Регламент

по предупреждению мошенничества (фрода)

**Москва, 202 г.**

**Содержание**

[1. Общие положения 3](#_Toc117590754)

[1.1 Цель документа 3](#_Toc117590755)

[1.2 Общие принципы 3](#_Toc117590756)

[2. Определение мошенничества и его характеристики 3](#_Toc117590757)

[2.1 Определение мошенничества 3](#_Toc117590758)

[2.2 Характеристики мошенничества 4](#_Toc117590759)

[3. Виды мошенничества 4](#_Toc117590760)

[3.1 Мошенничество Клиентов 4](#_Toc117590761)

[3.2 Незаконное присвоение активов 4](#_Toc117590762)

[3.3 Кража 5](#_Toc117590763)

[3.4 Мошенничество с финансовой отчетностью 5](#_Toc117590764)

[3.5 Финансовые инструменты 5](#_Toc117590765)

[3.6 Процесс управления мошенничеством 5](#_Toc117590766)

[3.7 Информационные источники при управления мошенничеством 5](#_Toc117590767)

[3.8 Процесс управления мошенничеством 6](#_Toc117590768)

[3.9 Индикаторы мошенничества 6](#_Toc117590769)

[3.10 Инструменты и техника идентификации и предупреждения фрода 7](#_Toc117590770)

[4. Управление мошенничеством 7](#_Toc117590771)

[4.1 Основные правила 7](#_Toc117590772)

[4.2 Роли и обязанности 7](#_Toc117590773)

[5. Механизмы внутреннего контроля 9](#_Toc117590774)

[5.1 Превентивный контроль 9](#_Toc117590775)

[5.2 Контроль подразделения безопасности 9](#_Toc117590776)

[5.3 Деятельность по контролю 9](#_Toc117590777)

[6. Информирование 10](#_Toc117590778)

[6.1 Основное 10](#_Toc117590779)

[6.2 Базовые принципы 10](#_Toc117590780)

[7. Отчетность 10](#_Toc117590781)

[7.1 Отчетность по мошенничеству 10](#_Toc117590782)

[7.2 Консолидация отчетности 10](#_Toc117590783)

[7.3 Информирование об факте мошенничества 10](#_Toc117590784)

[8. Контроль и ответственность 11](#_Toc117590785)

[8.1 Уровень контроля 11](#_Toc117590786)

# Общие положения

## Цель документа

### Регламент по предупреждению фрода (мошенничеству) определяет общие принципы и рекомендации для понимания принципов мошенничества в ООО «\_\_\_\_\_\_\_\_\_\_\_\_».

### Регламент разработан для развития механизмов внутреннего контроля, которые помогут в выявлении и предотвращении мошенничества. Целью регламента является содействие последовательному организационному внедрению руководящих принципов и распределению ответственности за разработку механизмов контроля и проведение расследований.

### Регламент применяется в отношении любых совершившихся или предполагаемых нарушениях, связанных с сотрудниками, а также акционерами, консультантами, поставщиками, подрядчиками и / или любыми другими третьими сторонами, имеющими деловые отношения с ООО «\_\_\_\_\_\_\_\_\_\_\_\_». Все необходимые следственные действия должны быть проведены без учета должностного положения правонарушителя, его должности или отношения к ООО «\_\_\_\_\_\_\_\_\_\_\_\_».

## Общие принципы

### Управление мошенничеством является неотъемлемой частью управления рисками и охватывает следующие мероприятия:

### предотвращения каких-либо мошеннических действий;

### выработка и внедрение мер по смягчению последствий при обнаружении мошенничества для устранения выявленных недостатков;

### расследование предотвращенных и выявленных случаев мошенничества с целью выявления организованных мошеннических групп и надлежащего взаимодействия с местными национальными правоохранительными органами.

### Управление мошенничеством позволяет выявлять бизнес-процессы, с повышенными признаками фрода, а также реагирование на ложный (фиктивный) инцидент. Посредством анализа реализованных случаев мошенничества управление ими позволяет сформировать предполагаемую модель нового вида, установить связи между сделками, клиентами, партнерами и, следовательно, выявить организованные мошеннические группы.

