ФИНАНСОВЫЙ ДИРЕКТОР

Октябрь 2015
Практический журнал по управлению финансами компании

ISSN 1683-9501

Как поймать вора: система выявления внутреннего мошенничества

Методология обнаружения нечистых на руку сотрудников. Как определить нестандартное поведение человека, выявить подозрительные операции.

Читайте полный текст статьи на стр. 18

Также в номере:

«Актион»
Журнал издает медиагруппа «Актион»
Выходит 1 раз в месяц
www.fd.ru

№10

РАБОТА

Проверенные решения для повседневных задач финансового директора

КАК ПОЙМАТЬ ВОРА: ТРИ РЕПЕРНЫЕ ТОЧКИ СИСТЕМЫ ВЫЯВЛЕНИЯ ВНУТРЕННЕГО МОШЕННИЧЕСТВА

Методология обнаружения нечистых на руку сотрудников, включающая в себя приемы определения нестандартного поведения человека, а также аналитические мероприятия, устанавливающие факт совершения подозрительной операции.

Светлана Беляева,
главный эксперт департамента внутреннего аудита крупного западного банка

Любая компания может стать объектом внутреннего мошенничества, и если эти риски не минимизировать, она понесет не только прямой материальный, но и косвенный ущерб в виде потери партнеров, ухудшения деловой репутации (также см. «Воровская статистика» на стр. 23. – *Прим. ред.*). Почему сотрудники воруют, берут взятки и откаты? Причин немало. Так, большинство экономических преступлений совершаются работниками, привыкшими жить не по средствам или имеющими финансовые трудности. Не менее опасны люди, недовольные действиями руководителя или коллег. Стремясь компенсировать нанесенный моральный или материальный ущерб, они могут воспользоваться своим служебным положением для реализации мошеннических схем. Помню, был случай, когда анализ данных о полученных банком доходах показал, что от ряда клиентов не поступает комиссия за расчетно-кассовое обслуживание. В результате проведенного расследования было установлено, что сотрудник банка, обслуживающий этих клиентов, воспользовавшись несовершенной системой

контроля, перечислял всю полученную комиссию на собственные счета в других банках. Свое поведение он объяснил тем, что руководство лишило его премии и, чтобы компенсировать ущерб, он пошел на такой риск.

Потенциальной угрозой являются сотрудники, которые параллельно имеют свой бизнес в аналогичной сфере деятельности или намерены его создать. Они могут использовать базы данных компании для развития собственного бизнеса. Кстати, чтобы получить доступ к конфиденциальным документам компании, преступники порой готовы соглашаться на любую легкодоступную должность. Например, обслуживающий персонал может иметь неконтролируемый доступ к первичным документам и договорам, оставленным на рабочих столах, а также к файлам на незаблокированных компьютерах.

ЛИЧНЫЙ ОПЫТ

Елена Агеева, финансовый директор ООО «Голдер Электроникс», член экспертного совета журнала «Финансовый директор»

В моей практике был случай, когда в компанию пришел новый сотрудник, уже имея на руках офер от прямого конкурента – именно с целью получить доступ к базе данных клиентов и использовать ее у конкурента в качестве первого достижения на новой должности. Мошеннику не повезло – был пойман.

Иллюстрация Софья Мироедова

Об авторе
Светлана Беляева
С 2002 года работает в сфере бухгалтерского учета, налогообложения и аудита, в том числе: в АО ЮниКредит Банк (департамент внутреннего аудита), в компании Deloitte (департамент налогов и права), в ОАО Банк ВТБ (департамент бухгалтерского учета и отчетности). Образование: в 2003 году с отличием окончила Белгородский государственный технологический университет им. В.Г. Шухова по специальности «бухгалтерский учет и аудит».
С 2015 года является действительным членом Института профессиональных бухгалтеров и аудиторов России, имеет сертификаты Harvard Business School Publishing по программам Harvard Management Essentials и Harvard Leadership Essentials.

