

Османова Патимат Мустафаевна
к.э.н., доцент кафедры «Бухучет, АХД и аудит»
Валиева Макка Залимхановна
студентка 3 курса
факультета экономики и управления
ГАОУ ВО «Дагестанский государственный университет народного хозяйства»
г. Махачкала, Россия

Корпоративное мошенничество: практика выявления и противодействия

Аннотация. Статья посвящена актуальной проблеме: корпоративное мошенничество. В данной статье рассматривается практика выявления и противодействия корпоративному мошенничеству. Авторами проанализированы основные виды корпоративного мошенничества, выделены методы его выявления и эффективные стратегии борьбы с ним.

Ключевые слова: корпоративное мошенничество, практика выявления и противодействия, виды мошенничества, причины.

Osmanova Patimat Mustafaevna
Candidate of Economics, Associate Professor of the Department of Accounting,
Accounting and Auditing
Valieva Makka Zalimkhanovna 3rd year student
of the Faculty of Economics and Management
Dagestan State University of National Economy
Makhachkala, Russia

Corporate fraud: the practice of detection and counteraction

Annotation. The article is devoted to a current problem: corporate fraud. This article discusses the practice of identifying and combating corporate fraud. The authors analyzed the main types of corporate fraud, identified methods for identifying it and effective strategies to combat it.

Keywords: corporate fraud, practice of detection and counteraction, types of fraud, causes.

Проблема корпоративного мошенничества остается важной и востребованной среди бизнес-сообщества. Согласно последнему опросу Deloitte Forensic, в корпорациях стран Содружества Независимых Государств чаще всего организаторами и участниками мошеннических схем становятся сотрудники среднего звена. По данным РБК, за последние два года корпоративное мошенничество затронуло более половины (55%) компаний, действующих в России и странах СНГ. 73% жертв мошенников приходится на компании с численностью персонала более тысячи человек. Одной из самых распространенных мошеннических схем является сговор сотрудников пострадавшей компании с ее контрагентами.

В современном деловом мире корпоративное мошенничество представляет собой серьезную угрозу для организаций. Следовательно, корпоративное мошенничество представляет собой вид преступной деятельности, связанный с незаконными действиями в предприятиях, организациях, корпорациях или иных структурах.

Корпоративное мошенничество – это действия или бездействие физических и/или юридических лиц, нарушающие статьи Уголовного кодекса РФ, такие как статья 159 "Мошенничество", статья 160 "Присвоение или растрата" и статья 201 "Злоупотребление полномочиями". Эти действия направлены на личное обогащение или получение выгоды другому лицу за счет компании, повреждают интересы компании и могут причинить ей

финансовый и/или репутационный ущерб при помощи обмана, злоупотребления доверием или иных способов, используя свое служебное положение.

Мошенничество - это преступление, заключающееся в приобретении права на чужое имущество путем обмана и злоупотребления доверием, а также в присвоении чужого имущества.

Присвоение или растрата - это преступление, заключающееся в распоряжении чужим имуществом без права владельца, вверенным виновному лицу.

Корпоративные мошенничества могут включать в себя различные виды преступлений, например:

1. Финансовые мошенничества: включают в себя такие действия, как мошенничество с кредитными картами, инвестиционные схемы обмана, фальсификация финансовой отчетности, финансовый мошенничество и т. д. Данный вид мошенничества наносит ущерб как отдельным лицам, так и организациям, и может повлечь за собой серьезные юридические последствия для преступников. Поэтому важно быть внимательным и бдительным в финансовых операциях и не доверять личной информации или деньгам незнакомым людям или организациям;

2. Кража активов: это одна из форм корпоративного мошенничества, которая происходит, когда сотрудник или руководитель организации злоупотребляет своими полномочиями и укрывает средства или другие активы компании в свою личную пользу. Это может включать в себя такие действия, как сокрытие доходов, фальсификация финансовых отчетов, воровство наличных денег или других ценностей, использование фальшивых документов и т. д.;

3. Взятничество и коррупция: этот вид корпоративного мошенничества может привести к ущербу для компании не только в финансовом плане, но и в утрате репутации, клиентов и партнеров;

4. Ложное представление: в рамках корпоративного мира означает предоставление заведомо недостоверной информации или сокрытие фактов для получения выгоды или обмана другой стороны. Этот вид мошенничества может проявляться в различных формах, таких как ложные заявления о финансовом положении компании, завышенных прогнозах по доходам или сокрытии дефектов продукции;

5. Другие виды преступлений, направленных на экономическое обогащение за счет корпорации, ее сотрудников или клиентов.

