УДК 657.21.014.134:681.2

И.В. Федоренко

МЕТОДИЧЕСКИЕ ВОПРОСЫ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БУХГАЛТЕРСКОМ УЧЕТЕ

В статье рассматриваются методические вопросы оценки рисков информационной безопасности в бухгалтерском учете. Представлены направления оценки рисков и их классификация. Раскрыта методика оценки рисков информационной безопасности в бухгалтерском учете и кратко охарактеризовано содержание ее этапов.

***Ключевые слова**: риск, оценка риска, бухгалтерский учет, ущерб.*

I.V. Fedorenko

METHODOLOGICAL ISSUES OF THE INFORMATION SECURITY RISK ASSESSMENT IN ACCOUNTING

The methodological issues of the information security risk assessment in accounting are considered in the article. The risk assessment trends and the risk classification are presented. The methodology of the information security risk assessment in accounting is revealed, its stage content is briefly characterized.

***Key words**: risk, risk assessment, accounting, damage.*

Введение. В условиях рыночной экономики бухгалтерская отчетность должна давать достоверное представление о финансовом положении экономического субъекта на отчетную дату, финансовом результате его деятельности и движении денежных средств за отчетный период, необходимое пользователям этой отчетности для принятия экономических решений. Данные бухгалтерского учета и внутренней отчетности необходимы для менеджеров всех уровней для принятия верных и своевременных управленческих решений. На основе информации бухгалтерского учета исчисляются налоги в бюджетную систему Российской Федерации, а ошибки в их исчислении несут неблагоприятные последствия как для предприятий, так и для государства. Это определяет необходимость полноты, достоверности и своевременности информации, отражаемой в бухгалтерском учете.

Для оценки рисков информационной безопасности разработан специальный методический инструментарий, который используется специалистами в области информационной безопасности (ИБ) [7], в том числе различные программные продукты (как отечественной, так и зарубежной разработки). Для оценки же рисков системы бухгалтерского учета такой методический инструментарий не разработан. В современных работах специалистов [4, 5, 8, 12] рассматриваются только некоторые из аспектов рисков в бухгалтерском учете. В силу специфического характера информационной системы бухгалтерского учета требуется наличие для нее соответствующей методики оценки рисков информационной безопасности.

На основе исследования нормативных документов по бухгалтерскому учету, теоретических положений и взглядов специалистов в области бухгалтерского учета сделан вывод, что, выделив группы угроз, авторы, к сожалению, не осветили вопросы оценки этих угроз и связанных с ними рисков ИБ. Таким образом, методика оценки рисков информационной безопасности в бухгалтерском учете и инструменты снижения этих рисков практически не разработаны.

Цель исследований. Минимизировать риски информационной безопасности в бухгалтерском учете как специализированной информационной системе на основе разработанной методики.

Задачи исследований. Рассмотреть теоретические аспекты рисков информационной безопасности в бухгалтерском учете; проанализировать наличие, содержание и применимость различных методик оценки рисков информационной безопасности в бухгалтерском учете; разработать и апробировать методику оценки рисков информационной безопасности в бухгалтерском учете.

Материалы и методы исследований. В ходе исследований использовались общенаучные методы – группировка, обобщение, анализ, синтез, а также контент-анализ законодательных и нормативных актов в области бухгалтерского учета и защиты информации, моделирование, экспертная оценка.

Результаты исследований и их обсуждение. Специфической угрозой для бухгалтерского учета как информационной системы является недостоверность содержащейся в нем информации, которая может возникнуть вследствие различных факторов (преднамеренных и непреднамеренных ошибок учетного персонала или иных лиц, а также ошибок в используемых специализированных программных продуктах).

Для более полной оценки риска искажения информации была разработана классификация нежелательных событий в бухгалтерском учете как специализированной информационной системе. Оценка риска в рамках разработанной классификации позволит выявлять зоны повышенного риска с тем, чтобы принимать меры по его снижению.

Искажение или неполнота учетной информации могут возникнуть на любом этапе учетного процесса, поэтому при оценке рисков информационной безопасности в бухгалтерском учете следует анализировать все этапы ее движения. Однако неполнота и ошибки более ранних этапов автоматически сказываются на достоверности информации, формируемой на последующих этапах учета, поэтому этапу первичного наблюдения следует уделить наибольшее внимание.

