



ACFESM

Association of Certified Fraud Examiners

RUSSIA

ИССЛЕДОВАНИЕ

EY

Building a better
working world

«ОЦЕНКА РИСКОВ ХИЩЕНИЙ КАК АКТУАЛЬНОЕ НАПРАВЛЕНИЕ В БЕЗОПАСНОСТИ БИЗНЕСА»

Москва 2013 год



Президент
российского отделения ACFE
Сергей Мартынов



Партнер в группе по расследованию
мошенничества и содействию в
спорных ситуациях компании
«Эрнст энд Янг» в СНГ
Андрей Новиков

В течение последних пяти лет российское отделение ACFE проводило большую работу по изучению и разработке различных методов оценки рисков хищений. В данном исследовании, которое проводилось при поддержке компании Эрнст энд Янг (СНГ) Б. В., была собрана ключевая информация, необходимая для практической реализации разработанного метода оценки рисков хищений.

Особо хочется отметить вклад в данное исследование аудиторско-консалтинговой компании Эрнст энд Янг (СНГ) Б. В., постоянного партнёра российского отделения ACFE на протяжении более чем пяти лет. Благодаря поддержке и участию нашего партнёра во всех наших мероприятиях были реализованы многие проекты, проведены тренинги, впервые в России создана профессиональная квалификация – профессионал по безопасности бизнеса.

Эффективная оценка рисков хищений на предприятиях представляет собой важную составную часть комплекса мер, направленных на противодействие мошенничеству.

Современным службам экономической безопасности предприятий следует не только расследовать последствия мошеннических действий, но и уметь предвидеть и предотвращать их, стремясь снизить экономические потери до возможно более низкого уровня.

Принимая во внимание важность предотвращения злоупотреблений и мошенничеств на самом раннем этапе их возникновения, российским отделением ACFE при поддержке компании Эрнст энд Янг (СНГ) Б.В. проведена значимая работа по формулировке и оценке весов индикаторов рисков хищений, а также разработан алгоритм их использования, позволяющий получать качественную оценку риска хищения в исследуемом предприятии или процессе.

Уникальность полученных результатов и их практическая важность определяются, прежде всего, тем, что они представляют собой продукт творчества и экспертного мнения профессионалов, работающих в сфере экономической безопасности в России и СНГ, и, следовательно, могут быть использованы в операционной деятельности предприятий.

СОДЕРЖАНИЕ

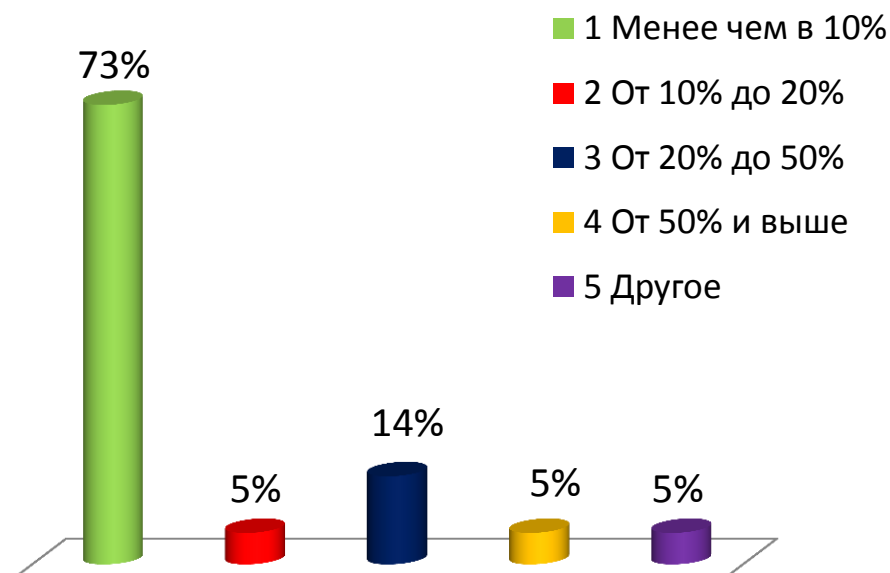
Введение	Стр. 4
Кто и как применяет оценки риска хищений?	Стр. 6
Методика оценки рисков хищений	Стр. 7
Организация проведения исследования. Перечень индикаторов хищений	Стр. 9
Применение индикаторов и вычисление итоговой оценки риска	Стр. 21
Обсуждение результатов	Стр. 22