Корпоративное мошенничество может быть связано с отдельными лицами, но также может быть организовано и систематизировано в рамках организации или корпоративной культуры, что делает его еще более опасным и распространенным. Это подчеркивает важность принятия эффективных мер для противодействия этому явлению внутри организаций и широкой общественности [3].

В зоне риска обычно находятся сферы, где сложно контролировать расходы организации:

- капитальное строительство;
- продажи;
- инвестиционные проекты;
- благотворительность;
- логистика;
- закупки и снабжение;
- финансы и операции с наличкой.

Корпоративное мошенничество можно классифицировать по различным признакам.

По отношению лица к компании:

-внутреннее — противоправные действия совершаются руководителями или сотрудниками компании;

-внешнее — противоправные действия совершают лица, не являющиеся сотрудниками компании, например, контрагенты или посторонние лица.

По характеру противозаконных действий:

-махинации с активами компании, сопровождающиеся их незаконным изъятием, включая фальсификацию финансовой отчетности, умышленное перевод финансовых средств на личные счета, и другие действия, направленные на незаконное обогащение за счет компании.;

-противоправные действия без хищения активов компании, такие как предоставление ложных сведений для трудоустройства, подделка документов, фальсификация результатов общих собраний акционеров, утечка конфиденциальной информации и другие манипуляции, целью которых является незаконное получение выгоды или нанесение ущерба предприятию.

Исследователи мошенничества разделяют корпоративное мошенничество на три основные категории:

- корпоративная коррупция;
- мошеннические действия с отчетностью;
- злоупотребление активами компании.

Основной причиной корпоративного мошенничества является стремление конкретного сотрудника извлечь для себя дополнительную выгоду за счет компании, независимо от возможного ущерба для нее. Человек совершает корпоративное мошенничество по разным причинам, которые могут быть связаны с его личными, финансовыми или психологическими обстоятельствами.

Во-первых, финансовые трудности могут побудить к мошенничеству. Например, если есть высокие долги, финансовые обязательства или неустойчивая финансовая ситуация, это может привести к желанию быстро получить деньги или обеспечить себе финансовую стабильность. Мошенничество представляется как способ решить эти проблемы, хотя это незаконно и вредно.

Во-вторых, чувство алчности и желание обогащения может играть роль в совершении корпоративного мошенничества. Некоторые люди испытывают неудержимое желание получить больше денег и материальных благ без учета этических и законных принципов. Они могут видеть в мошенничестве возможность быстрого обогащения или достижения личных целей.

Третьим мотивом может быть давление и стремление к успеху. Особенно в конкурентных организационных средах, где могут существовать высокие ожидания и жесткие требования к достижению результатов, некоторые люди могут чувствовать необходимость обмануть, подделать данные или совершить другие мошеннические действия, чтобы соответствовать этим ожиданиям или достичь успеха.

Кроме того, желание мести или возмездия может быть причиной мошенничества. Люди, чувствующие себя несправедливо или недостаточно вознаграждаемыми за свой труд, могут испытывать чувство обиды и желание навредить своей организации или своим коллегам, что приводит к мошенническим действиям [2].

Для сокращения риска корпоративного мошенничества компания должна работать над разработкой и внедрением комбинированных мер, включающих как реактивные, так и превентивные меры.

Превентивные меры или меры противодействия — это меры, направленные на предупреждение возникновения угроз и снижение риска корпоративного мошенничества.

