения матрицы парных сравнений в вероятностной калибровке квалиметрическая шкала строго линейного порядка $S=<H,R>$ подвергается арифметизации. Задача арифметизации шкалы состоит в приписывании определенных действий чисел пунктам h_i носителя H шкалы S с сохранением заданных отношений, входящих в структуру $R_>$ этой шкалы. При оценке весовых коэффициентов наиболее распространена ситуация, когда арифметизация квалиметрической шкалы $S=<H,R_>>$ происходит в условиях дефицита информации, что проявляется в затруднении аудитора отдать предпочтение той или иной допустимой арифметизации. Основываясь на результатах математических методов теории квалиметрических шкал, можно получить следующие теоретически обоснованные расчетные формулы [4]. Пусть в результате попарного сравнения

рисков r_t и r_s по фиксированной нечисловой характеристике аудитор относит риск r_t к пункту h_p квалиметрической шкалы строго линейного порядка $S=<H,R_>>$, где $H=(h_0,h_1,h_2,h_3,h_4,h_5,h_6)$, пара $(h_i,h_{i+1}) \in R$ i=0,1...,5, h_i, i=0,1,...6 – пункты в таблице 2 шкалы S, $R_>$ – отношение строго линейного порядка, заданное на носителе H, а риск r_s к пункту h_q, $p \neq q$.

Тогда элементы матрицы парных сравнений $A(t,s)=(a_{ts})_{kxk}$ в вероятностной калибровке определяются следующим образом:

$$a_{ij}=\sum_{S=1}^{z} p_s \sum_{g=0}^{s-1} p_q + 0{,}5\sum_{i=0}^{z} p_i p_q,$$

$$a_{ij}=1-a_{ij},$$

где: $p_s(p_q)$ – вероятность приписывания пункту $h_p(h_q)$ шкалы S=<H, R$_>$> числового значения $\frac{s}{z}$, $s=0,1,...z$ $\left(\frac{q}{z},q=0,1,...z\right)$ в результате арифметической шкалы $S=<H,R_>>$ в нормированную шкалу баллов $SB=<H,R_\geq>$ с носителем шкалы $Z=\left\{0,\frac{1}{z},\frac{2}{z},...,\frac{z-1}{z},1\right\}$ и отношением линейного порядка $R_\geq$ при помощи нормированного стохастического процесса с равновероятностными монотонными траекториями. Они представляют собой наборы точек прямоугольной целочисленной решетки [0, m+1]x[0,z] размером (m+2)(z+1). В случае шкалы, представленной в табл. 2 m=5. Эти вероятности рассчитываются по следующим формулам [4]:

$$p_s=\binom{p+s-1}{s}\binom{5-p+z-s}{z-s}\binom{5+z}{z}^{-1}$$

$$p_{q=}\binom{p+q-1}{q}\binom{5-p+z-q}{z-q}\binom{5+z}{z}^{-1}$$

В данном случае погрешность арифметизации оценивается дисперсией случайной величины, принимающей числовое значения:

$$\frac{s}{z},s=0,1,...z\ \left(\frac{q}{z},q=0,1,...z\right)\ a_{ij}=0.5.$$

После утверждения аудитором предложенных ему весовых коэффициентов $k_{ij}=a_{ij}$ рисков r_g по фиксированной нечисловой характеристике, риски упорядочиваются при помощи построенной матрицы парных сравнений $A=(a_{is})_{kxk}$ и подмножеством оптимальных упорядочений $I^*_{opt}(A)_{kxk}$.