ВВЕДЕНИЕ

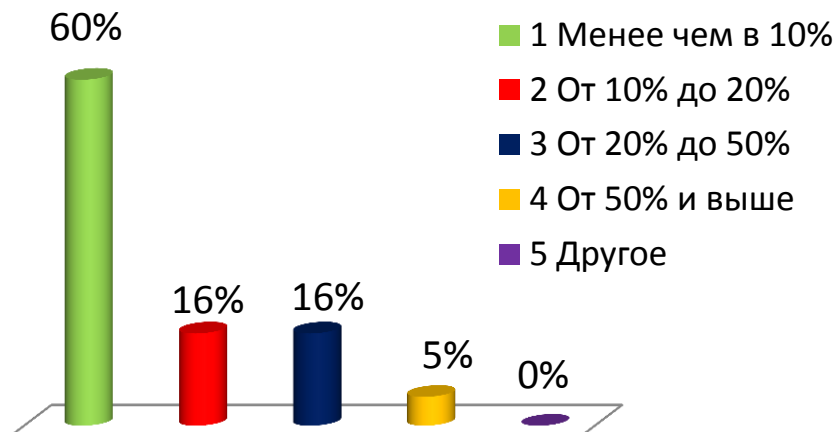
Любой бизнес заинтересован в снижении непроизводительных издержек и потерь, и, прежде всего, потерь от хищений в любых формах – мошенничества, растраты, коммерческого подкупа и других. Выявление уже состоявшихся преступлений, привлечение к ответственности виновных лиц и возмещение ущерба – необходимые функции системы безопасности бизнеса любой компании. Однако, наиболее эффективной является стратегия противодействия хищениям на наиболее ранней стадии, когда преступление ещё не состоялось, находится в начальной стадии, или потенциальный преступник только создаёт благоприятные условия для его совершения. В этом случае компания имеет возможность избежать затратных процессов уголовного преследования виновного сотрудника и возвращения похищенного, сохранить свою деловую репутацию в глазах инвесторов и общества. По результатам опроса экспертов российского отделения ACFE, 73% экспертов отметили, что обвинительный приговор суда был вынесен менее чем в 10% случаев проведённых внутренних расследований хищений; по опыту 60% экспертов, виновное лицо возместило нанесённый в результате хищения ущерб в менее чем 10% случаев. Ниже приведены результаты опроса одной из групп экспертов (по результатам опроса других групп

результаты примерно такие же)

В скольких случаях из ста проведенных расследований виновным был вынесен обвинительный приговор суда?



В скольких случаях из ста проведенных расследований виновный возместил причиненный ущерб?



Таким образом, выявление и предотвращение хищений на ранних стадиях позволяет повысить эффективность системы противодействия хищениям в компании в десятки раз.

Одним из способов ранней диагностики хищений является оценка рисков хищений. Она позволяет выявить потенциально опасные с точки зрения хищений и других непроизводительных потерь процессы, сделки и сотрудников. Именно в этих «чувствительных» точках можно предпринять упреждающие действия – установить дополнительные контрольные процедуры, снижающие возможность совершения хищений, провести ротацию или обучение персонала, или провести аудиторскую проверку с целью детального изучения ситуации.

Как и любой другой метод, данный подход к выявлению «узких» мест в системе внутреннего контроля имеет свои достоинства и недостатки, свою область применения.

К достоинствам подхода относятся низкие затраты (в десятки раз ниже, чем при проведении полноценного расследования), к недостаткам – получаемая оценка риска, как и любая другая оценка, не является доказательством факта хищения. На основании оценки риска нельзя выдвигать обвинения и получать доказательства, однако можно собрать необходимую информацию о точках, которые требуют повышенного внимания со стороны менеджмента и контрольных подразделений. Причиной высокой оценки риска хищений могут служить не только хищения, но и разные факторы, приводящие к непроизводительным потерям, например, халатность, саботаж или отсутствие у персонала необходимой квалификации. Тем не менее, если бизнес-процесс имеет высокую оценку риска хищений, то при отсутствии надлежащего контроля в нем имеются благоприятные условия для хищения.

Многие регуляторы (например, FRC – Financial Reporting Council, ведущий регулятор Великобритании в области аудита), в настоящее время уделяют особое внимание применению оценки риска хищений при оценке контрольных процедур (Audit Quality Thematic Review: Fraud risks and Law and Regulations, January 2014).

КТО И КАК ПРИМЕНЯЕТ ОЦЕНКИ РИСКА ХИЩЕНИЙ?

Перечислим несколько применений оценки рисков хищений в бизнесе.