Украсть, навредить компании может любой сотрудник – даже самый, на первый взгляд, положительный, преданный своему делу. Чтобы обнаружить мошенника, надо разработать комплексную методологию. В ее основу необходимо включить как общие наблюдения, выявляющие неоднозначность поведения сотрудников, так и сугубо аналитические мероприятия, устанавливающие факт совершения подозрительной операции. Кроме того, основные причины и способы реализации мошеннических схем выявляются в ходе служебных расследований. Итак, по порядку опишу главные реперные точки при внедрении методологии обнаружения воров и нечистых на руку работников.

1. РАЗРАБОТКА КЛАССИФИКАЦИИ ВИДОВ МОШЕННИЧЕСТВА

Согласно отчету ACFE, все виды внутреннего мошенничества можно классифицировать, разделив на три категории.

Категория 1. Незаконное присвоение активов. Это преступление реализуется в виде кражи денежных средств, материальных или нематериальных активов. Приведу несколько наиболее часто встречающихся примеров:

- перечисление заработной платы «мертвым душам» (уволенным сотрудникам компании, но не исключенным из списочной численности, или третьим лицам, внесенным в базу данных о работниках компании умышленно);
- хищение данных о поставщиках и заказчиках компании путем направления информации по электронной почте или скачивания на flash-носитель;
- хищение фирменных бланков, форм документов, в том числе и различных договоров, которые компания отнесла к разряду конфиденциальной информации;
- заключение фиктивных сделок на оказание услуг (выполнение работ) – наиболее распространены подобные сделки в сферах, которые сложно оценить, таких как реклама, ремонт помещения, юридические или консультационные услуги.

Категория 2. Коррупция. В основном это откаты и взятки, например:

- завышение суммы договора на оказание услуг (выполнение работ). Как и в ситуации с заключением фиктивных сделок, такие договоры заключаются на услуги (работы), которые сложно проверить и оценить. Обычно это разного рода услуги. Часть суммы, перечисленная компанией по такому договору, соответственно уплачивается исполнителем сотруднику, организовавшему заключение договора;
- дорогостоящие подарки сотрудникам от поставщиков, заказчиков за содействие в подписании с ними договоров.

ЛИЧНЫЙ ОПЫТ

Анна Грачева, вице-президент по финансам НПДП «Логос»

Менеджмент может воровать двумя способами: из доходной части предприятия (уводя часть выручки себе на счета в контролируемые предприятия, давая скидки от прайса и получая обратно часть скидки, и т.д.) и из расходной (завышая сметы, проводя нереальные расходы). Часть из этих злоупотреблений, таких как перечисление выручки на свои счета, можно доказать. А часть – нет. Например, предоставление скидки от базового прайса. В большинстве компаний на каждом уровне ответственных сотрудников есть возможность предоставить скидку от базового прайса для клиентов. Отдел продаж может иметь возможность предоставить скидку до 10 процентов, коммерческий директор – до 20 процентов, генеральный – до 30 процентов. Предположим, менеджер департамента продаж привлекает нового клиента и дает ему скидку в рамках своих полномочий в размере 9 процентов. Вопрос: он молодец? Ответ: да, так как у предприятия повысилась доходная часть и он не превысил свои полномочия. А если 5 процентов от этой скидки ему ежемесячно возвращается в карман в качестве благодарности от клиента? При этом возврат очень сложно доказать. Если же речь идет не о товаре, а об услугах, стоимость которых на рынке имеет больший разброс по ценам, то обычно и размер скидок может быть большим, и, соответственно, возможностей для недоказуемого воровства со стороны менеджмента уйма. Единственная возможность выявить такие случаи (если клиент не мелкая компания) – это финансовым контролерам предприятий поставщика выйти на финансовых специалистов клиента и сверить ходы... По завышениям расходной части тоже доказать мошенничество непросто, так как если смета не завышена в разы, а всего на 30 процентов, то это может быть в рыночных рамках и вполне вероятно, что эти дополнительные проценты уплачиваются за качество, скорость и т.д.

