

Противодействие корпоративному мошенничеству: выстраивание линии защиты с помощью внутреннего аудита



Володин Александр

CIA¹, CISA², CFE³, начальник управления дирекции по внутреннему аудиту ПАО «ФосАгро», член Ассоциации «Институт внутренних аудиторов»⁴

По данным Ассоциации специалистов по расследованию мошенничества (ACFE), мошенничество обходится организациям ежегодно в 5% выручки⁵. Свыше 2000 **выявленных** случаев мошенничества в 133 странах мира в 2020–2021 гг. привели к потерям на сумму 3,6 млрд долл., с медианным значением убытков в 117 тыс. долл. 21% случаев привели к потерям свыше 1 млн долл.

Пандемия коронавируса в 2020–2021 гг. и геополитическая обстановка 2022 г. усугубили ситуацию с рисками мошенничества. Основной причиной этого стал перевод многих функций и организаций в целом в чрезвычайный режим работы, когда система внутреннего контроля приносилась в жертву оперативности, гибкости, а иногда и самой возможности решения задач и достижения целей.

Все это повышает ценность функции внутреннего аудита как одного из независимых центров обеспечения необходимых гарантий для высшего руководства и собственников организаций.

В этой статье мы рассмотрим основные подходы к построению системы управления рисками мошенничества и роль функции внутреннего аудита в этой системе.

ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСТВА И РОЛЬ ВНУТРЕННЕГО АУДИТА

Уголовный кодекс РФ определяет мошенничество как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Международные профессиональные стандарты внутреннего аудита⁶ содержат более подробное определение мошенничества: любые незаконные действия, характеризующиеся обманом, сокрытием или злоупотреблением доверием. К мошенническим не относятся те действия, которые производятся

- 1 Международная сертификация Certified Internal Auditor (Дипломированный внутренний аудитор).
- 2 Международная сертификация Certified Information Systems Auditor (Сертифицированный ИТ-аудитор).
- 3 Международная сертификация Certified Fraud Examiner (Сертифицированный эксперт по мошенничеству).
- 4 Ассоциация «Институт внутренних аудиторов» (Ассоциация «ИВА»), зарегистрированная в 2000 г., является профессиональным объединением более чем 4000 внутренних аудиторов, внутренних контролеров и работников других контрольных подразделений российских компаний и организаций. Подробности на сайте www.iaa-ru.ru.
- 5 Источник — отчет ACFE «Occupational Fraud 2022: A Report to the Nations».
- 6 МПСВА (IPPF), ред. 2016: https://www.iaa-ru.ru/inner_auditor/professional/.

под воздействием силы или угрозы применения силы. Мошенничество совершается физическими и юридическими лицами в целях получения денег, собственности или услуг, уклонения от выплаты денежных средств или оказания услуг либо в целях личной или коммерческой наживы.

ACFE в отчете 2022 г. выделяет три основные категории мошенничества:

1

хищение активов — самый распространенный и наименее «дорогой» вид мошенничества (86% случаев, медианный ущерб — 100 тыс. долл.), включает в себя:

- хищение наличных и безналичных денежных средств,
- необоснованные выплаты,
- хищение товарно-материальных ценностей.

2

Коррупция (50% случаев, 150 тыс. долл.):

- подкуп,
- конфликт интересов,
- вымогательство.

3

Искажение финансовой отчетности — самый редкий вид с наибольшими суммами ущерба (9%⁷ и почти 600 тыс. долл.), предполагает существенное завышение или занижение активов или финансового результата посредством:

- сокрытия или приписывания доходов или расходов,
- некорректной оценки активов,
- нарушений сроков учета операций,
- нарушений правил раскрытия информации.

Разнообразие видов мошенничества, то, как они могут повлиять на конкретную организацию в конкретный момент времени, и даже различия в определении мошенничества в применимых нормативных документах — все это усложняет задачу противодействия мошенничеству и требует от внутренних аудиторов наличия специальных знаний и навыков, чтобы своевременно проводить оценку рисков мошенничества.