Регулярная оценка рисков хищений в подразделениях и бизнес-процессах компании позволяет провести диагностику наиболее уязвимых для хищений активов и процессов. Менеджмент может использовать оценку рисков хищений для принятия управленческих решений по усилению системы внутреннего контроля, обучению персонала, принятию кадровых решений по противодействию хищениям. Контрольные подразделения (внутренний аудит, экономическая безопасность, контрольно-ревизионная служба) используют оценку рисков при формировании плана работы на год, выделяя больше ресурсов объектам аудита, имеющим высокие риски хищений. Таким образом реализуется риск-ориентированный подход к внутреннему аудиту.

При проведении внутренней аудиторской проверки оценка рисков хищений является обязательной составляющей частью набора аудиторских процедур. Не все контрольные процедуры разработаны с целью создания препятствий для хищений. Многие процедуры рассчитаны на добросовестных исполнителей и легко могут быть обойдены преступником. Поэтому оценка эффективности контрольных процедур в определённом процессе включает

в себя оценку риска хищений как составную часть общей оценки эффективности.

Оценка рисков хищений используется менеджментом и контрольными подразделениями компании при проведении внутренних расследований, в тех случаях, когда невозможно получить доказательства преступления. Законодательство (Закон РФ «Об оперативно-розыскной деятельности») накладывает строгие ограничения на использование в коммерческих компаниях методов, которые применяются при проведении расследования правоохранительными органами. Поэтому получение доказательств, формирующих состав преступления (например, доказательства умысла в случае мошенничества), оказывается невозможным. В этом случае внутреннее расследование заканчивается не возбуждением уголовного дела, а формированием вывода о величине риска хищения. Оценка риска может использоваться менеджментом для принятия управленческих решений по совершенствованию системы внутреннего контроля в данном бизнес-процессе или подразделении.

Сегодня система оценки рисков хищений является обязательным компонентом системы безопасности бизнеса любой крупной компании.

МЕТОДИКА ОЦЕНКИ РИСКОВ ХИЩЕНИЙ

В настоящее время известен ряд методов оценки рисков хищений. К сожалению, ни один из этих методов не стал широко применимым на практике, так как все они основываются на субъективной оценке степени риска аудитором. Это означает, что применяя одну и ту же методику к одному и тому же объекту исследования, разные аудиторы могут прийти к разным оценкам риска хищений, в зависимости от своего профессионального опыта и толерантности к риску. Поэтому задача создания методики оценки рисков, которая зависела бы от суждения аудитора в меньшей степени, остаётся актуальной.

Методика оценки рисков хищений, которая рассматривается в настоящем исследовании, основана на выявлении и оценке индикаторов хищений. Метод выявления скрываемого факта по его косвенным проявлениям (в нашем случае, «индикаторам») часто используется аналитиками в разных сферах деятельности, например, в аналитике и в разведке.

Индикатор хищения – это факт, который не скрывается или легко устанавливается и который обычно сопутствует хищению, но не является его прямым доказательством. По смыслу, индикатор близок к косвенному доказательству преступления, то есть к факту, который кроме криминального объяснения, может иметь

другие, некриминальные версии.

Например, образ жизни сотрудника, не соответствующий его доходам, является типичным индикатором хищения, однако не может быть доказательством, так как теоретически может существовать множество некриминальных объяснений того, откуда у данного сотрудника деньги (наследство, выигрыш в лотерею и т.д.).

Существует достаточно большое количество индикаторов, которые используются профессионалами на практике для выявления хищений.

Наличие одного и более индикаторов рисков хищений является для профессионала исходной информацией для углублённого изучения процесса на предмет наличия хищений. Наличие одновременно нескольких индикаторов свидетельствует о повышенном риске хищений.

Для получения количественной оценки рисков хищений на основе индикаторов необходимо решить следующие задачи:

- Сформировать набор индикаторов хищений, которые наиболее часто сопутствуют хищениям в коммерческих организациях. Очевидно, что выбор индикаторов должен быть основан на опыте

-
- профессионалов по расследованию хищений.
- Определить условный «вес» каждого индикатора. Дело в том, что индикаторы хищений по своему значению (степени связи именно с хищениями, а не с прочими некриминальными объяснениями), неравноценны. Одни индикаторы могут иметь больший вес, то есть их присутствие говорит о высоком риске хищений; другие индикаторы не всегда сопутствуют хищению, так как могут быть вызваны другими причинами. Насколько один индикатор весомее других? Очевидно, что наиболее объективной будет оценка экспертов.
 - Разработать алгоритм вычисления итоговой оценки риска на основе известных значений индикаторов риска и их весов.