Категория 3. Умышленное искажение важных данных с целью обогащения. *Обычно это первичные документы, финансовая отчетность. Вот примеры:*

- подделка сотрудниками документов по командировочным, представительским и прочим расходам;
- занижение балансовой стоимости активов для последующей их реализации по низкой цене лицам, аффилированным с сотрудником, проводившим их оценку.

ЛИЧНЫЙ ОПЫТ

Елена Агеева, финансовый директор ООО «Голдер Электроникс», член экспертного совета журнала «Финансовый директор»

Возможно еще искажение данных о состоянии тех или иных активов компании. Например, это может быть дорогостоящая оргтехника. Под этим предлогом ее списывают, затем происходит передача участникам схемы.

Анна Грачева, вице-президент по финансам НПДП «Логос»

Пропажа денежных средств из кассы, пропажа товаров из торговых точек, со склада, торговля «левым» товаром и так далее – это виды мошенничества низшего персонала компании. Решение проблемы – коллективная ответственность и удержание сумм ущерба с ответственных лиц. То есть, если по результатам инвентаризации выявлена недостача товара в магазине, весь персонал магазина несет материальную ответственность за это и сумма ущерба удерживается из их зарплаты. Но добавлю, что важно иметь механизм удержания. То есть, если у сотрудников есть фиксированная зарплата, которая не зависит ни от чего, для удержания суммы недостачи необходимо оформить существенный объем документов с участием правоохранительных органов. Если же персонал имеет фиксированную + переменную часть зарплаты, то удержать проще, и компания сможет компенсировать ущерб.

2. ВНЕДРЕНИЕ МЕТОДИКИ ВЫЯВЛЕНИЯ ВОРОВ

Внедряя методику, очень важно пройти все описанные далее этапы.

Этап 1. Разработка индикаторов мошенничества. Эти «красные флаги» свидетельствуют о необычном поведении сотрудника и являются отправной точкой для дальнейшего анализа ситуации. Вот основные и самые значимые индикаторы.

Значительные расходы, не сопоставимые с доходами. Одежда, аксессуары, машины, квартиры, дома, места отдыха, увлечения – это индикаторы, на которые следует обратить внимание в первую очередь. И если сотрудник живет не по средствам, то существует большая вероятность, что официальный заработок – это не единственный его доход.

Финансовые трудности. К информации о том, что у сотрудника финансовые проблемы, стоит отнестись серьезно. Получить ее можно как от самого сотрудника, так и от его коллег. Кроме того, такой показатель, как наличие большого числа кредитов, также является сигналом о возможных финансовых трудностях.

Особенные отношения с поставщиком или заказчиком. Наличие таких отношений вы можете определить по следующим признакам:

- срочность в заключении сделки;
- согласование и подписание контрактов после поставки оборудования или оказания услуг;
- невыставление штрафных санкций при нарушении условий контрактов;
- разбивка крупных контрактов на мелкие для избежания их согласования при наличии в компании лимитов для согласования;
- работа родственников или бывших коллег на руководящих позициях в компаниях-контрагентах.

Необычное поведение сотрудника. По моему опыту, странным следует считать его отказ от новой должности; постоянные задержки на работе; просмотр информации, несвойственной должностным обязанностям; нежелание сотрудника передавать часть своих функций коллегам; работу без отпусков продолжительное время; жалобы на руководство и низкую оплату; социальная изоляция. Такое поведение вполне может свидетельствовать о мошенничестве со стороны сотрудника.

Создание препятствий для проведения аудита. Давление, компрометация, предложение аудитору взяток, задержки в представлении документов, представление ложной информации, невыполнение плана мероприятий без видимых причин, внезапное увольнение ключевых сотрудников – это важные сигналы для аудитора, свидетельствующие о необходимости проведения более тщательной проверки.

