Быстрые победы в управлении рисками мошенничества

Василий Кудрин, CFE, CIA, CCSA

10 сентября 2010 г.

Содержание

- **Природа мошенничества, влияние на «вселенную» рисков компании**
- **Типовые универсальные инструменты противодействия мошенничеству**
- **Пути повышения продуктивности «горячих линий»**
- **Аудит vs. Расследования: эффективный баланс**

Определение и природа мошенничества

- **Мошенничество (Fraud)** – это «использование служебного положения для целей ***личного*** обогащения путем ненадлежащего использования или воровства собственности или ресурсов организации».

  Источник: Association of Certified Fraud Examiners (ACFE)

- **Мошенничество, Fraud** (ISA 240) – это «***преднамеренное*** действие, совершаемое одним лицом или группой лиц (руководящим звеном, работниками или третьей стороной), целью которого является незаслуженное и неправомерное получение выгоды путем обмана».

- Намерения – производное ***внутренней культуры*** и ***воспитания*** личности. Это самые важные конечные факторы мошенничества.

- Это понимание есть основа для построения модели кадровой безопасности, а также общей модели управления рисками мошенничества.

Ожидания – Управление рисками мошенничества

Линейные менеджеры | **Высшее руководство** | **Совет директоров**

- Повышение ***контрольной дисциплины*** (бдительности) со стороны менеджеров и исполнителей
- ***Защита от*** мошенничества со стороны ***недобросовестных*** менеджеров и персонала
- Процедуры противодействия мошенничеству ***органично*** вписываются в бизнес-процессы и осознаются как необходимые и полезные менеджерами и исполнителями
- Быстрое ***принятие решений*** и эффективная ***координация*** со смежными подразделениями вследствие отсутствия конфликтов интересов
- «Сложные случаи» быстро и эффективно ***расследуются***

- ***Улучшения*** СВК на уровне основных процессов и ниже гарантируются
- Повышение эффективности «горячей линии» и прочих каналов ***информирования***
- ***Риски*** мошенничества осознаются и предпринимаются действия по ***управлению*** ими, повышение эффективности и управленческих решений
- Эффективный ***информационный обмен и коммуникация*** между подразделениями, создание атмосферы доверия
- Имеется эффективный механизм отслеживания качества и постоянного ***совершенствования*** системы управления рисками мошенничества

- Руководством демонстрируется должный ***«тон сверху»*** в отношении ***неприятия мошенничества*** и неэтичного поведения, улучшение в целом контрольной среды
- Обеспечение (финансовой) ***прозрачности*** компании
- Полное понимание, раскрытие и обсуждение ***ключевых рисков*** компании, понимание и обсуждение факторов
- Руководство реализует наиболее ***приоритетные улучшения*** в системе противодействия мошенничеству (anti-fraud программа)
- Единые и прозрачные ***протоколы*** выявления и расследования случаев мошенничества

Зоны «быстрых побед» в модели управления рисками мошенничества

- Компоненты защиты (обороны) против рисков мошенничества

Внутренняя Среда (Этика)	Система внутреннего контроля (СВК)	Мониторинг СВК	Whistleblowing («информирование»)	Расследования
Ценности Компании Тон со стороны Совета директоров и высшего руководства Этические нормы Кодекс корпоративных правил Система внедрения и поддержания Кодекса корпоративных правил и этических норм	Оценка рисков хищений / мошенничества на уровне мега-процессов и ниже Система процедур и механизмов предотвращения мошенничества Ответственность Нормы и правила Контрольные процедуры Регулярные проверки по сигналам (признакам) HR	Мониторинг СВК на уровне владельцев бизнес-процессов Мониторинг СВК со стороны вспомогательных функций Мониторинг (диагностика) СВК со стороны Дирекции по безопасности Отдел внутреннего аудита Мониторинг IT-систем и IT-мониторинг	Внедрение «горячих» линий Вопросы подотчетности и обеспечение защиты «горячих» линий Защита информаторов и фильтрация сигналов Система инициирования действий по сигналам «горячих» линий	Исследование менеджментом (инцидентов) Расследования на уровне Дирекции по безопасности (подотчетной CEO) Отдел внутренних расследований Координация IT-расследования Отчетность и информирование

Общекорпоративные универсальные средства: «быстрые победы» и «следующие шаги»

«Быстрые победы»:

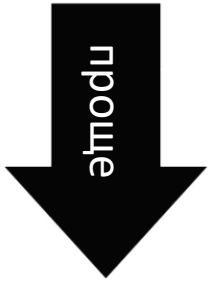
- Кодекс этики
- Запуск «горячей линии» по этическим вопросам
- Практика независимых расследований
- Специальные интервью при увольнении сотрудников
- Система проактивных опросов сотрудников
- «Введение» при приеме на работу
- Оценка рисков мошенничества

«Следующие шаги»:

- Эффективная координация между разными службами
- Единые протоколы расследований
- Формирование практики аудита (диагностики) внутреннего контроля над рисками мошенничества

Оценка рисков мошенничества: 2 варианта

Формирование представления относительно (риска) мошенничестве



- **Скоординированная оценка присущих рисков общекорпоративного уровня**
- **Рассмотрение фактора мошенничества при оценке каждого риска (“возможность”, “мотивация”, “давление”)**

- **Отражение, или проявление риска в процессах или специальных проектах - «мэппинг» рисков на процессы/проекты**
- **Уровень отражаемости риска - «высокий», «средний», «низкий»**
- **Насыщенность процессов/проектов рисковыми событиями**
- **Организационная сложность процессов/проектов: «внутренняя сложность» и «объемность»**
- **Учет эффективности универсальных средств противодействия мошенничеству**

- ➔ ***Подготовительная работа (подготовка типовой карты рисков, предварительные интервью, подтверждение описаний рисков)***
- ➔ ***Вступительная презентация и вспомогательные раздаточные материалы***
- ➔ ***Голосование с дальнейшим обсуждением***
- ➔ ***Ориентирование на мнения экспертов***
- ➔ ***Рассылка материалов и подтверждающие интервью***

ПЕРЕХОД НА СЛЕДУЮЩИЙ УРОВЕНЬ

Использование полиграфа

В 2003 году Национальная академия наук США опубликовала отчёт «Полиграф и выявление лжи».

Академия наук обнаружила, что большинство исследований полиграфа было «ненадёжно, ненаучно и предвзято». После проведения экспериментов было установлено, что проверка на полиграфе большого количества людей в отношении различных событий (например, при приёме на работу) даёт результат ***ничем не лучше, чем случайное угадывание***.

В то же время тестирование небольшого количества людей в отношении определённого произошедшего события (например, конкретного преступления) позволяет распознать ложь и правду «***на уровне немного выше, чем случайное угадывание***».

Фактор «ошибки» методов с использованием полиграфа:

Предубеждение испытуемого — реакции организма отражают не истинность фактов, а всего лишь веру испытуемого в их истинность или ложность. Испытуемый может думать, что его знание правдиво, хотя на самом деле ему оно было внушено или навязано.

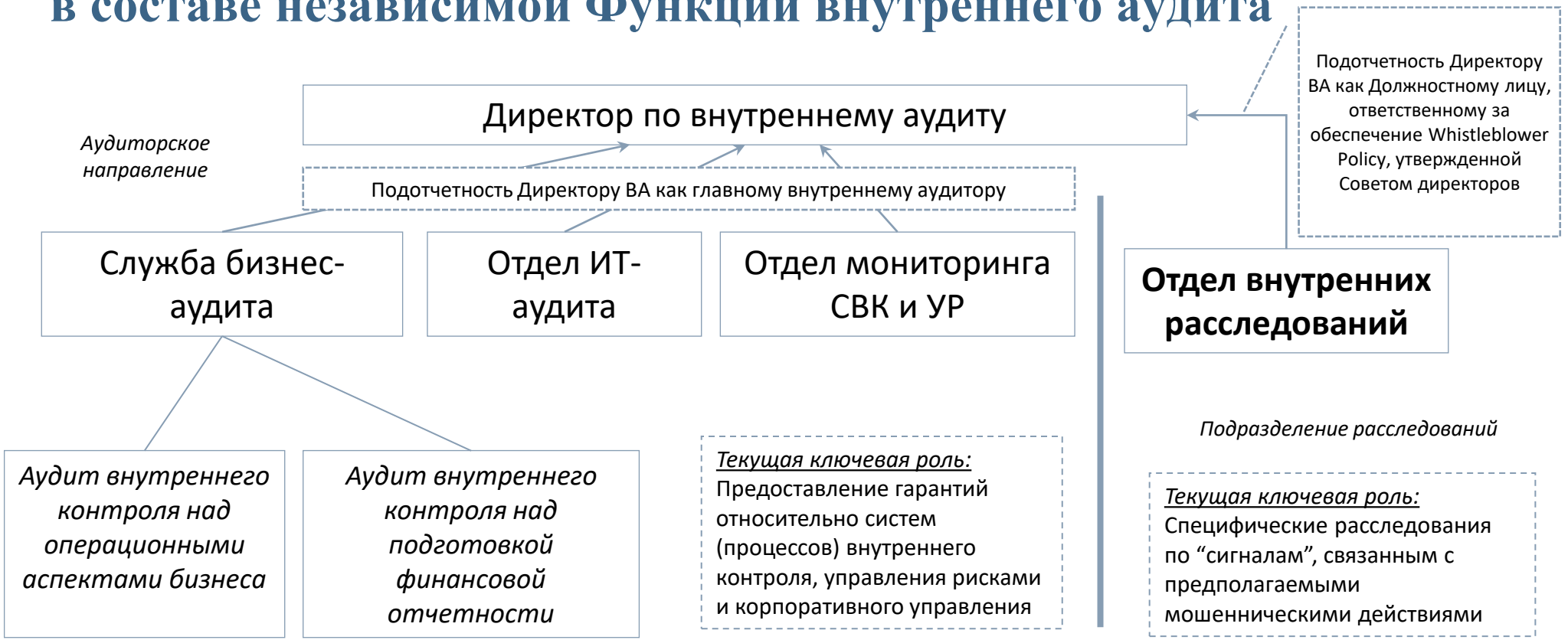
Повышение эффективности «горячей линии»

