УДК 004.056

Т.И. Булдакова, Д.А. Миков

МЕТОД ПОВЫШЕНИЯ АДЕКВАТНОСТИ ОЦЕНОК ИНФОРМАЦИОННЫХ РИСКОВ

Проанализированы основные подходы к оценке информационных рисков и отмечены ограничения их практического применения. Предложен метод повышения адекватности оценок с использованием коэффициента конкордации.

E-mail: buldakova@bmstu.ru

***Ключевые слова*:** *защита информации, информационные риски, методы оценки, коэффициент конкордации*

Введение. В настоящее время оценка и управление информационными рисками представляют собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. Основная задача направления — объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски, а также определить адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании. Качественное оценивание и управление информационными рисками позволяет выбрать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании.

Анализ методов оценки рисков. Существует большое количество методов и инструментальных средств, которые можно применить для оценки рисков информационной безопасности (ИБ). Однако конкретный выбор наиболее эффективного подхода — сложная и чрезвычайно важная задача для каждой компании. Целесообразно выделить следующие основные методы оценки рисков информационной безопасности, широко применяющиеся во многих организациях [1]:

1) статистические методы;
2) методы моделирования;
3) специализированное программное обеспечение;
4) методы экспертных оценок.

Статистические методы предполагают анализ уже накопленных данных о реально случавшихся инцидентах, связанных с нарушением ИБ. На основе результатов такого анализа строятся предположения о вероятности проведения атак и уровнях ущерба от них в аналогичных корпоративных информационных системах (КИС). Анализировать можно как внутреннюю статистику самой компании, так и внешнюю статистику других организаций. Несмотря на достаточную распространенность и простоту в применении статистических методов, их использование не может являться серьезным решением задач оценки рисков ИБ. Это связано с неполнотой и, зачастую,

с неточностью накопленных статистических сведений, а также в силу их неспособности учитывать скрытые уязвимости КИС компании, с которыми не был связан ни один инцидент ИБ, но которые могут стать причиной инцидентов в будущем.

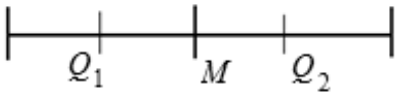
Методы моделирования основаны на построении, изучении и анализе математических моделей, описывающих функционирование КИС. В отличие от статистических методов, методы моделирования являются более точными, однако могут возникнуть сложности при разработке математической модели КИС. Как правило, неясно, какие параметры необходимо закладывать, как с наибольшей достоверностью описать все взаимосвязи и взаимодействие между различными характеристиками КИС. Кроме того, недостатками в использовании таких методов являются высокая стоимость разработки и сложность в формировании точного логического вывода о информационных рисках, так как данный процесс очень трудно разложить на простые составляющие. Таким образом, моделирование КИС и управление информационными рисками на основе математических моделей — сложная задача, и требуется время для внедрения этого метода в практическую деятельность компаний.

Существует ***специализированное программное обеспечение***, позволяющее автоматизировать процесс анализа исходных данных и расчет значений информационных рисков при аудите и управлении рисками ИБ. Такое программное обеспечение, как правило, дорогостоящее и при этом не всегда позволяет адекватно оценить требуемые параметры для конкретной организации вследствие слишком большого разброса возможных характеристик, сфер деятельности и условий функционирования различных компаний. Однако применение указанного метода может оказаться полезным в сочетании с другими методами, позволяющими проанализировать результаты, полученные по итогам работы программного обеспечения. В настоящее время наибольшее распространение получили программные комплексы CRAMM, RiskWatch и ГРИФ [2]. Наиболее эффективен программный комплекс ГРИФ, поскольку он не требует специальной подготовки в области иностранных языков, высокой квалификации аудитора, серьезных временных и финансовых затрат на установку, настройку и применение комплекса. Кроме того, с помощью комплекса ГРИФ процесс анализа информационных рисков обеспечивается всей необходимой отчетностью (без излишней бумажной документации) с использованием как количественной, так и качественной оценки. Комплекс ГРИФ также обладает модулем для сетевого применения.