В соответствии с ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения» [1] под риском понимается «сочетание вероятности события и его последствий».

Проведенный анализ литературы [2, с. 14–56; 3, 6, с. 18–26; 11, с. 7–19] показал, что существуют различные концепции риска, его определения и классификационные модели.

В качестве основы для проведения исследования была выбрана концепция риска как меры опасности, которая близка к классической теории риска.

Центральным звеном в концепции риска как меры опасности выступает *нежелательное событие*, результатом которого могут быть некие *неблагоприятные последствия* (расходы, убытки). Основные измерители риска: *сумма расходов* (убытков) как одна из мер неблагоприятного последствия и *вероятность* наступления нежелательного события (рис. 1).

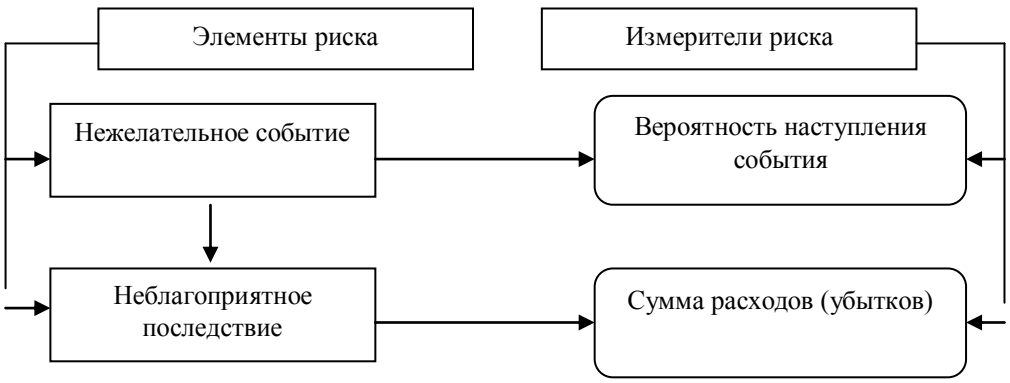

Рис. 1. Основные структурные элементы риска и их измерители

Ущерб как компонент риска связан с тяжестью последствий нежелательного события (НС) и может быть определен численно как сумма ущерба, или семантически (качественно) как категория (например, низкий, средний, высокий).

Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Общая идея этого подхода может быть выражена соотношением: риск есть произведение вероятности события на ущерб от него [3, с. 23]. Недостатком такого подхода (оценки риска как математического ожидания потерь) является снижение информативности в ходе проведения анализа рисков.

Использование уровневой оценки по двум факторам (без использования математического ожидания потерь как единственного результирующего показателя) позволяет полнее оценить риск.

При более высоких требованиях может использоваться модель оценки риска по трем факторам: угроза, уязвимость и цена потери [3, с. 61]. Однако в реализации такого подхода имеются сложности, которые могут привести к недостоверности результатов оценки [3, с. 61–62].

В табл. 1 представлены показатели оценки риска ИБ, реализованные в некоторых специализированных программных продуктах.

Таблица 1

Показатели оценки риска, используемые в программных продуктах

Показатель	Программный продукт				
	Risk Watch	COBRA	ГРИФ	CRAMM	CORA
Оценки риска	Мат. ожидание потерь (за год)	-	Несколько	Качественные и количественные	Количественные
Примечание	-	Уровни рисков не определяются	Отдельно для конфиденциальности, целостности и доступности оцениваются вероятность и задается ущерб	-	Оценивается пообъектно

Как видно из табл. 1, реализованные в программных продуктам методики используют отличные друг от друга подходы к оценке риска.

Как отмечает технический директор ООО «ПКИ» Андрей Сафонов, «существующие методы и средства имеют множество принципиальных недостатков. Учитывая, что основная причина ущерба есть прямое следствие нарушения свойств активов (конфиденциальности, целостности и т.п., а не реализации угроз), то, задав ущерб как следствие реализации угроз, каждая из которых может влиять на несколько свойств активов, может получиться, что один и тот же ущерб может быть учтен несколько раз» [7].

