Арженовский Сергей Валентинович
д-р экон. наук, профессор
Бахтеев Андрей Владимирович
канд. экон. наук, доцент
ФГБОУ ВО «Ростовский государственный
экономический университет (РИНХ)»
г. Ростов-на-Дону, Ростовская область

СПОСОБЫ ОРГАНИЗАЦИИ АУДИТА ДЛЯ СНИЖЕНИЯ РИСКА МОШЕННИЧЕСТВА

***Аннотация**: в работе изучены типичные способы применения аудиторских процедур при мошенничестве для возможных вариантов организации аудита с учетом мошеннических действий. Рекомендуется использование упреждающего подхода для снижения риска мошенничества.*

***Ключевые слова**: индикаторы мошенничества, риск мошенничества, планирование аудита.*

Исследование выполнено при финансовой поддержке РГНФ. Проект «Риск фальсификации финансовой отчетности и его оценка в процессе внешнего аудита» №16–02–00035.

Обзор экономических преступлений в России, подготовленный PricewaterhouseCoopers, выявил, что большинство преступлений обнаруживаются службами внутреннего аудита и корпоративной безопасности (20 и 15% соответственно). При этом около 41% опрошенных отметили значительную угрозу мошенничества, причем, основным его видом является присвоение активов [2].

Аудиторы могут выявлять случаи мошенничества с помощью тестирования средств контроля, выявления присутствия индикаторов («красных флагов») или специально сформированной процедуры для поиска мошенничества. Возможны следующие варианты организации аудита с учетом мошенничества [5]:

– пассивный: аудитор определяет наличие контроля и готов к выявлению красных флагов мошенничества;

– реактивный: выполняется изучение конкретных фактов мошенничества и процедуры аудита сосредоточены на решении конкретных задач по фактам мошенничества;

– упреждающий или аудит мошенничества: происходит поиск мошенничества, когда нет никаких фактов, но слабость системы внутреннего контроля позволяет предположить, что мошенничество имеется.

В соответствии с ISA 240 – Международным стандартом аудита «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» [4], аудитор должен идентифицировать и оценить риск существенного искажения финансовой отчетности, в том числе искажения, допущенного преднамеренно, т.е. вследствие мошенничества. Кроме того, в соответствии с упомянутым, а также другими профессиональными аудиторскими стандартами (ISA 315 – «Выявление и оценка рисков существенного искажения посредством изучения организации и ее окружения», ISA 320 – «Аудиторские процедуры в ответ на оцененные риски») в обязанности аудитора входит принятие необходимых мер, позволяющих снизить идентифицированный и оцененный риск искажения до приемлемого уровня. Под ответными мерами в перечисленных профессиональных стандартах подразумеваются процедуры, позволяющие аудитору повысить уровень своей уверенности в достоверности или недостоверности проверяемой финансовой отчетности, и, как следствие, снизить информационный риск заинтересованных пользователей этой отчетности, в том числе и относительно ее преднамеренной фальсификации в результате мошеннических действий руководства.

При планировании аудита необходимо понимание того, насколько сложные схемы мошенничества могут быть использованы. Типичными способами реагирования на мошенничество являются [5]:

– не предпринимать никаких аудиторских мер в ответ на риск мошенничества;

– оценить риск мошенничества и идентифицировать элементы управления, которые соответствуют элементам оргструктуры для управления риском мошенничества;

– тестировать систему внутреннего контроля по красным флагам мошенничества;

– выполнить аудит бизнес-системы/финансовых счетов на предмет мошенничества;

– интегрировать процедуры аудита для обнаружения мошеннических операций в ядро бизнес-системы;

– расследование заявлений о мошенничестве.

План аудита при мошенничестве в отличие от традиционного предполагает, во-первых, создание неслучайной выборки, смещенной для поиска мошенничества, во-вторых создание аудиторских процедур для выявления схем мошенничества.

В первом случае подход пассивен и выявление мошеннических операций опирается на мониторинг системы внутреннего контроля, горячую линию организации, осведомленность руководства и т. п.