При использовании ***методов экспертной оценки*** анализируются результаты работы группы экспертов, компетентных в области ИБ, которые на основе имеющегося у них опыта определяют количественные или качественные уровни информационных рисков [3]. Поскольку применение одного эксперта для получения количественных оценок объекта или явления крайне неэффективно (возникают вопросы по поводу релевантности, достоверности), то при проведении опроса, как правило, участвует группа квалифицированных экспертов. В качестве экспертов

могут выступать как специалисты организации, обладающие соответствующей информацией, так и внешние консультанты. Методы экспертной оценки наиболее распространены, но при этом они характеризуются достаточной субъективностью, непрозрачностью и непроверяемостью экспертного мнения. Нельзя с абсолютной уверенностью знать, на основании каких факторов эксперт сделал вывод. При этом очень важно обеспечить согласованность и релевантность формируемых оценок в группе. Поэтому неизбежно возникает вопрос об адекватности оценок и решений, предлагаемых экспертами. Такие методы экспертного опроса, как анкетирование, интервьюирование, метод комиссии, мозговой штурм не могут решить эту проблему [4]. В конечные результаты могут попасть совершенно неадекватные и ничем не обоснованные оценки, которые негативно повлияют на точность и эффективность итогового решения.

Предлагаемое решение проблемы. Повысить объективность оценок информационных рисков можно с помощью метода Дельфи, суть которого заключается в разбиении всех экспертных оценок на два равных интервала (рисунок).



Шкала оценок метода Дельфи

Экспертов, чьи оценки попадают в крайние интервалы (не лежат внутри некоторого диапазона Q_1—Q_2), просят обосновать свое мнение по поводу этих оценок. С их обоснованием и выводами (не указывая, от кого именно они получены) знакомят остальных экспертов. Подобная процедура позволяет специалистам изменять, при необходимости, свою оценку, принимая в расчет те обстоятельства, которые они могли случайно упустить или которыми пренебрегли на первом этапе опроса. С учетом этого результаты второго и последующих этапов опроса дают, как правило, меньший разброс оценок. Однако метод Дельфи предполагает большие затраты времени на многоэтапную экспертизу, вследствие чего полученные сведения могут потерять актуальность. Кроме того, применение указанного метода может привести к поверхностному индивидуальному анализу проблемы и стремлению к «групповому» мнению.

Избежать подобной громоздкости и чрезмерной длительности проведения экспертного опроса, а также исключить мнения экспертов, значительно выпадающие из общего контекста, позволяет коэффициент конкордации [5]. Для его использования не требуется многоэтапного опроса, достаточно одного этапа с последующей обработкой полученных данных, у которой может быть несколько циклов, но при этом задействуется один человек для проведения математических расчетов. Коэффициент конкордации W рассчитывается по формуле

$$W = \frac{12S}{m^2\left(n^3 - n\right)},$$

где S — сумма квадратов отклонений сумм рангов (ответов всех экспертов на каждый вопрос) от среднего значения суммы рангов по предмету (объекту) исследования; m — число экспертов; n — число вопросов. Коэффициент конкордации W принадлежит интервалу [0, 1]. Чем ближе значение коэффициента к единице, тем выше уровень согласования мнений экспертов. Обычно минимально допустимое значение коэффициента конкордации составляет 0,4. При несоблюдении этого условия следует провести коллективное обсуждение, выяснить причины существенных расхождений в оценках экспертов и скорректировать эти оценки так, чтобы получить согласованный результат.

Особенности применения предлагаемого метода. Покажем возможный вариант использования метода конкордации на примере проведения экспертного опроса об уровне критичности защищаемых информационных активов и ресурсов компании. Предположим, что компания обладает следующими наиболее важными информационными активами и ресурсами:

— сервер КИС;
— персональный компьютер (ПК) генерального директора;
— ПК исполнительного директора;
— автоматизированное рабочее место (АРМ) главного инженера;
— конструкторская документация;
— технологическая документация;
— АРМ главного бухгалтера;
— бухгалтерский баланс;
— отчет о движении денежных средств;
— АРМ управляющего сбытом;
— ПК директора по кадрам;
— личные дела сотрудников;
— АРМ заведующего складской группой;
— накладная и счет-фактура.