Вам желательно составить свой список индикаторов исходя из специфики деятельности компании. Как показывает практика, он облегчает аудиторам работу по обнаружению мошеннических схем. По моему опыту, такие схемы выявляются там, где есть совокупность сигналов. Например, сотрудник отказывается от перевода на новую должность, позволяет себе дорогостоящие отпуска, не соответствующие его доходам. А при проведении проверок он затягивает представление требуемых документов и пишет руководству компании служебные записки с жалобами на некомпетентность внутренних аудиторов. Вместе с тем отдельные сигналы также не стоит игнорировать.

Этап 2. Проведение мероприятий по выявлению мошенничества. Следующие мероприятия разоблачают факты мошенничества с большой достоверностью.

Системный анализ данных. Используется для анализа большого объема данных с целью установления подозрительных операций. Осуществляется сотрудниками департамента рисков на основе информации, полученной из автоматизированной учетной системы. В результате выявляются аномалии, тенденции и показатели риска среди множества операций.

«Воровская» статистика

Отчет Report to the Nations on Occupational Fraud and Abuse (по тексту – Отчет), подготовленный Association of Certified Fraud Examiners (по тексту – ACFE) в 2014 году, приводит следующую статистику:

- 5% годового дохода – средние потери компаний от мошеннических действий сотрудников;
- 18 месяцев – средняя продолжительность реализации мошеннических схем (от момента запуска до ее обнаружения);
- 85% случаев мошенничества приходится на незаконное присвоение активов, 37% – на коррупцию и 9% – на умышленное искажение финансовой отчетности.

Организация горячей линии. Позволяет идентифицировать практически любые виды мошенничеств. Хоть в российских компаниях к доносам относятся как к пережитку советских времен, горячая линия – наиболее эффективный и малозатратный метод выявления мошенничества.

Служебное расследование. Вот что вам надо сделать, чтобы провести его оперативно и результативно.

1. Создать комиссию по расследованию. Формируется она на основании приказа руководителя компании, в котором определяются сроки расследования и ответственные лица. В зависимости от специфики совершенного преступления в состав комиссии могут входить руководящий менеджмент, главный бухгалтер или его заместитель, а также представители отдела внутреннего аудита, юридического департамента, службы по работе с персоналом, службы безопасности и отдела информационных технологий.

2. Провести расследование. Расследование, как правило, включает в себя следующие действия:

- интервью с потенциальным виновником, свидетелями, иными вовлеченными лицами и получение письменных объяснений;
- сбор доказательств (первичная документация, договоры и др.);
- анализ политик и бизнес-процессов компании;
- системный анализ данных.

Затем комиссия готовит отчет и план корректирующих мероприятий, которые согласовываются с ответственными подразделениями и определяются сроки его исполнения. Результаты расследования представляются руководству и аудиторскому комитету компании.

Этап 3. Контроль исполнения плана мероприятий. Чтобы упорядочить процесс контроля, все корректирующие мероприятия нужно учитывать в единой базе данных, из которой можно в любой момент получить информацию об их исполнении (завершенные, в процессе исполнения и просроченные).

77%

мошеннических схем

реализуется сотрудниками одного из семи подразделений компаний и банков: бухгалтерского учета, операционного департамента, отдела продаж, отдела обслуживания клиентов, департамента закупок, финансового отдела, а также высшим менеджментом.

По результатам исполнения мероприятий ответственное подразделение отчитывается контролеру. Возможны ситуации, когда мероприятия не выполняются длительное время, так как ответственное подразделение не хочет или не может их исполнить, а у контролера нет механизма воздействия на него. В этом случае необходимо разобраться, в чем причина неисполнения плана мероприятий, а контролера наделить необходимыми полномочиями. Например, если мероприятия не исполнялись по независящим от сотрудника обстоятельствам, то нужно перенести сроки исполнения или отменить мероприятие, в противном случае контролер информирует о факте игнорирования требований по выполнению плана мероприятий руководство компании, а то, в свою очередь, принимает решение о наказании руководителя подразделения и сотрудника, ответственного за выполнение мероприятий, в том числе путем депремирования, объявления замечания или выговора.