Во втором случае план аудита предполагает оценку рисков мошенничества, которые присущи бизнес-операциям. Разработаны соотнесенные с внутренним контролем сценарии возможного мошенничества. В этом случае вероятность мошенничества сведена к минимуму.

В рамках третьего подхода предполагается реактивная реакция на мошенничество путем проверки тех трансакций, которые обеспечивают определенную схему мошенничества. Красные флаги включаются в план аудита и позволяют протестировать наличие конкретных схем мошенничества.

В исследовании [1] выявлено 48 индикаторов мошенничества и каждому из них присвоен весовой коэффициент по степени риска. Наиболее высокий риск, в частности, имеют следующие красные флаги: 1) утеря или уничтожение документов и электронных файлов, содержащих ключевую информацию о сомнительных операциях; 2) отсутствие первичных подтверждающих документов;

3) стоимость личной собственности и образ жизни не соответствует доходам; 4) отсутствие наказаний за выявленные нарушения; 5) проведение сделок, по форме не соответствующих содержанию; 6) неупорядоченная система хранения товарно-материальных ценностей, документов, электронных файлов; 7) необоснованное сосредоточение ключевых полномочий; 8) противоречия в объяснениях персонала или замена объяснений; 9) внезапный отказ персонала от сотрудничества в рамках проверки; 10) права доступа для изменения архивных записей об операциях и файлов, и др.

В [5] приведены типы событий и шаблонов, и их возможные сочетания, которые по сути позволяют сконструировать соответствующие индикаторы мошенничества.

При четвертом подходе аудиторские процедуры применяются для совокупности бизнес-операций, чтобы увеличить вероятность выявления мошенничества. То есть используется упреждающий подход. Цель при проведении аудита мошенничества заключается в формировании суждения о существовании мошенничества. Отбор бизнес-операций осуществляется на основе интеллектуального анализа данных и согласуется с конкретными схемами мошенничества и коррелируют с профилем специфического изменения отчетности при соответствующей схеме мошенничества. В этом случае аудитор должен [5]:

1. Идентифицировать схему мошенничества.

2. Идентифицировать различные варианты схемы мошенничества.

3. Идентифицировать стратегии маскирования и связанные с ними красные флаги.

4. Идентифицировать возможности мошенничества.

5. Разработать сценарий мошенничества.

6. Построить профиль данных для схемы мошенничества.

7. С помощью методов анализа данных найти трансакции в соответствии с профилем данных.

8. Разработать процедуры аудита.

9. Рассмотреть достаточность, надежность и достоверность собранных доказательств.

10. Сформулировать вывод о мошенничестве.

Элементы перечисленного списка представляют собой непростые процедуры, обсуждение каждой из которых является отдельным направлением.

В пятом варианте ответа на мошенничество также упреждающим используется аудит мошенничества и предполагается, что имеются возможности распознавания мошеннических действий до их реализации.

В шестом варианте предполагается использование в том числе административных и уголовных процедур при реагировании на мошенничество.

В России возможность совершить мошенничество остается самым весомым фактором (84% респондентов в [2]), причем его значимость выросла на 8% в 2016 году по сравнению с 2014 годом. Наличие мотива и возможности скрыть/обосновать совершенное мошенничество по значимости одинаковы (8%). Таким образом, необходимо свести к минимуму имеющиеся «ниши» для совершения мошеннических действий путем применения механизмов выявления и предотвращения противоправных действий в рамках упреждающего подхода.

Список литературы

1. Мартынов С. Оценка рисков хищений как актуальное направление в безопасности бизнеса / С. Мартынов, А. Новиков. – М.: ACFE, 2013. – 23 с.

2. Оутен Дж. Российский обзор экономических преступлений за 2016 год / Дж. Оутен, И. Новикова, И. Фокина, И. Мушкет, А. Ульякин. – М.: PwC Россия, 2016. – 36 с.

3. Albrecht W.S. and C.O. Albrecht. Fraud Examination. Cengage Learning, 2011. – 696 p.

4. Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements. Vol. 1. New York: IFAC, 2013. – 926 p.

5. Vona I.W. Fraud Risk Assessment: Building a Fraud Audit Program. Hoboken, New Jersey: John Wiley and Sons, 2008. – 211 p.