Группа из 10 экспертов должна оценить значимость каждого из перечисленных ресурсов и активов для компании. Для оценки будет использоваться количественно-качественная шкала от 1 до 10, состоящая из уровней (в скобках указаны соответствующие количественные показатели): минимальный (1, 2); низкий (3, 4); умеренный (5, 6); высокий (7, 8); критический (9, 10).

Для облегчения процесса оценки экспертам целесообразно использовать соответствующие денежные эквиваленты. Для этого необходимо определить бюджет, который компания ежегодно тратит на ИБ. Эта стоимость будет соответствовать максимальному уровню критичности актива — 10 баллов, так как все, что по стоимости превышает общие затраты компании на ИБ, является наиболее критичным. Например, если ежегодные затраты составляют 1 млн руб., то эксперт, разделив денежную стоимость ресурса в рублях (V) на 100 000, получает (с учетом округления) количественный балл критичности защищаемого актива

$$A = \frac{V}{100\ 000},$$

после чего ставит ему в соответствие качественный уровень шкалы.

Каждый эксперт должен самостоятельно определять стоимость каждого актива, поскольку невозможно оценить ее однозначно. При этом эксперту необходимо учитывать и возможный ущерб, который понесет компания в результате потери конфиденциальности, целостности или доступности информации, содержащейся в активе. Экспертные оценки заносятся в сводную таблицу, далее для расчета коэффициента конкордации вычисляются суммы оценок по каждому активу, среднее арифметическое этих сумм, отклонение от среднего арифметического и квадрат отклонения (табл. 1).

Таблица 1

Сводная таблица оценки критичности защищаемых активов

Защищаемые активы	Экспертные оценки уровня критичности защищаемых активов										Сумма рангов	Отклонение от среднего (61)	Квадрат отклонения
	1	2	3	4	5	6	7	8	9	10			
Сервер КИС	1	6	8	1	7	10	6	8	3	6	56	5	25
ПК генерального директора	8	8	6	8	1	9	1	3	8	4	56	5	25
ПК исполнительного директора	6	3	6	2	10	9	10	9	9	10	74	13	169
АРМ главного инженера	5	10	1	8	9	1	9	2	8	10	63	2	4
Конструкторская документация	6	3	6	2	6	9	1	3	8	1	45	16	256
Технологическая документация	3	3	6	9	1	3	8	9	7	10	59	2	4
АРМ главного бухгалтера	5	6	9	1	3	8	2	1	8	10	53	8	64
Бухгалтерский баланс	6	5	10	2	9	3	6	3	6	4	54	7	49

Защищаемые активы	Экспертные оценки уровня критичности защищаемых активов										Сумма рангов	Отклонение от среднего (61)	Квадрат отклонения
	1	2	3	4	5	6	7	8	9	10			
Отчет о движении денежных средств	10	8	1	7	10	6	8	2	10	1	63	2	4
АРМ управляющего сбытом	8	1	7	10	6	8	9	10	5	6	70	9	81
ПК директора по кадрам	9	1	3	8	6	7	10	6	8	10	68	7	49
Личные дела сотрудников	2	9	2	1	1	5	10	7	10	6	53	8	64
АРМ заведующего складской группой	8	10	2	9	7	8	6	10	1	8	69	8	64
Накладная и счет-фактура	3	6	6	7	10	6	8	10	2	9	67	6	36

Суммируя значения квадратов отклонений, получаем

$$S = 25 + 25 + 169 + 4 + 256 + 4 + 64 + 49 + \\ + 4 + 81 + 49 + 64 + 64 + 36 = 894.$$

Затем приступаем к расчету коэффициента конкордации:

$$W = \frac{12 \cdot 894}{100 \cdot \left(2\ 744 - 14\right)} = \frac{10\ 728}{273\ 000} = 0,04 .$$

В рассмотренном случае $W < 0,4$ (оценки несогласованны), поэтому необходимо избавиться от самых крайних оценок, наиболее отличающихся от среднего арифметического по каждому активу (табл. 2).