### В результате управление мошенничеством определяются и реализуются внутренние правила и меры по предотвращению мошенничества.

### Управление мошенничеством использует автоматизированные и ручные инструменты для предотвращения, обнаружения и расследования инцидентов.

### В случае выявления слабых мест в ООО «\_\_\_\_\_\_\_\_\_\_\_\_» или потенциального риска мошенничества, ООО «\_\_\_\_\_\_\_\_\_\_\_\_» или ее дочерняя компания должны принять соответствующие меры по исправлению положения для предотвращения таких случаев.

# Определение мошенничества и его характеристики

## Определение мошенничества

### Термин "мошенничество" обычно означает акт обмана, взяточничества, подлога, вымогательства, кражи, незаконного присвоения, ложного представления, заговора, коррупции, сговора, растраты, преднамеренного мошенничества или бездействия для обеспечения необоснованной личной выгоды.

### Мошенничество является нарушением доверия, которое, в целом, относится к умышленному деянию, совершенному с целью излечения личной или деловой выгоды.

### Хотя мошенничество может охватывать многие виды деятельности, этот регламент направлен главным образом на финансовые вопросы, которые могут быть юридически определены как мошенничество.

## Характеристики мошенничества

### Мотивация к совершению мошенничества.

### Мотивация к совершению мошенничества обычно относится к ситуационным мерам в виде потребности в деньгах, личного удовлетворения или сокрытия неэффективных управленческих решений.

### Возможность совершения мошенничества.

### Возможность совершения мошенничества означает наличие доступа к ситуации, когда мошенничество может быть совершено, например, слабость внутреннего контроля, потребности операционной среды, стили управления и корпоративная культура, низкий уровень обеспечения сохранности имущества компании, страх перед разоблачением, вероятностью обнаружения или неясные политики относительно того, что представляет собой приемлемое поведение.

### Возможность совершения мошенничества является самым простым и эффективным требованием для снижения вероятности мошенничества путем разработки эффективных систем внутреннего контроля с целью устранения возможностей совершения мошенничества.

### Личные характеристики мошенника.

### Личные характеристики означают готовность сотрудника, третьего лица к совершению мошенничества.

### Профессиональные навыки для совершения мошенничества могут иногда изменяться с помощью программ обучения и повышения осведомленности.

# Виды мошенничества

## Мошенничество Клиентов

### Кража личных данных - Клиент использовал свое имя, но умышленно предоставил ложные сведения о занятости, ложные доходы или скрытые адреса.

### Неудачная многофакторная аутентификация - Клиент не может правильно ответить на проблемы валидации и верификации или вопросы, заданные соответствующими сотрудниками ООО «\_\_\_\_\_\_\_\_\_\_\_\_».

### Захват счета - форма кражи личных данных, при которой мошенник получает полный доступ к существующему счету Клиента, например, к паролям и банковским реквизитам.

### Подготовленное мошенничество – Клиент имеет хорошую кредитную историю со своевременным погашением в течении времени, пока лимит не будет увеличен, затем выбирает его полностью и перестает погашать.

### Мошенничество с брокерами - происходит, когда сторонний агент, участвующий в процессе предоставления кредита, совершает мошенничество (например, брокеры поощряют клиентов к фальсификации информации при одобрении кредита или неспособности выполнить проверку идентификации клиента и, таким образом, позволяют мошенникам проскользнуть мимо внутреннего контроля и других механизмов, реализованных с единственной целью минимизировать вероятность попыток мошенничества стать успешным).

### Сговор - группа лиц, работающая совместно над организацией мошеннических схем.

### Жертва мошенничества - жертвой мошенничества является лицо, действовавшее добросовестно и подвергшееся мошенничеству в результате противоправных действий, совершенных другим лицом. С жертвой мошенничества можно связаться и сообщить об этом местным правоохранительным органам. Во всех остальных случаях мошенничество, будет классифицироваться как кражи личных данных.

## Незаконное присвоение активов

### Подделка, изменение или незаконное присвоение чеков, проектов, простых векселей или ценных бумаг.

### Несанкционированное приобретение, использование или распоряжение средствами, инвентарными запасами, мебелью, оборудованием, записями или другими активами.

