УДК 004.056

А.С. Поморцев

Методика оценки рисков нарушения информационной безопасности организации с учётом квалификации экспертов

Предложена методика учёта квалификации экспертов при проведении оценки рисков нарушения информационной безопасности (ИБ) организации. Предложен подход для расчёта количественной и качественной оценки рисков нарушения ИБ организации.
Ключевые слова: информационная безопасность, оценка рисков, квалификация экспертов.

Оценка рисков нарушения ИБ для организаций различных форм собственности и сфер деятельности позволяет:

– обеспечивать поддержание системы ИБ в актуальном состоянии;

– определять целесообразность экономических затрат на обеспечение ИБ;

– проводить оценку эффективности внедрения новых технических средств обеспечения ИБ;

– повышать имидж компании и доверие клиентов.

Для формирования оценки используются две составляющие – количественная и качественная. Количественная оценка необходима для определения конкретной величины риска, а качественная – для интерпретации полученного результата.

Поскольку эксперты, проводящие оценку, могут обладать различной квалификацией, необходимо её учитывать для повышения точности конечного результата. В этой связи актуальной задачей является разработка новой методики оценки рисков нарушения ИБ [1].

Количественная оценка. В работе [2, 3] была приложена система из 25 групповых параметров N, характеризующих инфраструктуру обеспечения ИБ. Каждый групповой параметр N_i включает в себя ряд частных показателей EV_{N_i} в виде конкретных требований по обеспечению ИБ. Перечень групповых параметров и частных показателей может меняться в зависимости от специфики конкретной организации.

Частные показатели EV_{N_i}, входящие в каждый групповой параметр N_i, неравнозначны. Это обусловлено тем, что на практике выполнение некоторых требований по обеспечению ИБ может быть намного важнее других. Например, обеспечение контроля доступа на территорию организации важнее, чем обеспечение контроля доступа к персональному компьютеру работника, так как, если злоумышленник не сможет попасть на территорию организации, то он не сможет получить физический доступ к компьютеру сотрудника. Важность группового показателя по сравнению с другими характеризуется коэффициентом значимости α_{ij}, при этом должно учитываться условие нормировки

$$\sum_{j=1}^{k} \alpha_{ij} = 1 . \qquad (1)$$

Степень выполнения частных показателей x_n определяется экспертом (или множеством экспертов) по шкале с 5 уровнями градации (0; 0,25; 0,5; 0,75; 1) в зависимости от степени фактического выполнения и документирования.

Особенностью данного подхода является то, что коэффициенты значимости α_{ij} и степень выполнения частных показателей x_n определяются экспертами. В этой связи предъявляются особые требования к квалификации экспертов, что существенно ограничивает сферу применения данного подхода.

Решение данной проблемы предлагается осуществить за счёт увеличения числа экспертов с проведением предварительной оценки их квалификации. Квалификация экспертов оценивается по двум составляющим:

– выполнение формальных признаков (стаж работы, число часов повышения квалификации за последние два года и т.д.);

– тестирование (на знание предметной области, действующей нормативно-технической документации и законодательства).

По результатам прохождения оценки квалификации предлагается разделять экспертов на 3 уровня, с присвоением соответствующего коэффициента y_n:

– эксперты с высокой квалификацией ($y=2$);

– эксперты со средней квалификацией ($y=1{,}5$);

– эксперты с низкой квалификацией ($y=1$).

Это означает, что при проведении оценки рисков нарушения ИБ мнение эксперта с высокой квалификацией будет иметь условный вес в 2 раза больше, чем эксперта с низкой квалификацией.

Таким образом, численное значение степени выполнения частного показателя S, с учётом квалификации экспертов, будет рассчитываться по следующей формуле:

$$S=\frac{\sum x_n y_n}{\sum y_n}. \tag{2}$$

Значение частного показателя EV_{N_i} будет рассчитываться как произведение численного значения степени его выполнения и коэффициента значимости:

$$EV_{N_i}=\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}. \tag{3}$$

Значение группового параметра N_i будет рассчитываться как сумма всех входящих в него частных показателей:

$$N_i=\sum_{i=1}^{k}\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}. \tag{4}$$

Среднее значение группового параметра D находится по формуле

$$D=\sum_{j=1}^{N}\sum_{i=1}^{k}\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}\Bigg/N. \tag{5}$$

Для дальнейших расчётов принимаем следующее условие – в случае полного выполнения всех требований по обеспечению ИБ, определённых множеством частных показателей, риск нарушения ИБ организации $R\to 0$. В таком случае формула для расчёта процентного значения величины риска нарушения ИБ будет иметь вид

$$R=(1-D)\times 100. \tag{6}$$

В результате расчёт количественной оценки рисков нарушения ИБ организации принимает вид

$$R=\left(1-\sum_{j=1}^{N}\sum_{i=1}^{k}\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}\Bigg/N\right)\times 100. \tag{7}$$

Качественная оценка рисков нарушения ИБ. Для перехода от количественной оценки к качественной предлагается использовать метод неравномерных шкал [4]. Пусть качественная шкала оценки рисков имеет 5 уровней градации («низкий», «ниже среднего», «средний», «выше среднего», «высокий»), затем устанавливается соотношение между количественной и качественной оценками, представленное в таблице.