Таблица 2

Сводная таблица оценки критичности защищаемых активов (цикл 1)

Защищаемые активы	Экспертные оценки уровня критичности защищаемых активов										Сумма рангов	Отклонение от среднего (57)	Квадрат отклонения
	1	2	3	4	5	6	7	8	9	10			
Сервер КИС	**1**	6	8	1	7	10	6	8	3	6	56	5	25
ПК генерального директора	8	8	6	8	1	9	**1**	3	8	4	56	5	25
ПК исполнительного директора	6	3	6	**2**	10	9	10	9	9	10	74	13	169
АРМ главного инженера	5	10	**1**	8	9	1	9	2	8	10	63	2	4
Конструкторская документация	6	3	6	2	6	**9**	1	3	8	1	45	16	256
Технологическая документация	3	3	6	9	**1**	3	8	9	7	10	59	2	4
АРМ главного бухгалтера	5	6	9	1	3	8	2	1	8	**10**	53	8	64
Бухгалтерский баланс	6	5	**10**	2	9	3	6	3	6	4	54	7	49
Отчет о движении денежных средств	10	8	**1**	7	10	6	8	2	10	1	63	2	4
АРМ управляющего сбытом	8	**1**	7	10	6	8	9	10	5	6	70	9	81
ПК директора по кадрам	9	**1**	3	8	6	7	10	6	8	10	68	7	49
Личные дела сотрудников	2	9	2	1	1	5	**10**	7	10	6	53	8	64

Защищаемые активы	Экспертные оценки уровня критичности защищаемых активов										Сумма рангов	Отклонение от среднего (57)	Квадрат отклонения
	1	2	3	4	5	6	7	8	9	10			
АРМ заведующего складской группой	8	10	2	9	7	8	6	10	**1**	8	69	8	64
Накладная и счет-фактура	3	6	6	7	10	6	8	10	**2**	9	67	6	36

Примечание. Выделены самые крайние оценки, отличающиеся от среднего арифметического по каждому активу и исключенные из расчета.

Проводим повторный расчет:

$$S = 4 + 4 + 225 + 25 + 441 + 1 + 196 + 169 + \\ + 25 + 144 + 100 + 196 + 121 + 64 = 1\,715;$$

$$W = \frac{12 \cdot 1715}{81 \cdot (2\,744 - 14)} = \frac{20\,580}{221\,130} = 0,09 < 0,4\,.$$

Экспертные оценки несогласованны. Поэтому циклы обработки данных необходимо продолжить, убирая крайние оценки в каждой строке. В рассматриваемом случае потребовалось пять циклов обработки (табл. 3).

Таблица 3

Сводная таблица оценки критичности защищаемых активов (цикл 5)

Защищаемые активы	Экспертные оценки уровня критичности защищаемых активов										Сумма рангов	Отклонение от среднего (34)	Квадрат отклонения
	1	2	3	4	5	6	7	8	9	10			
Сервер КИС	**1**	6	**8**	**1**	7	**10**	6	8	**3**	6	33	1	1
ПК генерального директора	8	8	**6**	8	**1**	9	**1**	**3**	8	**4**	41	7	49
ПК исполнительного директора	**6**	**3**	**6**	**2**	**10**	9	10	9	9	10	47	13	169

Защищаемые активы	Экспертные оценки уровня критичности защищаемых активов										Сумма рангов	Отклонение от среднего (34)	Квадрат отклонения
	1	2	3	4	5	6	7	8	9	10			
АРМ главного инженера	**5**	**10**	**1**	8	9	**1**	9	**2**	8	10	44	10	100
Конструкторская документация	**6**	3	**6**	2	**6**	**9**	1	3	**8**	1	10	24	576
Технологическая документация	**3**	**3**	6	9	**1**	**3**	8	9	7	**10**	39	5	25
АРМ главного бухгалтера	5	**6**	**9**	1	3	**8**	2	1	**8**	**10**	12	22	484
Бухгалтерский баланс	6	5	**10**	**2**	**9**	**3**	6	**3**	6	4	27	7	49
Отчет о движении денежных средств	10	8	**1**	**7**	10	**6**	8	**2**	10	**1**	47	13	169
АРМ управляющего сбытом	8	**1**	7	**10**	6	8	**9**	**10**	**5**	6	35	1	1
ПК директора по кадрам	9	**1**	**3**	8	**6**	**7**	10	**6**	8	10	45	11	121
Личные дела сотрудников	2	**9**	2	1	1	5	**10**	**7**	**10**	**6**	11	23	529
АРМ заведующего складской группой	**8**	10	**2**	9	**7**	8	6	10	**1**	8	45	11	121
Накладная и счет-фактура	**3**	6	6	7	**10**	6	8	**10**	**2**	**9**	33	1	1

Примечание. Выделены самые крайние оценки, отличающиеся от среднего арифметического по каждому активу и исключенные на пятом цикле обработки.