- Простые, понятные «каналы» и коммуникации
- Кадровое ресурсообеспечение «горячей линии»
- Гарантия независимости
- Кампания (план) информирования о «горячей линии»
- Постоянная программа совершенствования

Роли внутреннего аудита в вопросах борьбы с мошенничеством

- Оценка систем защиты от мошенничества – КЛЮЧЕВАЯ
- Оценка рисков мошенничества – КЛЮЧЕВАЯ
- Выявление признаков мошенничества – КЛЮЧЕВАЯ
- Обслуживание «горячей линии» – СООТВЕТСТВУЮЩАЯ
- Выявление (detection) случаев мошенничества – ВОЗМОЖНАЯ
- Расследование (investigation) случаев мошенничества – ВОЗМОЖНАЯ
- Сообщение о результатах мошенничества – ВОЗМОЖНАЯ
- Участие в принятии решений по результатам расследований – ЗАПРЕТНАЯ
- Внедрение (по поручению менеджмента) «механизмов» защиты от мошенничества – ЗАПРЕТНАЯ

Пример: место подразделения внутренних расследований в составе независимой Функции внутреннего аудита

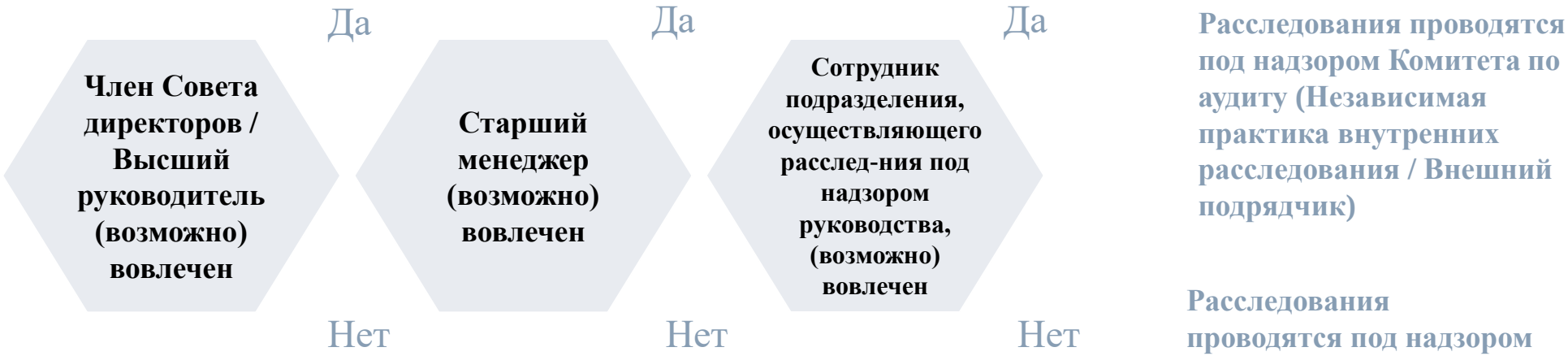


Отношение ко времени / Тип нарушения	**В будущее – “Перспектива” * Событие (Риск) может случиться**	**В прошлое – “Ретроспектива” * (Негативное) событие случилось**
Ошибка (нет намерения)	Внутренний аудит	*Нет постоянной роли у ДВА*
Мошенничество (есть намерение)	Внутренний аудит	Расследования мошенничества