Таблица соответствия между количественными и качественными оценками

Уровень риска	Риск нарушения ИБ, %
Низкий уровень риска	0–5
Уровень риска ниже среднего	5–15
Средний уровень риска	15–30
Уровень риска выше среднего	30–50
Высокий уровень риска	50–100

Графическое представление соотношения количественной и качественной оценок показано на рис. 1.

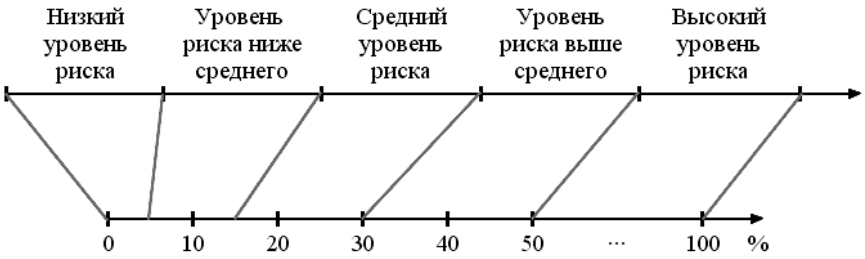

Рис. 1. Шкала соответствия качественных и количественных значений

В качестве апробации данной методики была проведена оценка рисков нарушения ИБ следующих организаций:

– ФГОБУ ВПО «СибГУТИ» (количественная оценка составила 66%, качественная – «высокий уровень риска»);

– ООО «Сибирский Центр Госзаказа» (количественная оценка риска составила 9,8%, качественная оценка – «уровень риска ниже среднего»). Данная оценка признана приемлемой, что подтверждается актом о проведении апробации.

По результатам проведения апробации были разработаны рекомендации в виде организационных и технических мер, направленных на снижение риска нарушения ИБ организации.

Заключение. В результате проведённых исследований можно сделать следующие выводы:

1. Поскольку эксперты могут обладать разной квалификацией, необходимо её учитывать при проведении оценки рисков нарушения ИБ.

2. Предложенная формула для расчёта количественной оценки риска нарушения ИБ позволяет учитывать квалификацию экспертов.

3. Для перехода от количественной оценки к качественной предложено использовать метод неравномерных шкал.

Литература

1. Поморцев А.С. Анализ методик оценки рисков предприятия // Материалы российской НТК «Современные проблемы телекоммуникаций», 25–26 апреля 2013 г. – Новосибирск: СибГУТИ, 2013. – С. 311–312.

2. Поморцев А.С. Об оценке рисков нарушений требований по обеспечению информационной безопасности предприятий телекоммуникационного профиля / А.С. Поморцев, А.А. Киселёв // Интернет-журнал «Технологии техносферной безопасности». – 2013. – № 3 (49). – С. 1–5.

3. Анализ и выбор параметров оценки рисков нарушения информационной безопасности организаций / С.Н. Новиков, А.А. Киселёв, А.С. Поморцев, О.В. Корзун // Ваш надежный партнер: информ. бюл. Новосиб. гор. торгово-пром. палаты. – 2013. – № 2 (69). – С. 11–12.

4. Сергеев А.Г. Метрология. Стандартизация. Сертификация: учеб. пособие для вузов / А.Г. Сергеев, М.В. Латышев, В.В. Терегеря. – М.: Логос, 2005. – 559 с.

Поморцев Антон Сергеевич
Аспирант каф. безопасности и управления в телекоммуникациях
Сибирского государственного университета телекоммуникаций и информатики (СибГУТИ), Новосибирск
Тел.: +7 (383) 2-69-82-45
Эл. почта: pomortsev.anton@gmail.com

Pomortsev A.S.

Risk assessment methodology violations of information security with regard to the qualifications of Experts

A method for accounting qualification of experts in risk assessment of information security violations is proposed. An approach for calculating the quantitative and qualitative assessment of risks of violation of information security is proposed.

Keywords: information security, risk assessment, qualification of experts.