## Кража

### Фальсификация табелей учета рабочего времени или записей о заработной плате, включая, но не ограничиваясь этим, неработающие часы, данные отчетности или руководитель, не позволяющий сообщать обо всех часах, отработанных почасовыми сотрудниками.

### Фальсификации командировочных и представительских расходов и / или использования иных документов финансовой отчетности для оплаты личных расходов.

### Фиктивная отчетность о поступлениях от поставщиков или отгрузках клиентам.

### Присвоение, принадлежащих группе компьютерное оборудование, программное обеспечение, данные или другие документы, в том числе нематериальные активы (например, конфиденциальная информация, коммерческая тайна, патенты и т. д.).

## Мошенничество с финансовой отчетностью

### Ненадлежащее управление фондом оплаты труда.

### Неправильное признание доходов для исчисления налогов.

### Завышение активов.

### Занижение обязательств.

## Финансовые инструменты

### Ложная информация, содержащаяся в кредитных документах (например, документы, удостоверяющие личность, занятость, доход и / или оценочные документы).

### Искажение залога в кредитных или иных документах.

## Процесс управления мошенничеством

### Главные принципы

### В связи с разнообразием бизнес-моделей и рынков, на которых работает ООО «\_\_\_\_\_\_\_\_\_\_\_\_», настоящий Регламент по предупреждению мошенничества не должен рассматриваться как исчерпывающий документ с точки зрения видов мошенничества и / или механизмов их идентификации, оценки и контроля.

### Настоящий Регламент обеспечивает руководство минимальными требованиями для разработки мероприятий по борьбе с мошенничеством и мер, учитывающих специфику бизнес-процессов.

### Каждый сотрудник должен проявлять должную осмотрительность по отношению ко всем новым контрагентам и должную осмотрительность по всем новым операциям для выявления возможных проблем соответствия или добросовестности.

## Информационные источники при управления мошенничеством

### Интеграция с внешними источниками данных должна осуществляться с максимально возможным числом различных поставщиков (где это применимо), с тем чтобы свести к минимуму вероятность мошенничества со стороны клиентов.

### Бюро кредитных историй – целесообразно использовать для подтверждения личности клиента и его кредитной истории.

### Формирование баз данных "черного списка" и базы данных "списка мошенничества" - используется для подтверждения того, что клиент не имел ранее отношения к зарегистрированным фактам мошенничества (если это применимо, и никаких юридических препятствий для их использования не существует).

### Проверка работодателей Клиента – подтверждения реального наличие работодателя и его юридический статус (например, активный статус, при ликвидации и т. д.).

### Следует стремиться к интеграции с внешними источниками данных, если выгоды от использования такой услуги перевешивают затраты на нее.

### Рекомендуется разрабатывать свои собственные мошенничества-механизмы обнаружения и сообщать о риск-факторах, в письменной форме и предоставлять факты, аргументы, если они не соответствуют требованиям и ожиданиям, изложенным в этом документе.

### Следует разработать и использовать механизмы внутреннего контроля в целях предотвращения мошенничества и минимизации негативных последствий.

## Процесс управления мошенничеством

### Процесс управления мошенничеством для онлайн-операций.

### Валидация персональных данных клиента из регистрационной формы, включая правильную перекрестную проверку данных во внешних базах данных, валидацию данных с использованием статистических алгоритмов и предопределенных форматов полей.

### Проверка сообщений для обеспечения неразглашения любой конфиденциальной информации о мошенничестве.

### Мониторинг и оценка поведения в интернете с помощью дактилоскопии устройства и IP-адрес и географическое расположение номеров.

### Внутренний мониторинг и анализ качества черного списка.

### Регулярное обновление политики и руководящих принципов на основе фактических ситуаций из практики или выявленных пробелов во внутренней политике и процессах в ходе регулярной оценки.

### Проведение оценки эффективности, регулярное обучение и обратную связь в тех областях, где требуется улучшение.

### Процесс управления мошенничеством для автономных операций.

### Предоставление четких инструкций в повседневной деятельности, обеспечение обучения сотрудников по выявлению попыток мошенничества и мошеннических схем.