Реактивные меры — это мероприятия, направленные на обнаружение и ликвидацию фактов корпоративного мошенничества либо на устранение его последствий после совершения преступления.

Для эффективного противодействия мошенничеству необходима практика выявления и противодействия. Основой этой практики является внедрение политик и процедур, направленных на предотвращение мошенничества. Первостепенное значение имеет создание системы внутреннего контроля, которая включает меры по обнаружению и предотвращению мошеннических действий [4].

Практика выявления корпоративного мошенничества включает использование различных методов и инструментов для обнаружения подозрительных действий и аномалий внутри организации. Ниже приведены несколько вариантов, которые часто используются для данной цели:

1. Анализ данных и аудит.

Это включает систематический анализ бухгалтерских данных, финансовых отчетов и других операционных данных организации. Аудиторы и аналитики проводят проверку на предмет несоответствий, неправильных операций и других указателей мошенничества.

2. Внутренний контроль и мониторинг.

Установление строгих процедур и стандартов внутреннего контроля может помочь выявить мошенничество. Это включает регулярную проверку различных бизнес-процессов, оценку рисков, внедрение автоматизированных систем контроля и мониторинга, а также анализ сигналов о нарушениях.

3. Анонимное сообщение и жалобы.

Создание механизмов для анонимного сообщения сотрудников о предполагаемых случаях мошенничества может содействовать выявлению проблем. Руководство организации должно обеспечить доверие и поддержку среди сотрудников, чтобы они чувствовали себя комфортно сообщать о подозрительной деятельности.

4. Внешние аудиты и экспертиза.

Регулярные внешние аудиты и проверки со стороны независимых экспертов также могут помочь выявить мошенничество. Это может включать анализ бухгалтерской отчетности, проведение комплексных проверок и расследований в случае подозрений.

5. Обучение и осведомленность сотрудников.

Эффективная программа обучения и повышения осведомленности для сотрудников может помочь предотвратить и выявить случаи мошенничества. Это может включать обучение о распознавании признаков мошенничества, процедурах сообщения о подозрительных действиях и этическим стандартам.

Важно применять комбинацию этих практик в рамках целостной стратегии противодействия мошенничеству [1].

Выделим основные методы противодействия корпоративному мошенничеству, хотя не существует универсального списка мероприятий, способных полностью и окончательно устранить проблему корпоративного мошенничества. Для предотвращения такой угрозы организациям следует уделить внимание следующим аспектам:

1. Разделение полномочий и финансовый контроль: операции должны подписывать несколько сотрудников, представляющих разные уровни управления в компании. Таким образом, каждая финансовая операция будет проходить через несколько утверждающих инстанций, что усложнит возможность совершения мошенничества.

2. Разработка и внедрение системы контроля и аудита, которая будет автоматически фиксировать и записывать все финансовые операции и действия пользователей в системе. Использование CRM или ERP систем с интегрированным сервисом проверки контрагентов поможет обеспечить более прозрачную и надежную работу. Важно установить четкие правила доступа и редактирования данных для определенного круга сотрудников, чтобы минимизировать риски несанкционированных действий.

3. Управление доступом к информации. Каждому сотруднику должен быть предоставлен доступ только к необходимым для работы данным. Необходимо внимательно отслеживать и обновлять список доступов для каждого сотрудника, чтобы избежать нежелательного использования ресурсов компании после увольнения.

4. Внедрение интеллектуальных систем мониторинга и аудита информации. Такие системы способны анализировать и контролировать служебную переписку, отслеживать отправку файлов, обнаруживать использование ключевых слов или фраз,

позволяя предотвратить утечку конфиденциальной информации или несанкционированные действия сотрудников.

5. Внедрение системы видеонаблюдения. Камеры видеонаблюдения являются важным инструментом для предотвращения кражи материальных ценностей. Однако важно помнить, что при использовании систем слежения необходимо соблюдать прозрачность и предупредить сотрудников о наличии таких систем в помещениях компании.