Модель функции доминирования ориентирована на обработку нечетких предпочтений лица, принимающего решения, – аудитора – при интеграции элементов матрицы парных сравнений $A=(a_{is})_{kxk}$ степенью принадлежности сравниваемых рисков r_i и r_j к нечеткому отношению предпочтения, заданному на множестве $R=(r_1,r_2,r_3,...r_k)$ рассматриваемых рисков информационной безопасности корпоративной системы. В этом случае функция доминирования $L_R(r_i)=max\ a_{ji}$ характеризует значимость риска r_i. При $L_R(r_i)=0$ – нет ни одного риска, который бы приводил к более тяжелым последствиям, чем риск r_i, а при $L_R(r_i)=1$ – есть риск, который по сравнению с риском r_i приводит к более тяжелым последствиям. Риски $R=(r_1,r_2,r_3,...r_k)$ упорядочиваются по возрастанию функции доминирования. При этом дополнительные ранжирующие факторы для устранения дележа мест не используются. Поэтому после упорядочения рисков r_i каждому из них приписывается числовое значение y_t,t=1,...,p, равное минимальному номеру риска r_t в оптимальном упорядочении $y_t=minN_i(I^*_{opt}(A)_{kxk})$.

В случае, когда бинарное отношение предпочтения $R_>$ на множестве рисков $R=(r_1,r_2,r_3,...r_k)$ задается системой аудитора, предполагается, что в основном источником информации служит человек, располагающий сведениями для принятия единственного решения.

В другом классе задач многокритериальной оптимизации под бинарным отношением предпочтения R$_>$ понимается отношение Парето или Слейтера [4], которое порождается параметрическим семейством (системой) критериев сравнительной эффективности :

$$\varphi_A=\{\varphi_i|\ R^2 \to E^1,\ i=1,...l\}$$

$$\varphi_i(r_t,r_s)\ W=W_i(r_t)-W_i(r_s)$$

$$\text{и } W_i: R \to E^1,\ i=1,...l$$

– критерии эффективности.

Зададим бинарные отношения $R_>^{(i)}$ следующим образом :

$$R_>^{(i)}=\{(r_t,r_s) \in R^2 \mid \phi_A(r_t,r_s) \in \delta\},\ i=1,2$$

где: $\delta_1=\{z \in E^l_+ \mid z \neq 0\}$; $\delta_2=\{z \in E^l_+ \mid z>0\}$.

$E^l_+=\{z_1,z_2,...z_l \in E^l \mid z_1,z_2,...z_l \geq 0\}$ – конус из неотрицательного ортанта пространства E^l.

В соответствии с заданием отношения $R_>^{(i)}$ векторные критерии эффективности $W(g)=(W_1(g), W_2(g), W_3(g),... W_l(g))$ и конусы δi, i=1,2 определяют следующие бинарные отношения:

$$r_t\ R_>^{(1)}\ r_s \leftrightarrow W_i(r_t) \geq W_i(r_s)\ i=1,...l \text{ и } W(r_t) \neq W(r_s)$$

$$r_t\ R_>^{(2)}\ r_s \leftrightarrow W_i(r_t) > W_i(r_s)\ i=1,...l.$$

Отношение $R_>^{(1)}$ получило название Парето, а $R_>^{(2)}$ – строгого доминирования (отношение Слейтера). Из определения видно, что решение является Парето – оптимальным, если значение любого из критериев можно улучшить лишь за счет ухудшения значений некоторых других критериев [6]. Если обозначить ядра отношений $R_>^{(1)}$ и $R_>^{(2)}$ (подмножество максимальных в R элементов через $P(R, W)$ и $S(R, W)$ соответственно, то ядро $S(R, W)$ называется множеством полуэффективных (слабоэффективных, оптимальных по Слейтеру) точек, а $P(R, W)$ – множеством эффективных (оптимальных по Парето) точек.

Если решение оценки рисков заключается в отыскании множества Парето, то методологи-

ческих проблем не возникает, а остаются только трудности вычислительного характера.