Роль службы внутреннего аудита в предотвращении мошенничества заключается в предоставлении гарантий адекватности и эффективности системы управления рисками мошенничества и консультировании по вопросам ее улучшения. Внутренний аудит может проводить оценку качества управления рисками мошенничества на уровне организации как в форме специального проекта, так и путем сбора воедино наблюдений и выводов отдельных проверок.

Чтобы быть эффективными в деле противодействия мошенничеству, внутренние аудиторы должны понимать природу и свойства мошенничества, возможные точки возникновения в их организации, эффективные стратегии управления рисками, ролевую модель и распределение обязанностей. Помимо этого, аудиторы должны уметь сформулировать и подать руководству и совету директоров свое мнение о качестве системы управления рисками и предотвращения мошенничества.

Хотя мошенничество и может принимать самые разные формы, оно опирается на три базовых фактора:

- мотивация — финансовые или эмоциональные стимулы совершать мошенничество;
- возможность — воспринимаемая способность воплотить в жизнь план без страха наказания;

7 Примечание: указанные частоты (86%, 50% и 9%) в сумме дают больше 100%, так как одно событие может включать более одного вида мошенничества.

- рационализация — внутреннее обоснование неэтичных поступков.

Мошенничество — осознанный акт, это отличает его от халатности или ошибки. Мошенник осознанно старается извлечь выгоду из обстоятельств, используя уязвимости контролей, — либо для обогащения, либо под давлением. Как правило, мошенники стремятся убедить себя и, возможно, окружающих, что их действия правомерны.

Руководство по управлению рисками мошенничества COSO определяет предотвращение мошенничества как процесс исключения факторов, позволяющих мошенничеству совершиться.

ТРЕБОВАНИЯ К ВНУТРЕННЕМУ АУДИТУ

В МПСВА мошенничество упоминается в контексте профессионализма (стандарт 1210) и должной осмотрительности (стандарт 1220). Стандарт 1210.A2 требует от внутренних аудиторов

«обладать достаточными знаниями, чтобы оценить риск мошенничества и то, каким образом организация управляет этим риском. В то же время не предполагается, что внутренние аудиторы обладают компетенцией специалиста, чья основная функция заключается в выявлении и расследовании фактов мошенничества».

Стандарты требуют принимать во внимание вероятность мошенничества в работе в целом (1220.A1) и при планировании аудиторских проверок (2210.A2).

В ходе оценки эффективности процесса управления рисками организации в целом служба внутреннего аудита должна оценивать возможности совершения мошенничества и подходы

организации к управлению риском мошенничества (стандарт 2120.A2).

Стандарт 2060 предписывает руководителю службы внутреннего аудита периодически отчитываться перед менеджментом и советом директоров о выявленных существенных рисках и недостатках контролей, в том числе связанных с мошенничеством.

СПЕЦИФИКА ОРГАНИЗАЦИИ

Не существует единого универсального подхода к управлению рисками мошенничества. Определение, выявление, управление и снижение рисков мошенничества в организации зависит от следующих факторов:

- отрасль и географическое положение;
- размер, организационная структура и стратегические цели;
- существующие структуры и системы корпоративного управления, управления рисками и внутреннего контроля;
- корпоративная культура и ценности;
- информационные системы и технологии;
- деловая среда, включая применимое законодательство и регулирование на всех уровнях (местном, региональном, государственном и международном).

Все эти факторы определяют подходы к идентификации, оценке и приоритизации рисков, схем и случаев мошенничества и реагирования организации на них. Менеджмент и совет директоров должны определить риск-аппетит организации — уровень риска, который они готовы принять, — и оценивать затраты на управление рисками в сравнении с выгодами от их снижения или устранения.

Предоставление гарантий и консультаций по адекватности и эффективности рисков мошенничества внутренним аудитом требует от службы глубокого

понимания всех аспектов организации. Успешное управление рисками мошенничества зависит от правильного распределения ролей, обязанностей и ресурсов, для чего рекомендуется применять Модель трех линий защиты⁸:

- 1 Первая линия — менеджмент — руководит и осуществляет действия, необходимые для достижения целей организации, устанавливает структуры и процессы для управления рисками.
- 2 Вторая линия — менеджмент — предоставляет дополнительные знания, поддержку, мониторинг и помощь в решении проблем.
- 3 Третья линия — внутренний аудит и внешние поставщики гарантий — предоставляет независимые и объективные гарантии и рекомендации менеджменту и совету директоров относительно адекватности и эффективности корпоративного управления и управления рисками для поддержки достижения целей организации.