Проведя анализ методик оценки риска в пяти программных продуктов, А. Сафонов установил, что в трех из них ущерб оценивается на основе нарушения свойств активов (CRAMM, ГРИФ, BCM-Analyser), а в двух – на основе реализации угроз (Counter Measures, РискМенеджер-Авангард) [7].

Разработанная методика оценки рисков ИБ в бухгалтерском учете сформирована на основе произведенных ранее исследований по сущности и содержанию бухгалтерского учета [9], сформированной классификации рисков в бухгалтерском учете и методик оценки рисков информационной безопасности. Этапы разработанной методики представлены на рис. 2.

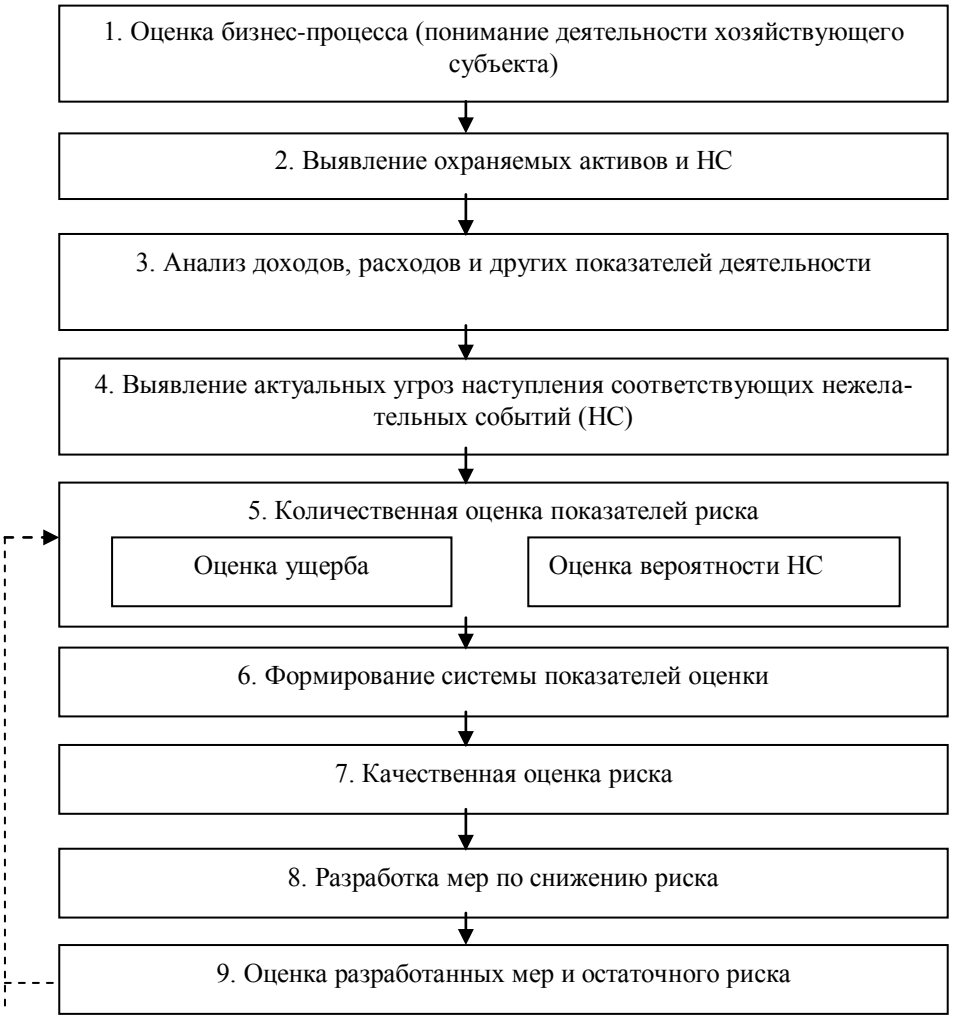

Рис. 2. Этапы оценки риска информационной безопасности в бухгалтерском учете

На *первом этапе* осуществляется оценка бизнес-процесса хозяйствующего субъекта. Цель этапа – понимание экспертом сущности осуществляемой деятельности и роли бухгалтерского учета в ней. Например, если акции открытого акционерного общества торгуются на организованном рынке, информация о прибыли будет оказывать существенное влияние на курс его акций и показатель капитализации.