ОРГАНИЗАЦИЯ ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ

В проведённом исследовании при решении перечисленных выше задач мы полагались на опыт профессионалов, работающих в России и странах СНГ, которые принимали участие в тренингах, встречах и конференциях российского отделения ACFE и Эрнст энд Янг (СНГ) Б. В. в 2013 году. В целом, в проведении исследования участвовало более чем 500 профессионалов, работающих в области расследований, внутреннего аудита, риск менеджмента и других областях обеспечения безопасности бизнеса. У нас есть все основания считать состав экспертов достаточно компетентным: участники наших мероприятий являются профессионалами в различных сферах безопасности бизнеса и проведения расследований, и имеют многолетний опыт работы.

При проведении экспертной оценки необходимо учитывать ряд факторов, влияющих на качество получаемых результатов:

- Эксперты должны быть независимыми. Они не должны быть заинтересованы в получении определённых результатов – положительных или отрицательных.
- Эксперты должны быть профессионалами и иметь практический опыт работы в данной области.
- Мы должны обеспечить экспертам возможность полной анонимности для получения их

действительного мнения, а не «желаемых» ответов.

При проведении данного исследования мы учитывали перечисленные ниже факторы:

- ✓ Во-первых, в исследованиях принимали участие профессионалы, которые посещали мероприятия ACFE и «Эрнст энд Янг (СНГ) Б. В.».
- ✓ Во-вторых, вопросы составлены таким образом, что не могут быть привязаны к какой-то конкретной организации. Например, вместо вопроса «сколько ваша организация потеряла от хищений в прошлом году» предлагается вопрос «по вашему мнению, какой уровень потерь от хищений существует в российских компаниях».
- ✓ В третьих, для обеспечения анонимности экспертов мы использовали технологии очного интерактивного голосования фирмы Turningpoint. Они позволяют в формате презентации PowerPoint показывать на экране вопрос, а затем участникам опроса высказывать своё мнение с помощью индивидуальных пультов, нажимая соответствующую выбранному ответу кнопку. Перед началом голосования участники выбирали пульты из общей корзины случайным образом, и, таким образом, не существовало возможности их идентифицировать.

В процессе исследования проводились опросы нескольких групп экспертов, включающих от 30 до 100 человек. Результаты каждой сессии обрабатывались с использованием профессионального статистического программного обеспечения, затем результаты разных групп объединялись и усреднялись.

Основной задачей, которая решалась в каждой сессии, было обсуждение списка индикаторов и их формулировок, и затем определение весов различных индикаторов риска. Интересно, что опрос в разных, независимых друг от друга группах показал, что имеется высокая корреляция между оценками разными группами одних и тех же индикаторов риска. Например, пять первых и пять последних по значимости мест во всех группах заняли одни и те же индикаторы.

Для каждого из индикаторов была получена средняя оценка по ординарной шкале от 1 до 5, где 1 означает, что индикатор слабо связан с риском хищения, а 5 - что индикатор вполне определён (очень часто) сопутствует хищению.

Далее приведён перечень индикаторов хищений (за исключением тех, которые по мнению экспертов, были признаны несущественными - эти индикаторы были исключены из списка).

Индикатор 1. Нестабильность и кризисные явления.

Влияние кризисных явлений на уровень хищений в компании. К кризисным явлениям относятся: предстоящие реорганизации и сокращения, смена менеджмента – все, что создаёт у сотрудников ощущение нестабильности и неуверенности в завтрашнем дне.

Индикатор 2. Вид бизнес-процесса.

Влияние типа бизнес-процесса на уровень хищений в нем. К традиционно высокорисковым для хищений процессам относятся закупки, капитальное строительство, инвестиции.

Индикатор 3. Периодичность оценки.

Влияние на уровень хищений частоты проверок и оценки рисков хищений в подразделении (предприятии): насколько часто контролирующие службы проводят аудиторские, ревизионные проверки на предприятии – например, раз в год или раз в три года.

Индикатор 4. Низкий уровень корпоративной культуры.

Влияние на уровень хищений степени развитости корпоративной культуры в компании. Высокая корпоративная культура, приверженность персонала целям и ценностям компании является одним из факторов, снижающих уровень хищений.

Индикатор 5. Объем материальных ценностей в обороте.

Чем больше в обороте подразделения или бизнес-процесса материальных ценностей (денег, товаров и т.д.), тем выше риск хищений.

Индикатор 6. Наличие программы по противодействию хищениям.

Влияние на уровень хищений наличия в компании эффективно работающей программы по противодействию хищениям.

Индикатор 7. Уровень развития контрольных процедур.