Модель трех линий подчеркивает важность четкого и последовательного «тона сверху», сотрудничества и взаимодействия между функциями и сотрудниками внутри организации и независимости функции внутреннего аудита.

РАСПРЕДЕЛЕНИЕ РОЛЕЙ

Управление рисками мошенничества — общая задача всей организации, от членов совета директоров до рядовых сотрудников. Система управления рисками мошенничества может также на формализованной основе включать внешних консультантов, поставщиков гарантий и других экспертов по противодействию мошенничеству.

Совет директоров несет общую ответственность за эффективное управление рисками мошенничества и задает соответствующий «тон сверху». Совет совместно с высшим менеджментом формулирует ожидания этического поведения и определяет риск-аппетит организации. Совет директоров может назначить одного из своих представителей или представителей высшего руководства куратором вопроса управления рисками мошенничества для повышения осведомленности и координации деятельности.

Совет директоров должен осуществлять мониторинг и оценку деятельности менеджмента по противодействию мошенничеству, включая действия по выявлению и оценке рисков, внедрение мер противодействия и текущую оценку эффективности системы.

Совет может сформировать отдельный **комитет по аудиту** для надзора за функцией внутреннего аудита. В таком случае комитету по аудиту могут быть переданы функции по мониторингу и надзору за управлением рисками мошенничества, включая предотвращение и выявление мошенничества со стороны менеджмента.

Менеджмент выполняет поставленную советом директоров задачу по достижению целей организации и является главным ответственным за функционирование системы предотвращения, выявления и реагирования на мошенничество.

В обязанности менеджмента входит построение и поддержание эффективной системы внутреннего контроля с разумными затратами на нее. Менеджмент осуществляет надзор за деятельностью сотрудников, как правило, через внедрение и мониторинг процессов и внутренних контролей. Также менеджмент оценивает уязвимость организации перед мошенническими действиями.

8 Подробнее см. <https://www.iaa-ru.ru/news/iaa-vypustil-vazhnoe-obnovlenie-kontseptsii-trekh-linij-zashchity/>.

Роли менеджмента применительно к управлению рисками делятся на первую и вторую линии защиты.

Первая линия включает сотрудников и менеджеров, ответственных за внедрение и мониторинг контролей за рисками мошенничества, а также за информирование и эскалацию в случае возникновения подозрения на мошенничество.

Вторая линия занимается управлением рисками мошенничества совместно с высшим руководством. Конкретные функции и задачи сильно зависят от отрасли, зрелости и размера организации и других факторов. В целом роль второй линии заключается в обеспечении эффективности дизайна и функционирования процессов и контролей по управлению рисками мошенничества.

Для небольших организаций с ограниченными ресурсами могут быть оправданы аутсорсинг функций управления рисками мошенничества или передача части функций внутреннему аудиту. При этом необходимо зафиксировать эту передачу в положении о внутреннем аудите и принять меры по обеспечению внутреннего аудита ресурсами, знаниями и навыками, а также уделить особое внимание сохранению независимости и объективности внутреннего аудита.

Внутренний аудит — третья линия — предоставляет менеджменту и совету директоров гарантии эффективности процесса оценки и управления рисками мошенничества, включая оценку последовательности мер по противодействию мошенничеству и их соответствия стратегии, целям и нюансам деятельности организации.

Внутренний аудит должен всегда руководствоваться принципами профессионализма, соблюдения Кодекса этики и Правил поведения, поддержания объективности, конфиденциальности и компетентности. Внутренние аудиторы в своей работе должны служить образцом для подражания

и всегда учитывать риски мошенничества при планировании и выполнении аудиторских заданий и отчетности о результатах.