Окончательно получаем:

$$S = 1 + 49 + 169 + 100 + 576 + 25 + 484 + \\ + 49 + 169 + 1 + 121 + 529 + 121 + 1 = 2395;$$

$$W = \frac{12 \cdot 2395}{25 \cdot (2\ 744 - 14)} = \frac{28\ 740}{68\ 250} = 0,42 > 0,4 .$$

Поскольку значение коэффициента конкордации W превысило пороговое значение, то экспертные оценки можно признать согласованными и приступить к расчету их среднего арифметического, убрав все выделенные значения из сводной таблицы (см. табл. 3). Оставшиеся оценки принимаются (считаются адекватными), и критичность каждого актива определяется как их среднее арифметическое с учетом округления (табл. 4).

Таблица 4

Итоговая оценка критичности защищаемых активов

Защищаемые активы	Уровень критичности защищаемых активов при обработке экспертных оценок	
	с использованием метода конкордации	без использования метода конкордации
Сервер КИС	7 (высокий)	6 (умеренный)
ПК генерального директора	8 (высокий)	6 (умеренный)
ПК исполнительного директора	9 (критический)	7 (высокий)
АРМ главного инженера	9 (критический)	6 (умеренный)
Конструкторская документация	2 (минимальный)	5 (умеренный)
Технологическая документация	8 (высокий)	6 (умеренный)
АРМ главного бухгалтера	2 (минимальный)	5 (умеренный)
Бухгалтерский баланс	5 (умеренный)	5 (умеренный)
Отчет о движении денежных средств	9 (критический)	6 (умеренный)
АРМ управляющего сбытом	7 (высокий)	7 (высокий)
ПК директора по кадрам	9 (критический)	7 (высокий)
Личные дела сотрудников	2 (минимальный)	5 (умеренный)
АРМ заведующего складской группой	9 (критический)	7 (высокий)
Накладная и счет-фактура	7 (высокий)	7 (высокий)

Из табл. 4 ясно, что без использования метода конкордации критичность всех активов лежит в небольшом диапазоне (5…7), что свидетельствует о недостаточной точности результатов, полученных лишь на основе среднего арифметического оценок. Метод конкордации помогает избежать включения ошибочных оценок в усредненные

показатели, которые в противном случае будут примерно равными и для критических, и для маловажных активов.

Заключение. Рассмотренный метод также можно использовать и для оценки вероятности реализации угроз и уязвимостей, и для оценки эффективности контрмер, выработанных для снижения уровня риска (перечень возможных контрмер удобно определять с помощью программного комплекса ГРИФ, а затем приступать к экспертной оценке с помощью метода конкордации для выбора наиболее результативных из них).

Главное преимущество метода — простота применения, возможность использования как для крупных, так и для малых предприятий.

СПИСОК ЛИТЕРАТУРЫ

1. Методы и средства анализа рисков и управление ими в ИС: [Электронный документ] (http://www.bytemag.ru/articles/detail.php?ID=9076).
2. Астахов А. Искусство управления информационными рисками. — М.: ДМК Пресс, 2010. — 312 с.
3. Экспертные методы в задачах оценки рисков информационной безопасности: [Электронный документ] (http://ua3gdw.info/ecoProtectt4r3part1.html).
4. Методы и модели анализа данных: OLAP и Data Mining / А.А. Барсегян, М.С. Куприянов, В.В. Степаненко. — СПб.: БХВ-Петербург, 2004. — 336 с.
5. Лагутин М.Б. Наглядная математическая статистика. — М.: БИНОМ. Лаборатория знаний, 2007. — 472 с.

Статья поступила в редакцию 4.07.2012