На этом этапе эксперт получает информацию по следующим направлениям:

- место деятельности предприятия, юрисдикция и наличие филиалов и иных обособленных подразделений;
- организационно-правовая форма, форма собственности и основные собственники;
- виды осуществляемой деятельности;
- основные поставщики и покупатели;
- система налогообложения, освобождения и льготы;
- организация бухгалтерской службы и ее место в системе управления;
- структура бухгалтерской службы и разделение обязанностей;
- применяемые для ведения бухгалтерского учета программные продукты;
- наличия и полномочия служб контроля;
- результаты внешних и внутренних проверок.

На *втором этапе* осуществляется выявление актуальных охраняемых активов и нежелательных событий. Цель этого этапа – выявить и оценить активы организации, которые могут быть подвержены риску вследствие неэффективности работы системы бухгалтерского учета (СБУ). Возможные охраняемые активы и связанные с ними нежелательные события (НС) представлены в табл. 2.

Таблица 2

Пример перечня охраняемых активов и связанных с ними нежелательных событий

№ п/п	Группа активов / наименование НС	Причина влияния СБУ	Для каких организаций используется
1	Информация бухгалтерского учета	Обрабатывается средствами СБУ	Для всех
1.1	Недоступность информации		
1.2	Утрата информации		
1.3	Искажение информации		
1.4	Разглашение информации		
2	Денежные средства (ДС)	-	-
2.1	Отток ДС поставщикам	Досрочное предъявление требований по ГК РФ вследствие снижения чистых активов	Для АО, ООО
2.2	Штрафы налоговых органов	Штрафы по главе 16 НК РФ вследствие нарушений в учете	При интегрированной системе бухгалтерского и налогового учета
2.3	Административные штрафы	Штрафы по главе 15 КоАП вследствие нарушений в учете	Для всех организаций
2.4	Штрафы по договорам	Ошибки в учете расчетов	Для всех организаций
2.5	Разовое хищение ДС	Организационная – слабый контроль бухгалтерии в рамках учета ДС	Для всех организаций
2.6	Излишняя выплата дивидендов	Завышение прибыли	Для коммерческих организаций
2.7	Излишние выплаты ДС (любым лицам, с возможностью декомпозиции по категориям получателей и другим признакам)	Ошибки в учете расчетов	Для всех организаций
3	Капитализация		
3.1	Снижение капитализации	Информация о прибыли и активах в бухгалтерской отчетности	Для ОАО, акции которых торгуются на рынке
4	Дебиторская задолженность (ДЗ)	-	-
4.1	Убытки от списания ДЗ	Вследствие нарушений в учете	Для всех организаций
5	Основные средства (ОС)	-	-
5.1	Убытки от недостач и хищений ОС	Вследствие недостаточности контроля со стороны бухгалтерии	Для всех организаций
6	Материально-производственные запасы (МПЗ)	-	-
6.1	Убытки от недостач и хищений МПЗ	Вследствие недостаточности контроля со стороны бухгалтерии	Для всех организаций

Представленные в табл. 2 охраняемые активы и связанные с ними нежелательные события могут дополняться с учетом специфики конкретного хозяйствующего субъекта. Некоторые НС могут

быть признаны неактуальными для конкретного хозяйствующего субъекта.

В табл. 2 даны виды активов, из которых первый относится собственно к информационным, а остальные относятся к имущественным и финансовым активам.

Информация бухгалтерского учета выделена как специфический охраняемый актив (информационного характера).

Денежные средства – наиболее ликвидный имущественный актив, для которого сформировано несколько видов нежелательных событий;

Капитализация – текущая рыночная стоимость размещенных акций (актуальна только для акционерных обществ, акции которых торгуются на организованном рынке).

На *третьем этапе* проводится анализ доходов, расходов и других показателей деятельности. Цель этапа – знакомство эксперта с показателями финансово-хозяйственной деятельности экономического субъекта для последующего сопоставления их с оцениваемым размером ущерба. На этом этапе необходимо получить информацию об основных показателях финансово-хозяйственной деятельности не менее чем за три года (или иных периода оценки риска): план текущего года и фактические данные за два предшествующих.