Внутренний аудит может участвовать в разработке политик, в обучении персонала и в проведении расследований. Еще раз стоит подчеркнуть, что любое участие внутреннего аудита в управлении рисками мошенничества должно быть предусмотрено положением о внутреннем аудите и отражено в регламентах и процедурах функции. Это необходимо в первую очередь для того, чтобы менеджмент и совет директоров понимали и были согласны с ролью внутреннего аудита и осознавали необходимость и меры по обеспечению независимости и объективности внутреннего аудита.

Задача внутреннего аудита — предоставить независимые и объективные гарантии касательно всех значимых аспектов рисков мошенничества. Каждая аудиторская проверка помогает лучше узнать организацию, ее контрольную среду и культуру управления рисками мошенничества.

По результатам своей работы внутренний аудит информирует менеджмент и совет директоров об адекватности и эффективности системы управления рисками мошенничества на уровне конкретного аудируемого бизнес-процесса и в масштабах всей организации и предлагает свои соображения и рекомендации по возможностям улучшения процедур.

МОДЕЛИ УПРАВЛЕНИЯ РИСКАМИ МОШЕННИЧЕСТВА

Чтобы эффективно управлять рисками мошенничества, требуется целостный, систематический подход, включающий политики, инструменты, обучение и другие контрольные процедуры, а также вовлечение в культуру противодействия мошенничеству всех уровней внутри организации. Для внедрения такого подхода следует

использовать целостную модель управления рисками мошенничества, что обеспечит систематический, последовательный характер мероприятий по выявлению, оценке и управлению рисками. Модель можно разработать самостоятельно или адаптировать к специфике организации одну из существующих моделей, например Модель управления рисками COSO.

Модель управления рисками COSO опирается на пять компонентов системы внутреннего контроля из Интегрированной модели внутреннего контроля COSO, из которых вытекают пять принципов управления рисками мошенничества:

- 1** Управление рисками мошенничества: организация создает программу управления рисками мошенничества, которая показывает ожидания совета директоров и высшего руководства и их стремление обеспечить честность и этичность ведения бизнеса.
- 2** Оценка рисков мошенничества: организация проводит оценки рисков мошенничества, выявляет применимые риски и схемы, оценивает их вероятность и значимость, оценивает эффективность контролей и разрабатывает меры по снижению остаточных рисков мошенничества.
- 3** Контрольные процедуры: организация выбирает, разрабатывает и внедряет превентивные и выявляющие контроли для снижения риска совершения или несвоевременного выявления случаев мошенничества.
- 4** Расследования мошенничества и корректирующие мероприятия: организация выстраивает процесс коммуникации для сбора информации о возможных случаях мошенничества и принимает скоординированные шаги для их расследования

и выработки корректирующих мероприятий.

5

Мониторинг системы управления рисками мошенничества: организация выбирает, разрабатывает и осуществляет регулярную оценку наличия и эффективного функционирования каждого из пяти принципов и своевременно сообщает ответственным лицам о выявленных недостатках.

РОЛЬ СЛУЖБЫ ВНУТРЕННЕГО АУДИТА В ОЦЕНКЕ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ МОШЕННИЧЕСТВА

Предоставление гарантий по системе управления рисками мошенничества в масштабах всей организации требует от внутреннего аудита оценки адекватности и эффективности применяемой модели управления рисками мошенничества, а также структур, процессов и текущей деятельности по противодействию мошенничеству. Важным источником информации для такой оценки являются отдельные аудиторские проверки, которые затрагивали риски мошенничества. Помимо этого, внутренний аудит должен периодически проводить общий анализ рисков мошенничества в масштабах организации совместно с первой и второй линиями, но сохраняя независимость и объективность.

Помимо участия в расследованиях уже выявленных случаев мошенничества, внутренний аудит также может самостоятельно искать признаки мошенничества. В этом важную роль играют компьютеризированные методы аудита: непрерывный аудит, анализ данных и интеллектуальный анализ данных (data mining). Также внутренний аудит может использовать аналитические и иные процедуры для поиска аномалий и подробного анализа высокорисковых процессов и операций с целью выявления потенциального мошенничества.