6. Тщательная проверка персонала. Особенно важна при назначении на должности с доступом к финансовым ресурсам и материальным ценностям.

7. Автоматизация учета рабочего времени сотрудников. Система отслеживания рабочего времени поможет контролировать соблюдение графика работы и предотвратить возможные случаи злоупотребления.

8. Мониторинг подозрительной активности сотрудников. Наблюдение за действиями сотрудников в выходные дни, проверка на предпочтение определенных деловых партнеров.

9. Контроль корпоративной атмосферы. Очень важно внимательно следить за обстановкой внутри команды. Постоянное недовольство сотрудников, будь то из-за низкой оплаты труда, излишних переработок, неудовлетворительных отношений и прочих причин, может способствовать возникновению проблем с корпоративной этикой и мошенничества внутри организации.

10. Прозрачная и справедливая система наказаний. Сотрудники, совершившие корпоративное мошенничество, должны быть наказаны в соответствии с установленными правилами и положениями организации. Все работники должны быть осведомлены о последствиях нарушений и уверены в том, что никакие привилегии или настроения руководителя не могут повлиять на процесс наказания.

11. Создание корпоративного кодекса этики. Цели компании и принципы поведения сотрудников должны быть четко определены в специальном документе, который будет руководителем использоваться для обучения и информирования персонала.

12. Пересмотр фонда оплаты труда и неденежная мотивация. Очень важно, чтобы зарплата сотрудников соответствовала рыночным стандартам и была справедливой. Низкий уровень оплаты труда может стимулировать сотрудников к незаконным действиям, включая корпоративное мошенничество. Если нет возможности увеличить заработную плату, можно рассмотреть возможности неденежной мотивации, такие как предоставление добровольного медицинского страхования, бесплатного парковочного места, компенсации части расходов на спорт и другие льготы. Повышение уровня удовлетворенности сотрудников может помочь предотвратить ситуации корпоративного мошенничества.

13. Проведение анализа контрагентов. Для обеспечения безопасности сделок необходимо тщательно изучить деловую репутацию и финансовое состояние потенциального контрагента. Для автоматизации этого процесса рекомендуется использовать специализированные сервисы, такие как АРІ Контур.Фокус, которые помогут проверить платежеспособность и общую надежность партнера.

Однако, не стоит забывать о том, что излишний контроль может негативно сказаться на атмосфере в коллективе и привести к ухудшению рабочих отношений.

Важно формировать корпоративную культуру, где работники чувствуют себя комфортно и могут обсуждать проблемы, а их мнение учитывается. Доверительные отношения и соблюдение правил безопасности помогают предотвращать мошенничество и создают благоприятную среду для работы.

Таким образом, корпоративное мошенничество является серьезной проблемой, которая может нанести значительный ущерб компаниям в виде финансовых потерь, потери репутации и доверия со стороны клиентов и партнеров. Эффективная борьба с корпоративным мошенничеством требует комплексного подхода: не только выявления и наказания нарушителей, но и создания этической культуры в организации, способствующей предотвращению подобных преступлений. Это включает в себя установление четких

правил и процедур, механизмов контроля и мониторинга, обучение сотрудников и поощрение честности и прозрачности.

Список источников

1. Алтухова Н.В. Количественная методика оценки аудитором риска мошенничества в аудируемой организации / Н. В. Алтухова, И. Н. Кулинич, О. А. Шпырко // Управленческий учет. - 2019. - № 11. - С. 68
2. Басова М. Е. Финансовое мошенничество / М. Е. Басова // Право и экономика. - 2020. - № 2. - С. 75.
3. Тарасов А. Н. Современные формы корпоративного мошенничества: практическое пособие / А. Н. Тарасов. — Москва : Издательство Юрайт, 2024. — 59с
4. Шульга И. Г. Как противодействовать мошенничеству / И. Г. Шульга // Стандарты и качество. - 2021. - № 1. - С. 68.
5. Шакирова Н.Н. Недобросовестные действия и аудит мошенничества//Актуальные вопросы современной экономики. 2022.- №12. С.744-753