Этапы с первого по третий носят подготовительный характер в оценке риска, обеспечивая сбор необходимой информации.

На *четвертом этапе* проводится выявление актуальных угроз наступления соответствующих нежелательных событий (НС). Цель этапа – выявить угрозы во взаимосвязи с выявленными на втором этапе нежелательными событиями.

Схема действий на четвертом этапе состоит в том, что сначала выявляются актуальные угрозы для НС, выявленные на втором этапе, и составляется перечень актуальных угроз во взаимосвязи с НС. После этого дополнительно анализируются угрозы, не включенные в перечень, на предмет их актуальности.

В случае выявления актуальных угроз, не включенных в перечень, перечень дополняется. При этом может быть дополнен и перечень НС.

При проведении количественной оценки на следующем этапе выделенные угрозы подлежат декомпозиции относительно предмета оценки (соответствующего раздела и/или этапа учетного процесса).

На *пятом этапе* проводится количественная оценка показателей риска (вероятности НС и суммы ущерба). Цель этого этапа – получить количественные показатели для анализа риска.

В случае наличия достаточных для анализа статистических данных оценка вероятности НС проводится на их основе и в последующем может корректироваться экспертом с учетом изменений, произошедших в учетной системе или БИС по отношению к прошедшим периодам (по которым использовались статистические данные).

При определении количества интервалов и определении их границ рекомендовано использовать критерий неприемлемости в качестве верхней границы интервала.

При оценке суммы ущерба информационных активов рекомендовано использовать методы, представленные в [10].

Итогом пятого этапа является получение числовых значений (S; p) для сформированных на четвертом этапе нежелательных событий.

На *шестом этапе* осуществляется формирование системы показателей оценки риска. Цель этого этапа – сформировать систему показателей оценки риска с учетом фактических и планируемых результатов деятельности хозяйствующего субъекта, проанализированных на третьем этапе.

Кроме показателей риска (S; p), в эту систему включено математическое ожидание потерь R, показатели оценки ущерба, соотнесенные с базовыми величинами (одно или несколько значений s). Возможно соотнести с базовыми величинами и ожидаемые потери. Рекомендованные показатели представлены в табл. 3.

На *седьмом этапе* проводится качественная оценка риска. Цель этапа – классифицировать риски по группам важности для последующего принятия управленческих решений.

Для этого можно использовать два подхода:

- на основе двух показателей риска (S; p);
- на основе системы всех показателей (табл. 3).

Таблица 3

Система показателей оценки риска

№ п/п	Условное обозначение	Наименование	Формула расчета	Примечание
1	S	Сумма убытков при наступлении НС	-	-
2	p	Вероятность наступления НС	-	-
3	R	Математическое ожидание ущерба	S·p	-
4	s	Сумма ущерба при наступлении НС, соотнесенная с базовым показателем	s/бп	бп – базовый показатель для сравнения
4.1	s(д)	Сумма ущерба по отношению к доходам	s/д	д – сумма доходов за оцениваемый период
4.2	s(п)	Сумма ущерба по отношению к прибыли	s/п	п – сумма прибыли за оцениваемый период
4.3	s(ча)	Сумма ущерба по отношению к чистым активам	s/ча	ча – сумма чистых активов за оцениваемый период
5	r	Математическое ожидание ущерба при наступлении НС, соотнесенное с базовым показателем	r/бп	-
5.1	r(п)	Математическое ожидание ущерба по отношению к прибыли	r/п	-
5.2	r(ча)	Математическое ожидание ущерба по отношению к чистым активам	r/ча	-

В рамках первого подхода для начала необходимо определить количество уровней классификации ущерба (как правило, от двух до пяти). Далее следует установить границы областей ущерба для выделенных групп. Затем при первом подходе классифицируется риск по критерию S, после чего для каждого НС определяется интегральный качественный показатель риска в рамках выбранной шкалы оценок.

При *втором подходе* используется система показателей оценки (табл. 3), где для каждого показателя r и s устанавливаются значения границ интервалов. Итоговая оценка устанавливается по худшему варианту, то есть выбирается наиболее высокое значение интегрального показателя риска.