Внимание!
Индикаторы не являются однозначным свидетельством преступления, они лишь указывают на возможность его осуществления. Например, приобретать дорогую недвижимость можно за счет доходов супруга, срочность в заключении сделки может быть обусловлена получением выгодных условий. Подобные сигналы указывают руководителю подразделения и внутренним аудиторам на то, что стоит внимательнее присмотреться к работе ответственного сотрудника.

ЛИЧНЫЙ ОПЫТ

Анна Грачева, вице-президент по финансам НПДП «Логос»

Работа контролеров и проверки действий менеджеров – процесс ювелирный, так как очень многие люди негативно воспринимают проверки своей деятельности, а тем более появление каких-то намеков на мошенничество. Например, зачастую неаккуратно проведенная проверка в департаменте продаж выявляет одного ворующего сотрудника, но отбивает желание работать у всех остальных. И тут никакое командообразование не поможет. Поэтому прежде чем создавать комиссии по проверке и прочее, контролеры должны тихонько, не вызывая лишних вопросов, собрать факты по подозрительным случаям.

3. ВВЕДЕНИЕ ПРЕВЕНТИВНЫХ МЕР ЗАЩИТЫ

Мошенничество легче предотвратить, чем выявить. Поэтому необходимо наладить механизм сокращения рисков возникновения мошенничества. Следующие упреждающие меры помогут вам в этой работе.

Анализ бизнес-процессов и оценка рисков мошенничества. Предотвращение мошенничества начинается с изучения бизнес-процессов и обнаружения потенциальных угроз преступных действий. Далее оценивается существенность выявленных рисков, то есть просчитывается вероятность и последствия совершения преступления. Риск стоит игнорировать, если возможный ущерб от него меньше, чем затраты на его устранение. Например, хищение денежных средств сотрудником кассы – событие маловероятное, так как будет быстро обнаружено. Кроме того, при наличии своевременной инкассации оно не нанесет существенного ущерба компании. В противном случае необходимо принять меры по минимизации риска (доработать бизнес-процессы, внедрить дополнительные контрольные процедуры и др.). Например, для выбора какого-либо

поставщика услуг компания утверждает тендерную процедуру, позволяющую найти оптимального контрагента.

Если сократить риск не представляется возможным, стоит отказаться от такого бизнес-процесса.

Предварительные процедуры контроля. К ним относятся:

1) контроль фактического наличия и состояния объектов;

2) авторизация сделок и операций, то есть подтверждение контролирующим сотрудником всех операций, введенных в автоматизированную систему исполнителем;

3) проверка контролирующим сотрудником оформленных документов до совершения бухгалтерских записей по операциям, требующим дополнительного контроля. Перечень таких операций вы должны определить самостоятельно. Например, это могут быть крупные сделки или сделки с определенными контрагентами;

4) реализация принципа «знай своего сотрудника». Он заключается в том, что при приеме кандидата на работу важно оценить не только его квалификацию, но и получить о нем дополнительную информацию, в том числе характеристику с прежнего места работы, сведения из социальных сетей.

Проведение информационных мероприятий. Меры борьбы с мошенничеством, последствия преступлений для компании и персонала, действия сотрудников при подозрении на совершаемые со стороны коллег преступления, наказание за участие в мошеннических схемах – эти и другие темы необходимо регулярно обсуждать внутри компании. Подобные встречи являются не только источником информации, но и сигналом потенциальным мошенникам, что вопрос находится на контроле у руководства.

Для получения максимальной отдачи от таких тренингов, следуйте советам.

1. Тренинги и семинары, посвященные вопросам мошенничества, проводите не реже одного раза в три-четыре месяца.

2. В зависимости от темы доклада включите в них выступление представителей департаментов внутреннего аудита, рисков, службы безопасности, департамента по работе с персоналом, юридического отдела.