### Регулярная оценка качества клиентов со стороны партнеров, партнеров и партнеров, применяющих различные стратегии для клиентов (если применимо).

### Общение с представителями партнеров- жертв мошенничества и определение объемов мошеннических кредиты на ежемесячной основе и т. д.

## Индикаторы мошенничества

### Показатели мошенничества относятся к одной из двух категорий:

### Предупреждающие знаки:

### отсутствия антифрод-политики и культуры;

### неспособность руководства внедрить надежную систему внутреннего контроля и / или продемонстрировать приверженность ей;

### неадекватность процессов набора сотрудников и отсутствие проверки кандидатов;

### работники, работающие в нерабочее время без присмотра;

### работники, не использующие ежегодный отпуск в соответствии с графиком отпусков.

### нежелание сотрудников разделять функциональные обязанности;

### отсутствие отчетов и проделанной работе и независимой проверки ключевых операций и т. д.;

### предупреждения о мошенничестве-конкретные события или красные флаги, которые могут свидетельствовать о мошенничестве:

### анонимные электронные письма / телефонные звонки;

### электронные письма, отправленные в необычное время, с ненужными вложениями;

### фотокопии документов вместо оригиналов;

### факсимильные и / или штамповые подписи вместо оригиналов;

### выше среднего числа неудачных попыток входа в систему;

### систематическая деятельность вне обычных рабочих часов или от пределов нормальной области работы и т. д.

## Инструменты и техника идентификации и предупреждения фрода

### Обучение сотрудников на рабочем месте является отправной точкой для реализации эффективной политики борьбы с мошенничеством. Второй момент - сотрудники должны иметь необходимое понимание, что всегда есть возможность для совершения мошенничества.

### Регулярно обновлять процедуры предупреждения мошенничества, используемые инструменты, причины реализации.

### Доводить до сотрудников информацию о нарушениях, причинах, признаках мошенничества. вызывающих подозрения.

### Извлекать уроки из опыта каждого выявленного случая мошенничества или попытки мошенничества, в том числе по результатам проведенных расследований.

### Формирование единого информационного массива признаков фактов мошенничества, включая тех, которые были совершены уволенными сотрудниками, по которым истек срок давности или иным образом не расследованы необходимые мероприятия.

### Системный анализ - важно изучить существующие системы и выявить любые слабые места, которые могут предоставить мошеннику возможность использовать их.

###  Бенч-маркировка - сравнение одного финансового периода с другим или эффективность одного центра затрат или бизнес-единицы с другим; или сравнение общей эффективности бизнеса с отраслевыми стандартами-все это может выявить аномалии, заслуживающие дальнейшего изучения.

# Управление мошенничеством

## Основные правила

### Разделение ответственности за управление рисками мошенничества может отличаться в региональных отделениях в зависимости от размера, рыночных операций и бизнес-моделей.

## Роли и обязанности

### Роль Корпоративного центра.

### Разработка и обеспечение реализации политики управления мошенничеством.

### Определение Ключевые показатели эффективности и установление целевых показателей для мониторинга эффективности управления рисками мошенничества группы.

### Оценка рисков мошенничества нового продукта, процесса или существенных изменений существующих продуктов или процессов до запуска. Если оценка окажется неприемлемой, обеспечивает принятие соответствующих мер для снижения рисков до приемлемого уровня.

### Информационные системы / информационные персонал-технологии.

### Могут предоставлять технические консультации по ИТ-безопасности, возможностям, обеспечивать авторизованный доступ, устанавливать роли в соответствии с должностными обязанностями пользователя и, таким образом, поддерживать разделение обязанностей.

### Если компьютеры были использованы для совершения мошенничества или если они необходимы для доказательной информации, необходимо немедленно обратиться за консультацией к специалисту.

### Руководители подразделений.

### Учитывая свой предыдущий опыт работы на тех же или аналогичных карьерных должностях, руководители подразделений несут ответственность за выявление мошенничества и других нарушений в сфере их ответственности.