На *восьмом этапе* осуществляется разработка мер по снижению риска.

Меры по снижению риска могут быть направлены:

- на снижение вероятности наступления НС;
- снижение суммы ущерба при наступлении НС;
- снижение как вероятности НС, так и ущерба;
- покрытие ущерба (страхование);
- избежание ответственности (переложение риска).

На *девятом этапе* проводится оценка разработанных мер и остаточного риска. Цель этого этапа – определить, достаточно ли разработанных мер для снижения риска до приемлемых значений, а также оценить экономическую эффективность разработанных мер.

На этом этапе проводится оценка риска (этапы 5–7) с учетом предположения о том, что разработанные меры внедрены. Кроме этого, оцениваются затраты на внедрение мер. Эти затраты сопоставляются с ожидаемым снижением риска и имеющимися финансовыми ограничениями.

В случае удовлетворительного соотношения показателей, разработанные меры принимаются или рекомендуются к внедрению, иначе разрабатываются альтернативные меры по снижению риска.

Заключение. Результаты исследований могут быть использованы специалистами в области информационной безопасности, практикующими бухгалтерами для снижения рисков в учетных системах. Кроме этого, они могут быть использованы организациями аудиторов, подразделениями внутреннего аудита при разработке методик оценки надежности систем бухгалтерского учета и внутреннего контроля, в том числе при разработке собственных внутренних стандартов и методик проведения аудита.

Литература

1. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения [Электронный ресурс] // Консультант Плюс.
2. *Вишняков Я.Д., Радаев Н.Н.* Общая теория рисков: учеб. пособие. – 2-е изд., испр. – М.: Академия, 2008. – 368 с.
3. *Золотарев В.В.*, *Данилова Е.А.* Управление информационной безопасностью: учеб. пособие. Ч. 1. Анализ информационных рисков / Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2010. – 144 с.
4. *Копылова Е.К.* Аудит условий формирования учетной информации на этапе предварительного планирования: автореф. дис. ... канд. экон. наук. – Иркутск, 2012. – 24 с.
5. *Порфирьева А.В.* Формирование системы сквозного контроля деятельности автономных учреждений: автореф. дис. … канд. экон. наук. – Йошкар-Ола, 2012. – 24 с.
6. *Рыхтикова Н.А.* Анализ и управление рисками организации: учеб. пособие. – М.: ФОРУМ: ИНФРА-М, 2009. – 240 с.
7. *Сафонов А.* Практическое применение методов и средств анализа рисков // Информационная безопасность. – 2010. – № 3 [Электронный ресурс] // URL: http://www.itsec.ru/articles2/techobzor/prakticheskoe-primenenie-metodov-i-sredstv-analiza-riskov.
8. *Толстова А.С.* Бухгалтерские риски и их влияние на достоверность бухгалтерской отчетности: автореф. дис. … канд. экон. наук. – Йошкар-Ола, 2009. – 20 с.
9. *Федоренко И.В.* Виды информации в бухгалтерском учете и их классификация с учетом норм закона «О бухгалтерском учете» №402-ФЗ // Учет, анализ, аудит: проблемы теории и практики: сб. науч. тр. / под общ. ред. *Г.И. Золотаревой;* Сиб. гос. аэрокосм. ун-т. – Красноярск, 2012. – Вып. 10. –С. 111–115.
10. *Федоренко И.В., Лапина Е.В., Золотарев В.В.* Методика оценки рисков информационной безопасности в бухгалтерском учете // Учет, анализ, аудит: проблемы теории и практики: сб. науч. тр. / под общ. ред. *Г.И. Золотаревой*; Сиб. гос. аэрокосм. ун-т. – Красноярск, 2012. – Вып. 9. – С. 156–159.
11. *Чернова Г.В., Кудрявцев А.А.* Управление рисками: учеб. пособие. – М.: Проспект, 2009. – 160 с.
12. *Шевелев А.Е., Шевелева Е.В.* Риски в бухгалтерском учете: учеб. пособие. – 2-е изд., перераб. и доп. – М.: КНОРУС, 2009. – 304 с.