Внутренний аудит vs. Расследования

Объект сравнения	**Внутренний аудит (в отношении к рискам и системам противодействия мошенничеству)**	**Расследования мошенничества**
«Сигнал»	Специфический «сигнал» как таковой отсутствует	Имеется «сигнал»: жалоба, (обоснованное) заявленное подозрение кого-либо и т.п.
Предмет	Выявление индикаторов мошенничества	Собрать доказательства или опровергнуть «сигнал»
Подход	Оценка рисков мошенничества и выявление индикаторов мошенничества	Расследование специфического случая
Фокус	Понимание причин, почему случай мошенничества произошел/может произойти, определение недостатков в системе внутреннего контроля	Анализ, интерпретация и представление наблюдений как, как если бы они рассматривались в суде
Компетенции	Навыки и знания о том, как схемы мошенничества могут реализоваться и каковы ключевые индикаторы схем мошенничества. Понимание, когда необходимо расследование.	Навыки и знания о том, как проводить расследования

Координация практик выявления и расследования мошенничества (бизнес-кейс)



Решения:

- **Ни одно расследование не может быть назначено кому-либо, не обладающему необходимыми компетенциями (т.е., в частности, кому-либо, кроме специалистов особого независимого подразделения расследований мошенничества, специалистов службы безопасности или компетентных специалистов соответствующего внешнего подрядчика).**
- **Методология проведения расследований должна быть единой и согласованной с протоколами, одобренными Советом директоров.**
- **Роль внутренних аудиторов может состоять в оценке эффективности процедур расследований и их соответствия данным протоколам и единой методологии. В целом внутренние аудиторы могут быть вовлечены в расследование только после согласования этого вопроса с Главным аудитором, и только в качестве вспомогательных кадровых ресурсов.**
- **Главный аудитор должен быть информирован о всех существенных отчетах по результатам расследований.**

Пример: статистика *квалифицированных* «сигналов» и предпринятые действия

Примерная статистика распределения *квалифицированных* «сигналов» о (возможных) мошеннических действиях между подразделением (отделом), осуществляющим *независимые внутренние расследования* (НВР) и другим(и) проверяющим(и) подразделением(ями).

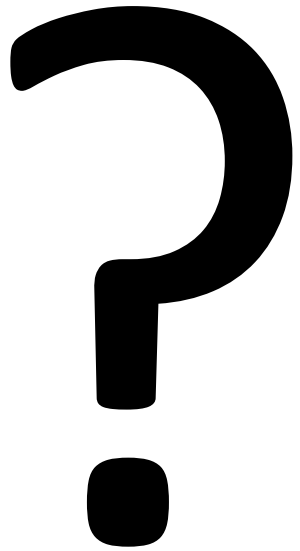
«Сигнал» считается *квалифицированным* при следующих условиях:

- он зарегистрирован в специальном журнале

- (в случае необходимости) проведена предварительная оценка «сигнала», по результатам которой сформулированы выводы о необходимости расследования

Q кв. 20XX	Кол-во квалиф. «сигналов»	Назначено в расслед.	Делегируемые…		Независимые (НВР) …		Завершено / Подтверждено	
			Полностью	с Участием	с Координацией	Полностью	*Делегир.*	*НВР*
“Крупные”	4	4	-	-	2	2	-	3/3
“Меньшие”	17	16	8	2	1	5	7/6	6/5
Общее число “сигналов”	**21**	**20**	**8**	**2**	**3**	**7**	**7/6**	**9/8**
Отчетов в критерием S	5	4	-	2	1	1	2/2	2/1
Этические проблемы, не связанные с мошенничеством	22	*Назначение и завершение проверок этических «сигналов», не связанных с мошенничеством, не отслеживается*						

Вопросы / Контакты



Василий Кудрин, CFE, CIA, CCSA

Член Совета Института внутренних аудиторов
Член Совета российского отделения ACFE

Vasily.Kudrin@gmail.com
http://kudrin.ru
http://kudrin.vc