Влияние на уровень хищений уровня развития контрольных процедур в компании. Чем больше внимания компания уделяет развитию и совершенствованию системы контрольных процедур, тем, в общем случае, ниже риск хищений.

Индикатор 8. Нарушение установленного порядка исполнения операций, объясняемое благими целями, если в результате нарушения создаются благоприятные условия для хищения.

Такая ситуация создаётся, когда контрольная процедура нарушается персоналом, но прямые доказательства хищения отсутствуют, но из-за нарушения КП были созданы благоприятные условия для хищения.

Индикатор 9. Некриминальные объяснения нанесённого ущерба, если проверка объяснений невозможна.

Факт нанесения ущерба компании обнаружен, ответственное лицо предоставляет некриминальные объяснения причины ущерба (стихийные бедствия, происки конкурентов и т.д.), однако проверка правдивости этих объяснений невозможна.

10. Противоречия в объяснениях или смена одних объяснений другими.

Многочисленные изменения объяснений причин ущерба или нарушений в ходе проведения проверки или расследования ответственным лицом.

11. Отсутствие первичных подтверждающих документов.

При проведении проверки (расследования) выяснилось отсутствие первичных подтверждающих документов.

12. Утеря или уничтожение документов и электронных файлов, содержащих ключевую информацию о сомнительных операциях.

При проведении проверки (расследования) выяснилось, что ключевые документы или файлы отсутствуют – утеряны (например, вследствие сбоя в компьютерной системе) или уничтожены (по любым основаниям).

13. У операционного персонала существуют права доступа для изменения архивных файлов и записей о проведённых операциях.

Персонал, ответственный за проведение и учёт операции имеет права изменения данных об операциях за прошлый период (например, бухгалтер, работающий с программой 1С, имеет права редактировать данные за прошедшие периоды или задним числом менять какую-то информацию).

14. Необоснованные задержки в предоставлении запрошенной документации и доступа к электронным файлам.

При проведении проверки возникают необоснованные реальными обстоятельствами задержки в предоставлении документов и доступа к информационным системам.

15. Даты модификации файлов не соответствуют дате, когда они должны быть созданы.

Например, файл, который был создан год назад, имеет вчерашнюю дату модификации.

16. Производные таблицы не подтверждаются первичными документами.

Расхождения между первичными и производными документами.

17. Наличие копий документов вместо оригиналов.

Копии документов первичных документов, например, счетов, счетов-фактур и т.д.

18. Неспособность менеджмента продемонстрировать заинтересованность в установлении соответствующего уровня контроля.

Как правило, в таких случаях менеджмент заявляет, что противодействие хищениям – это работа службы безопасности, внутреннего аудита и т.д.

19. Высокая текучесть кадров на уровне руководства/высшего менеджмента.

Частая сменяемость высшего менеджмента на ключевых позициях (директор, финансовый директор и т.д.).

20. Поведение менеджмента, демонстрирующее доминирование над внутренним аудитом и другими контрольными службами.

Типичные заявления: мы тут работаем, а вы (проверяющие) только мешаете.

21. Ограничения в доступе проверяющих к персоналу организации.

В частности, требование направлять все запросы и получать информацию только от руководителя подразделения, запрет проведения интервью с исполнителями.

22. Проведение сделок, по форме не соответствующих содержанию.

Например, заключается фиктивный договор на оказание аутсорсинговых услуг по предоставлению персонала, для компенсации якобы дополнительных расходов подрядчика.

23. Чрезмерно высокие ожидаемые ключевые показатели работы менеджеров.

Когда ключевые показатели эффективности работы менеджмента нереальны для исполнения в существующих условиях.

24. Менеджмент демонстрирует недостаточное внимание к этическим ценностям, недостаток коммуникаций с сотрудниками по вопросам этики, недостаточно агрессивное отношение к проблеме хищений.

25. Менеджмент демонстрирует повышенную склонность к риску, нежелание оценивать риски.

Типичный аргумент менеджера в таком случае: я принимаю решение и сам оцениваю риски, мне не нужен независимый и формализованный риск-менеджмент.

26. Недостаточный уровень автоматизированного контроля операций.

Необоснованный отказ от внедрения повсеместно принятых средств автоматизированного учёта операций,

например, ручное ведение бухгалтерского учёта, в то время как обычно в этих случаях используется программа 1С.

27. Большое расхождение между бюджетными и фактическими данными.

Данные фактического исполнения бюджета значительно (более чем на 15-20%) отличаются от первоначально утвержденного бюджета.

28. Неудовлетворённость персонала уровнем заработной платы.