3. Если на встрече планируется обсуждать вопросы, касающиеся внесения изменений во внутренние нормативные документы, тогда информацию о содержании доклада доведите до слушателей за два-три дня по e-mail, а по окончании мероприятия попросите их заполнить вопросник для оценки усвоенного материала.

4. По окончании каждой встречи слушатели анонимно должны заполнить листы с обратной связью (фитбэки), где им потребуется ответить на вопросы, касающиеся полезности полученной информации, и высказать пожелания к содержанию будущих докладов.

Мотивация и оценка работы сотрудников. Людям важно, чтобы их компетентность и высокие результаты работы признавались и были отмечены руководителем, в том числе путем материального вознаграждения. Работники, чьи заслуги игнорируются, которым не дается обратная связь о качестве проделанной работы, могут затаить обиду. Подобная ситуация угрожает безопасности компании.

ПРИМЕР

Сотрудник одной факторинговой фирмы не исполнял свои обязанности по верификации поставок товара от клиентов компании (поставщиков) дебиторам (покупателям), а именно не получал от дебиторов информацию и документы, подтверждающие факт поставки и суммы отгруженного товара. Воспользовавшись данной ситуацией, клиент (поставщик) смог реализовать мошенническую схему: получал от факторинговой компании финансирование и представлял ей фальсифицированные документы об отгрузках дебитору (покупателю), которых фактически не производил. Нанесенный факторинговой компании ущерб составил более 130 млн рублей. Из объяснительной

записки виновного сотрудника следовало, что руководитель его подразделения без объяснения причин неоднократно отказывал ему в переводе на вновь открытую позицию, а также в повышении заработной платы. В связи с этим он потерял интерес к выполнению своих обязанностей.

ЛИЧНЫЙ ОПЫТ

Елена Агеева, финансовый директор ООО «Голдер Электроникс», член экспертного совета журнала «Финансовый директор»

Очень эффективно применение механизмов нематериального стимулирования сотрудников, что особенно актуально в условиях минимизации затрат (о приемах нематериальной мотивации, вдохновляющих персонал на трудовые подвиги, читайте на стр. 82. – *Прим. ред.*).

Внимание!

Ограничивая полномочия, функции подразделения нужно закрепить в Положении об отделе (департаменте), а обязанности сотрудника – в должностной инструкции. Права доступа в операционную систему компании также должны быть ограничены в соответствии с функционалом сотрудника.

Ограничение полномочий. Слишком широкий круг полномочий и отсутствие четкого разграничения обязанностей представляют собой потенциальную угрозу. Функции необходимо распределить так, чтобы исполнение и контроль осуществляли разные подразделения, а в рамках одного подразделения разные сотрудники. Например, может быть такое разграничение полномочий и обязанностей: вводом заявок (первичных учетных документов и др.) в базу данных и их авторизацией занимается отдел закупок, а их проверку на соответствие бюджету осуществляет сотрудник финансовой службы.

Разработка документов, сокращающих риск мошенничества. К таким документам относятся:

1) комплексная политика – определяет основные процедуры, направленные на предотвращение мошенничества (в том числе критерии мошеннических действий, порядок организации контроля, хранения документов и ценностей, требования к применению паролей к персональным компьютерам);

2) кодекс поведения – это свод правил и норм делового поведения сотрудников компании. В кодексе может содержаться, например, следующая информация:

- нормы делового общения и взаимодействия с коллегами, клиентами,
- правила поведения на рабочем месте,
- отношение сотрудников к имуществу и интеллектуальной собственности компании, к конфиденциальной информации, к коррупции и мошенничеству,
- ответственность сотрудников и руководителей за соблюдение этических норм;

3) план реагирования в случае обнаружения мошеннической схемы, который может включать в себя информацию о порядке проведения расследования, составе комиссии, порядке информирования руководства о ходе и результатах расследования и т.д.