ЗАКЛЮЧЕНИЕ

Практический опыт аудита информационной безопасности корпоративной системы показал, что частные критерии $W_i(g)$ могут быть неравнозначными с точки зрения аудитора и несопоставимыми между собой. Назначение весовых коэффициентов, учитывающих различную значимость критериев $W_i(g)$, является субъективным и может расходиться у разных людей. Обзор различных методов назначения весов свидетельствует о том, что до последнего времени эта задача корректно не решена. Поэтому предлагается следующее. Поскольку область парето- оптимальных решений не зависит от масштаба измерения критериев $W_i(g)$, поскольку построение области Парето $P(R,W)$ по конечному множеству рисков корпоративной системы $R=(r_1,r_2,r_3,...r_k)$ сводится к непосредственному применению определения отношения Парето $R_{>}^{(1)}$ при $W_i(g)=y_i^{(g)}$. Если критерии $W_i(g)$ неравнозначны, то они упорядочиваются либо непосредственно аудитором, либо при помощи одной из моделей линейного упорядочения альтернатив. Затем по векторам $y^{(g)}$ области Парето $P(R,W)$ выделяют более значимые риски в результате применения механизма лексико- графической оптимизации с уступками, определяемого вектором уступок $\delta=(\delta_1, \delta_2,...\delta_k)$.

Анализ методов оценивания рисков показывает, что наиболее предпочтительным является метод ГРИФ. Данный метод при сравнительно невысокой цене дает количественные, качественные оценки, формирует отчет по всем ключевым ресурсам организации. Метод ориентирован на пользователей, не имеющих специальных знаний в области информационной безопасности.

Своевременность и правильность оценивания информационных рисков компании во многом определяет эффективность корпоративной системы обеспечения информационной безопасности [6]. В предложенном методе на основе сравнения и оценки сценариев метода парных сравнений обобщены, систематизированы и развиты практические результаты обработки нечисловой информации применительно к оценке рисков корпоративной системы. Результаты работы могут быть использованы для создания нового, более эффективного и практически обоснованного подхода к оценке информационных рисков компании и создания соответствующего программного продукта.

Литература.

[1] *С. А. Петренко, А.А. Петренко.* Аудит безопасности INTRANET. – Москва, 2002.

[2] *Белкин А.Р., Левин М.Ш.* Принятие решений: комбинаторные модели апроксимации информации. – М.: Наука, 1990.

[3] *Сергей Петренко, Сергей Симонов* «Методики и технологии управления информационными рисками» – IT Manager, 2004.

[4] *Ховалов Н.В.* Стохастические модели теории квалиметрических шкал. – Л.: ЛГУ, 1986.

[5] *Подиновский В.В., Ногин В.Д.* Парето-оптимальные решения многокритериальных задач – М: Наука, 1982.

[6] *С.А. Петренко, С.В. Симонов.* Анализ и управление информационными рисками. ДМИ Пресс. 2004.

Поступила в редколлегию 19.05.2011

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, канд. техн. наук, доцент. Область научных интересов: технологии защиты информации в информационно- телекоммуникационных системах.

Черныш Владислав Игоревич, студент кафедры БИТ ХНУРЭ. Область научных интересов: управление информационной безопасностью, техническая защита информации.

Землянко Юлия Валерьевна, ассистент кафедры информационных технологий ХГУПТ. Область научных интересов: научное обоснование направлений активизации исследования. Использование в учебном процессе игровых методик, видео-и медиа технологий.

УДК 004.056

Математичні методи оцінювання інформаційних ризиків компанії / О.А.Замула, В.І.Черниш, Ю.В. Землянко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 259–263.

Проводиться порівняльний аналіз методів оцінювання ризиків. Розглядається перспективний математичний метод оцінювання інформаційних ризиків корпоративної мережі.

Ключові слова: методи, інформаційні ризики, аудит інформаційної безпеки, управління інформаційною безпекою.

Табл. 2. Бібліогр.:06 найм.

UDC 004.056

Mathematical methods for estimating of a company's information risks / O.A.Zamula, V.I.Chernysh, Yu.V. Zemlyanko // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 259–263.

A comparative analysis of methods for assessing risks is performed. A perspective mathematical method of evaluating information risks of a corporate network is considered.

Keywords: methods, information risks, audit of information security.

Tab.2, Ref.:06 items.