ПРОЦЕСС ОЦЕНКИ РИСКОВ МОШЕННИЧЕСТВА СЛУЖБОЙ ВНУТРЕННЕГО АУДИТА

За операционную часть управления рисками мошенничества отвечает менеджмент организации, а задача внутреннего аудита — оценка рисков мошенничества. Результаты оценки следует обсуждать с представителями менеджмента, ответственными за риски мошенничества, а в отдельных случаях, определяемых применимым законодательством и регулированием, — и с внешними аудиторами.

В приложении к компонентам и принципам Модели управления рисками COSO процесс оценки рисков мошенничества состоит из следующих этапов:

1 Идентификация риска: внутренний аудит выявляет уязвимости на основании ранее проведенных аудитов, интервью с ответственными за управление рисками и опросы ключевых заинтересованных сторон.

2 Оценка существенности риска: внутренний аудит оценивает существенность риска путем анализа возможных факторов и схем мошенничества и измерения вероятности, воздействия, скорости реализации и прочих характеристик рисков в соответствии с принятым в организации подходом к оценке рисков.

3 Расстановка приоритетов: внутренний аудит определяет более и менее приоритетные для управления рисками с точки зрения целей организации.

4 Внедрение мер реагирования на риск: внутренний аудит анализирует меры реагирования на риск путем описания процессов и контролей, затрагивающих каждую схему мошенничества, и оценки остаточного риска.

5

Разработка целостного видения факторов риска: внутренний аудит создает единую картину рисков мошенничества, анализируя взаимосвязи между рисками мошенничества и влияние других рисков на вероятность совершения мошенничества. Основные факторы риска: изменения корпоративной структуры, изменения ролей и обязанностей, особенно в вопросах управления рисками мошенничества, текучесть и нехватка персонала, существующие меры по стимулированию и вознаграждению сотрудников и менеджеров и общие экономические условия.

ОЦЕНКА ПРОГРАММЫ УПРАВЛЕНИЯ РИСКАМИ МОШЕННИЧЕСТВА

Оценка службой внутреннего аудита каждого компонента программы управления рисками мошенничества — ключевой элемент процесса предоставления гарантий по рискам мошенничества.

Подходы к оценке программы управления рисками можно сгруппировать по пяти компонентам системы внутреннего контроля по модели COSO: контрольная среда, оценка риска, контрольные мероприятия, информация и коммуникация, мониторинг.

КОНТРОЛЬНАЯ СРЕДА

Если в организации применяется какая-либо модель управления рисками мошенничества (например, COSO Управление рисками организации), внутренний аудит должен убедиться, что внедрены все применимые компоненты этой модели и что роли и обязанности участников процесса четко прописаны и понимаются сотрудниками и руководителями.

В организации должны быть приняты и разъяснены всем сотрудникам Кодекс этики и делового поведения и политики и процедуры противодействия мошенничеству. Менеджмент должен продемонстрировать свою приверженность культуре противодействия мошенничеству и задавать правильный «тон сверху».

Ключевую роль в выявлении и предотвращении мошенничества играет возможность конфиденциально сообщить о возможных случаях мошенничества — например, через горячую линию. Также необходимы формализованные процедуры проведения расследований.

Внутренний аудит должен оценивать внешнюю и внутреннюю среду организации в поисках новых факторов риска мошенничества, таких как изменения регулирования, изменения организационной структуры, выход на новые рынки, проблемы в отрасли, проблемы с контрагентами (закупки, продажи, логистика), изменения подходов к компенсации сотрудников и менеджеров.

ОЦЕНКА РИСКА

Внутренний аудит должен оценить, насколько существующие процессы и методы выявления и оценки рисков мошенничества охватывают все основные потенциальные источники факторов риска:

- финансовое или эмоциональное давление или стимулы, которым подвергаются сотрудники (нехватка персонала, жесткие сроки выполнения задач, реорганизация, трудно-выполнимые показатели эффективности, внутренняя конкуренция);
- новые возможности совершения мошенничества (например, изменения оргструктуры, новые распределения обязанностей, изменения контрольных процедур);

- рационализация мошенничества (внешнее экономическое или социальное давление, сокращение компенсаций, понижения в должности).