Если персонал предприятия (отдела) выражает недовольство уровнем оплаты труда и использует это как объяснение (самооправдание) невыполнения контрольных процедур или халатности.

29. Низкая лояльность персонала.

Низкая лояльность персонала задачам и целям компании, отношение к компании как к временному месту работы, где интересы компании и сотрудников противоположны.

30. Создание обособленных групп персонала менеджером.

Создание неформальных групп «особо доверенных» или «приближенных» к менеджеру сотрудников, которые обладают большой властью не в соответствии с организационной структурой компании, а в силу неформальных отношений с руководителем.

31. Беспорядочная система хранения ТМЦ, документов и электронных файлов.

Отсутствие формально или неформально установленной системы хранения документов и файлов, невозможность найти документы и файлы без помощи конкретного сотрудника.

32. Удалённость производства от топ-менеджмента и контролирующих служб.

Географическая удалённость места проведения хозяйственной деятельности (производственных процессов) от высшего менеджмента и контролирующих подразделений.

33. Избирательный подход к выполнению контрольных процедур.

Отдельные контрольные процедуры не выполняются без обоснованных причин.

34. Стоимость личной собственности и образ жизни не соответствует доходам.

Расходы сотрудника значительно превышают его официально декларированные доходы.

35. Внезапный отказ персонала от сотрудничества в процессе проверки.

В процессе проведения проверки происходит внезапный отказ ранее хорошо сотрудничавших с группой проверки сотрудников от дальнейшего сотрудничества, отношение

меняется на недоброжелательное, начинают происходить задержки и отказы в предоставлении информации.

36. Отсутствие системы анонимного информирования («горячей линии») в компании.

Отсутствие в компании «горячей линии» для приёма анонимных сообщений сотрудников о злоупотреблениях, отсутствия должной осведомленности сотрудников о результатах работы «горячей линии», отсутствие доверия сотрудников к желанию руководства компании рассматривать сообщения по существу.

37. Необоснованное невыполнение рекомендаций по устранению недостатков.

Менеджмент необоснованно не выполняет рекомендации и не предпринимает мер по устранению выявленных недостатков в организации системы внутреннего контроля.

38. Длительная работа сотрудника на ключевой позиции без отпусков.

Длительная работа сотрудника на одной должности без отпусков и больничных, без временных замен другими сотрудниками.

39. Отсутствие наказаний за выявленные нарушения.

Виновные в нарушениях сотрудники не наказываются или наказываются формально (степень наказания не соответствует нанесённому компании ущербу).

40. Необоснованное чрезмерное сосредоточение ключевых полномочий.

Все ключевые полномочия в бизнес-процессе сосредоточены у одного менеджера, необоснованно избегается делегирование полномочий.

41. Использование расчётных показателей при наличии автоматизированных учётных систем.

При наличии автоматизированных учётных систем их возможности не используются, либо они часто выходят из строя.

42. Определение расхода сырья обратным счётом.

Объём сырья и материалов, израсходованного на производство продукции, определяется расчётным способом от объёма выпущенной продукции, а не на основании замера фактически израсходованного объёма.

43. Значительные корректировки отчётности и бюджетов.

В течение отчётного периода осуществляются значительные корректировки отчётности (бюджетов).

44. Чрезмерное волнение и неадекватное поведение при общении в процессе проверки.

Типичные вербальные и невербальные признаки неадекватного волнения - слезы, истерики, гнев и т.д.

45. Наличие персональных факторов давления (кредиты, зависимости и т.д.)

Зависимость от наркотических средств, алкоголизм, игровая зависимость, наличие близких родственников связей с людьми, ведущими асоциальный образ жизни, потребность в дорогостоящем лечении, привычка к расточительному образу жизни.

46. Отсутствие системы КПЭ у менеджмента.

Отсутствие ключевых показателей эффективности у менеджмента.

47. Отсутствие системы разделения прав и полномочий.

В контрольных процедурах отсутствует разделение полномочий по принятию решений и учёту результатов операций, оценке рисков.

48. Отключение предусмотренных возможностей контроля в автоматизированных системах.

По разным причинам контрольно-измерительные приборы и средства автоматизации отключаются и не фиксируют результаты операций. Например, автомобильные весы сломаны большую часть времени, или файлы с записями результатов ежедневно уничтожаются.

Примечания.

- По каждому из индикаторов могут быть приведены более подробные описания и примеры - это целесообразно сделать при разработке методики оценки риска хищений в рамках конкретной компании, чтобы учитывать особенности бизнеса.