### Разрабатывают, внедряют и организуют мониторинг системы (систем) внутреннего контроля (систем) для предотвращения мошенничества-качества, эффективности и экономической эффективности – и инициирование предложений по совершенствованию процесса, когда это необходимо.

### Проводят анализ, оценивают и используют статистическую информацию, чтобы разрабатывать и осуществлять действия, оказывающие положительное влияние на прибыль и убыток.

### Исследуют учетные записи, отображающие подозрительную деятельность, помеченную автоматическим обнаружением (если это возможно), группами идентификации руководства по обслуживанию клиентов или группами по взысканию долгов.

### Проводят аудит мошенничества во время командировок, осуществляют планирование и проведение аудитов, анализ результатов, представление отчетов в Корпоративный центр.

### Сотрудничают с руководителем подразделения по работе с Клиентами для организации и контроля процесса идентификации вручную.

### Разрабатывают и организовывают подготовку по вопросам предупреждения мошенничества для групп по ручной идентификации.

### Организовывают взаимодействие с компаниями-партнерами по восстановлению зарегистрированных и подтвержденных случаев мошенничества.

### Финансовый директор (если применимо).

### Финансовый директор часто несет общую ответственность за подготовку отчета по влиянию мошенничества финансовые результаты.

### Руководитель подразделения безопасности.

### Несет ответственность за инициирование, организацию и проведение расследований по фактам мошенничества.

### Отвечает за реализацию плана реагирования на мошенничество и за любые действия, требующие принятия последующих мер.

### Руководит любыми внутренними расследованиями.

### Организует коммуникацию со всеми заинтересованными сторонами как внутренними, так и внешними.

### Сотрудники компании.

### Подразделение по работе с персоналом несет ответственность за любые внутренние дисциплинарные процедуры.

### Рекомендации Подразделение по работе с персоналом должны учитывать профессиональную подготовку сотрудников, их трудовой стаж, а также вопросы, касающиеся трудового права и т. д.

### Внутренние ревизоры, аудиторы (если это применимо).

### На отдел внутреннего аудита, возлагается задача выявления любых случаев мошенничества.

### Необходимость назначения ревизоров, аудиторов, специалистов по мошенничеству определяется руководителем компании.

# Механизмы внутреннего контроля

## Превентивный контроль

### Превентивный контроль - попытка удержать или предотвратить нежелательные события из происходящих (т. е. они помогают предотвращать потери).

### Профилактические меры контроля имеют важное значение, поскольку они являются упреждающими и подчеркивают качество.

## Контроль подразделения безопасности

### Контроль подразделения безопасности направлен на обнаружение нежелательных действий. Они предоставляют доказательства того, что произошла потеря, но не препятствуют ее возникновению.

### Контроль подразделения безопасности играет важнейшую роль, предоставляя доказательства того, что превентивные меры контроля функционируют и предотвращают потери.

## Деятельность по контролю

### Мероприятия по контролю включают, но не ограничиваются:

### Утверждения, разрешения и проверки (превентивные) – руководство уполномочивает получателей выполнять определенные действия и совершать определенные операции в пределах предельных параметров. Кроме того, руководство определяет те виды деятельности или операции, которые нуждаются в надзорном одобрении до того, как они будут выполнены или выполнены сотрудниками. Утверждение руководителя (ручное или электронное) означает, что он или она проверили и подтвердили, что деятельность или операция соответствует установленным правилам и процедурам.

### Проверка - сотрудник связывает различные наборы данных друг с другом, выявляет и расследует различия и при необходимости принимает меры по исправлению положения.

### Обзоры эффективности (текущий) - руководство сравнивает информацию о текущей работе с бюджетами, прогнозами, предыдущими периодами или другими критериями, чтобы измерить степень достижения целей и задач и определить неожиданные результаты или необычные условия, требующие последующих действий.

### Безопасность активов (превентивный и текущий) – доступ к оборудованию, инвентарным запасам, услугам, наличным средствам и прочим активам ограничен; активы должны периодически учитываться и сравниваться с суммами, показанными на контрольных записях.

### Разделение обязанностей (превентивный) - обязанности разделяются между различными людьми, чтобы изменить риск ошибки (ошибок) или ненадлежащего действия(действий). Обязанности по санкционированию операций, регистрации операций (учета) и обработке соответствующего актива (хранения) разделены.