КОНТРОЛЬНЫЕ МЕРОПРИЯТИЯ

Никакие контроли не могут быть эффективными, если выполняющие их сотрудники или менеджеры не владеют должными навыками или не понимают конечной цели выполнения этих контролей.

Поэтому крайне важно, чтобы в организации был налажен процесс информирования и обучения сотрудников и менеджеров вопросам управления рисками мошенничества. Все кодексы, политики и процедуры должны регулярно обновляться в соответствии с новыми условиями, а все изменения — доводиться до сведения сотрудников.

Программы обучения также необходимо регулярно обновлять, а само обучение и информирование должно затрагивать всех сотрудников и менеджеров.

ИНФОРМАЦИЯ И КОММУНИКАЦИЯ

Роли и обязанности по управлению рисками мошенничества должны быть четко формализованы, доведены до сведения ответственных лиц и регулярно обновляться.

В организации должен быть внедрен механизм информирования о возможных случаях мошенничества (горячая линия). Этот механизм должен поддерживаться в рабочем состоянии, а все сообщения, получаемые через него, должны быть оперативно эскалированы и рассмотрены.

Расследования возможных случаев мошенничества должны проводиться в соответствии с установленной процедурой сотрудниками, свободными

от конфликтов интересов, с возможностью привлечения внешних экспертов. В рамках расследования необходимо не только анализировать конкретное событие, но и проводить анализ первопричин, сделавших это событие возможным. По итогам такого анализа должны оперативно приниматься меры по устранению выявленных уязвимостей.

Результаты расследований должны оперативно доводиться до сведения совета директоров и, при необходимости, до внешних аудиторов.

Крайне важно, чтобы дисциплинарные меры применялись последовательно ко всем виновным лицам, независимо от их положения в организации.

МОНИТОРИНГ

Результаты расследований и другие новые сведения о рисках мошенничества должны находить отражение в изменениях политик, процедур и контролей, а также в применяемых методиках непрерывного мониторинга и аудита.

Меры по мониторингу рисков мошенничества должны строиться в соответствии с риск-ориентированным подходом, то есть в первую очередь нужно рассматривать аспекты деятельности организации, где риски мошенничества наиболее существенны.

Менеджмент должен проводить регулярный мониторинг контролей по противодействию мошенничеству и оценивать их эффективность и покрытие.

ОТЧЕТНОСТЬ ВНУТРЕННЕГО АУДИТА ПО ОЦЕНКЕ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ МОШЕННИЧЕСТВА

Руководитель функции внутреннего аудита должен периодически докладывать высшему

руководству и совету директоров обо всех существенных рисках мошенничества и выявленных недостатках контролей и корпоративного управления. В зависимости от масштабов организации и других факторов может быть установлен уровень материальности или существенности, при превышении которого событие или недостаток должны быть доведены до сведения совета директоров. Также необходимо информировать совет директоров о статусе расследования ранее выявленных потенциальных случаев мошенничества.

Руководитель СВА должен сообщать совету директоров, соблюдает ли менеджмент установленный советом уровень риск-аппетита. Если принятый руководством уровень риска превышает риск-аппетит, внутренний аудит должен сначала попытаться решить эту проблему с менеджментом, а при невозможности — вынести этот вопрос на рассмотрение совета директоров.

Также руководитель СВА может выносить на обсуждение высшего руководства и совета директоров факторы корпоративной культуры и контрольной среды, которые создают давление или возможности совершать мошенничество.

В целом в рамках отчетности перед советом директоров и высшим руководством внутренний аудит должен ответить на вопрос, насколько система управления рисками мошенничества соответствует стратегическим целям организации и охватывает ли она все аспекты деятельности организации. Необходимо также оценить адекватность и эффективность мер по управлению рисками мошенничества, включая корпоративную культуру и ее поддержку менеджментом и советом директоров, и наличие у менеджмента необходимых навыков и ресурсов для эффективного управления рисками мошенничества. И главный вопрос — соответствует ли остаточный риск мошенничества риск-аппетиту организации?