- Каждая компания имеет свой уровень толерантности к риску хищений, в связи с этим оценка величины каждого из индикаторов должна осуществляться применительно к конкретной компании и направлениям бизнеса. В нашем исследовании приводятся оценки, которые представляют собой усреднённые оценки всех участвовавших в исследовании экспертов.

- Все индикаторы могут быть разделены на несколько групп, например: поведенческие (которые описывают поведение сотрудников компании в процессе проведения проверки и вне её), организационные (как организованы контрольные процедуры и процессы), документарные (содержание и наличие документов и информации об операциях), исходно присущие данному виду бизнес-процесса и так далее.

Ниже приведена таблица результатов оценки весов индикаторов риска, полученных в результате настоящего исследования.

12. Утеря или уничтожение документов и электронных файлов, содержащих ключевую информацию об сомнительных операциях	5,42
11. Отсутствие первичных подтверждающих документов	5,03
34. Стоимость личной собственности и образ жизни не соответствует доходам	4,79
39. Отсутствие наказаний за выявленные нарушения	4,71
22. Проведение сделок, по форме не соответствующих содержанию	4,69
31. Беспорядочная система хранения ТМЦ, документов и электронных файлов	4,69
40. Необоснованное чрезмерное сосредоточение ключевых полномочий	4,67
10. Противоречия в объяснениях или смена одних объяснений другими	4,63
35. Внезапный отказ персонала от сотрудничества в процессе проверки	4,60
13. Права доступа для изменения архивных файлов и записей о проведенных операциях	4,58
21. Ограничения в доступе проверяющих к персоналу организации	4,48

7. Уровень развития контрольных процедур: влияет ли на уровень хищений уровень развития контрольных процедур, и насколько	4,47
30. Создание обособленных групп персонала менеджером	4,43
42. Определение расхода сырья обратным счетом	4,43
16. Производные таблицы не подтверждаются первичными документами	4,40
26. Недостаточный уровень автоматизированного контроля операций	4,37
28. Неудовлетворенность персонала уровнем заработной платы	4,37
8. Нарушение установленного порядка исполнения операций, объясняемое благими целями, если в результате нарушения создаются благоприятные условия для хищения	4,36
5. Объем материальных ценностей в обороте: влияет ли на уровень хищений объем материальных ценностей в обороте подразделения (в процессе, проекте и т.д.), и насколько	4,33
48. Отключение предусмотренных возможностей контроля в автоматизированных системах	4,31
41. Использование расчетных показателей при наличии автоматизированных учетных систем	4,29
6. Наличие программы по противодействию хищениям: влияет ли на уровень хищений наличие программы по противодействию хищениям, и насколько	4,26
32. Удаленность производства от топ-менеджмента и контролирующих служб	4,26

45. Наличие персональных факторов давления (кредиты, зависимости и т.д.)	4,19
47. Отсутствие системы разделения прав и полномочий	4,18
19. Высокая текучесть высшего менеджмента	4,17
15. Даты модификации файлов не соответствуют дате, когда они должны быть созданы	4,17
29. Низкая лояльность персонала	4,13
14. Необоснованные задержки в предоставлении запрошенной документации и доступа к электронным файлам	4,11
20. Поведение, демонстрирующее доминирование менеджмента над внутренним аудитом и другими контрольными службами	4,11
33. Избирательный подход к выполнению контролей	4,10
23. Высокие ожидаемые ключевые показатели менеджеров, нереальные для исполнения	4,01
24. Менеджмент демонстрирует недостаточное внимание к этическим ценностям, недостаток коммуникаций с сотрудниками по вопросам этики, недостаточно агрессивное отношение к проблеме хищений	3,98
43. Крупные корректировки отчетности и бюджетов	3,96
27. Большое расхождение между бюджетными и фактическими данными	3,96
9. Некриминальные объяснения нанесенного ущерба, если проверка объяснений невозможна	3,95

37. Необоснованное невыполнение рекомендаций по устранению недостатков	3,87
18. Неспособность продемонстрировать заинтересованность в установлении соответствующего уровня контроля	3,86
17. Наличие копий документов вместо оригиналов	3,85
38. Длительная работа сотрудника на ключевой позиции без отпусков	3,79
2. Вид бизнес-процесса: влияет ли вид бизнес-процесса на уровень хищений в нем, и насколько	3,75
1. Нестабильность и кризисные явления: влияние кризисных явлений на уровень хищений в компании. К кризисным явлениям относятся: предстоящие реорганизации и сокращения, смена менеджмента – все, что создает у сотрудников ощущение нестабильности и не уверенности в завтрашнем дне	3,59
44. Чрезмерное волнение и неадекватное поведение при общении в процессе проверки	3,53
3. Периодичность оценки: влияет ли на уровень хищений частота проверок и оценки рисков хищений в подразделении (предприятии), и насколько	3,46
36. Отсутствие системы анонимного информирования в компании	3,32
25. Менеджмент демонстрирует повышенную склонность к риску, нежелание оценивать риски	3,27
46. Отсутствие системы КПЭ	2,88
4. Уровень корпоративной культуры: влияет ли на уровень хищений уровень корпоративной культуры, и насколько	2,68