### Контроль за информационными системами (профилактические и текущие).

### Общие элементы управления - включают в себя управление операциями центра обработки данных, освоение и обслуживание системного программного обеспечения, доступ, безопасность, а также разработку и обслуживание прикладных систем.

### Средства управления приложениями-включают в себя запрограммированные шаги в прикладном программном обеспечении, такие как компьютерное согласование и проверка редактирования. Они призваны помочь обеспечить полноту и точность обработки транзакций, авторизацию и валидность.

# Информирование

## Основное

### Информирование в ООО «\_\_\_\_\_\_\_\_\_» призвано облегчить всем сотрудникам возможность добросовестно сообщать о нарушениях, не опасаясь, что их действия могут иметь неблагоприятные последствия.

### Информирование направлено на повышение прозрачности контрольных процедур в ООО «\_\_\_\_\_\_\_\_\_» и поддержку ее системы борьбы по предупреждению мошенничества с практикой, которая может нанести ущерб ее деятельности и / или репутации.

## Базовые принципы

### Заинтересованные лица должны иметь выбор между различными каналами для информирования и связи.

### Сотрудники ни при каких обстоятельствах не должны подвергаться репрессиям за разглашение информации (т. е. сотрудники, добросовестно сообщающие об инцидентах, должны быть защищены, а их личность, насколько это возможно, должна оставаться конфиденциальной).

### Сообщения об инцидентах проверяются надлежащим образом, и, если они подтверждены, в Корпоративном центре предпринимаются все необходимые шаги для выявления соответствующих средств правовой защиты.

# Отчетность

## Отчетность по мошенничеству

### Информация по фактам мошенничества и отчеты отправляются в \_\_\_\_\_\_\_\_\_\_\_\_ (указывается либо подразделение, либо должностное лицо) на специальный адрес электронной почты.[[1]](#footnote-1)

### Региональные менеджеры и уполномоченные ими сотрудники несут ответственность за своевременность предоставления отчетности о риске мошенничества для каждого продукта, сотрудника, клиента, инициации кредита и кредитного возврата в соответствии с предусмотренным шаблоном.

### Отчетность в Корпоративный центр направляется со следующей периодичностью:

### территориальное подразделение - модель риска о попытки мошенничества / происшествия, как только она была определена с кратким описанием того, что произошло, какие дальнейшие шаги следует предпринять, чтобы расследовать это, по оценкам финансовых последствий для предприятия, и предложены пути смягчения негативных финансовых последствий.

### территориальное подразделение готовит ежемесячный отчет о мошенничестве для своих целей.

### в случае отсутствия попыток мошенничества / инцидентов в течение отчетного периода территориальное подразделение в докладе должно указать, что такой попытки не было.

## Консолидация отчетности

### После получения отчетов от всех филиалов, подготовка управленческих консолидированных отчетов на уровне Корпоративного центра осуществляется \_\_\_\_\_\_\_\_\_\_\_\_ (указывается либо подразделение, либо должностное лицо).

## Информирование об факте мошенничества

### Шаблон доклада о факте мошенничества должен содержать:

### Название региона, адрес;

### Сроки мошеннической деятельности;

### Подробное описание мошеннической деятельности;

### Подозреваемый мошенник и другая соответствующая информация;

### Причины совершения мошенничества;

### Признаки совершения мошенничества.

### Информирование о факте мошенничества осуществляется по электронной почте на специальный адрес, который передается всем подразделениям компании с предоставлением всех необходимых данных, которые будут использоваться при проведении расследования в случае, если он или она сообщает.

# Контроль и ответственность

## Уровень контроля

### Все руководители подразделений, региональных отделений ознакамливаются с настоящим Регламентом, а также затем несут ответственность за ознакомление своих подчиненных.

### Каждое подразделение, региональное отделение (филиал) внедряет разработанный регламент не позднее чем в течение 2 (двух) месяцев с даты его утверждения.

1. Адрес электронной почты целесообразно передать всем руководителям вместе с шаблоном отчета и сроками его представления. [↑](#footnote-ref-1)