ПРИМЕНЕНИЕ ИНДИКАТОРОВ И ВЫЧИСЛЕНИЕ ИТОГОВОЙ ОЦЕНКИ РИСКА

Для получения итоговой оценки риска необходим алгоритм, который позволит в каждом конкретном случае на основании найденных индикаторов получать результирующую оценку, отражающую суммарный уровень величины риска хищений в исследуемом процессе (подразделении, сделке, т.д.).

При разработке этого алгоритма мы предлагаем опираться на некоторые эмпирически установленные зависимости. Во-первых, это правило кластеризации, которое существует во многих технологиях выявления скрываемой информации. Оно заключается в том, что однократное появление одного индикатора (в нашем случае, индикатора риска), не является существенным признаком наличия ожидаемого результата. Например, при исследовании с помощью полиграфа (выявление лжи), значимыми считаются многократные проявления реакции на одни и те же вопросы. Точно также, при проведении интервью, определёнными признаками лжи считаются проявления вербальных и невербальных признаков лжи одновременно. В криминалистике, наличие комплекса (а не одного) косвенных доказательств является вполне определённым доказательством преступления.

В случае оценки риска на основе индикаторов

хищений, мы считаем обоснованным использовать правило «трех сигналов». Оно заключается в том, что трех независимых «желтых» (по уровню опасности) сигналов достаточно, чтобы считать риск высоким. «Желтыми сигналами» в нашем случае являются индикаторы хищений. Таким образом, наличие трех и более индикаторов, относящихся к разным группам, достаточно для оценки риска хищений как высокого.

Второй подход, который может использоваться в тех случаях, когда необходима количественная оценка уровня риска – например, при сравнении уровня рисков в нескольких бизнес-процессах, для выбора наиболее рискованного для проверки, является использование логарифмической зависимости. Эмпирически наиболее подходящей математической моделью является функция, использующая логарифм от количества найденных индикаторов и сумму весов всех найденных индикаторов риска. Подробное обоснование конкретной формулы является темой отдельного исследования.

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Представленные результаты – это уникальный экспертный опыт большого количества профессионалов, работающих в сфере безопасности бизнеса в России и СНГ. Безусловно, это масштабное исследование стало возможным только при поддержке компании Эрнст энд Янг (СНГ) Б. В.. Было собрано огромное количество информации, из которого в настоящем обзоре представлена лишь небольшая часть. Например, интересно проанализировать девиацию распределения ответов экспертов на вопросы исследования. Первый взгляд позволяет сделать вывод, что в оценке документарных и организационных индикаторов хищений эксперты более единодушны, чем в отношении к вербальным и поведенческим индикаторам. Интересно расхождение в оценке разными группами экспертов одних и тех же индикаторов. Возможно, оно было вызвано разными видами бизнеса, разной корпоративной культурой. Мы также отметили разницу между результатами, когда группа экспертов состояла из сотрудников одной компании, и оценками сборной группы экспертов. Все эти результаты должны быть проанализированы, также как должно получить развитие система классификации индикаторов и алгоритм вычисления итоговой оценки риска.

Представленные в нашем исследовании результаты могут быть использованы при разработке собственной методики оценки риска хищений любой компанией. Мы надеемся, что профессиональное сообщество примет активное участие в дальнейшем развитии методики оценки риска на основе данного подхода.

На основе результатов исследования нами был разработан программный продукт для оценки рисков хищений, который ориентирован на применение менеджментом и контрольными подразделениями. В настоящее время мы проводим опытную эксплуатацию программы и приглашаем к участию в тестировании всех профессионалов.



Президент
российского отделения ACFE
Сергей Мартынов

www.acfe-rus.org

Тел.: +7 (495) 728-76-10

info@acfe-rus.org



Партнер в группе по
расследованию
мошенничества и содействию
в спорных ситуациях компании
«Эрнст энд Янг» в СНГ
Андрей Новиков

www.ey.com.ru

Тел.: +7 (495) 648-9618

Andrey.Novikov@ru.ey.com