

Утверждено и рекомендовано к  
применению аудиторами Комитетом СРО  
ААС по противодействию коррупции  
легализации (отмыванию) доходов,  
полученных преступным путем, и  
финансированию терроризма  
Протокол от 22 декабря 2025 г. № 166

## **РАЗЪЯСНЕНИЯ ПО ВОПРОСАМ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА ПРИ ОКАЗАНИИ АУДИТОРСКИХ УСЛУГ ИТ-ОРГАНИЗАЦИЯМ**

### **1. Сфера применения**

Данные разъяснения направлены на вопросы требований Международных Стандартов Аудита (МСА) по рассмотрению соблюдения законодательства о противодействии ОД/ФТ/ЭК/ФРОМУ. На уровне стандартов аудиторской деятельности рассмотрение соблюдения законодательства по ПОД/ФТ/ЭК/ФРОМУ регламентируется, главным образом, МСА 240 «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» и МСА 250 (пересмотренным) «Рассмотрение законов и нормативных актов в ходе аудита финансовой отчетности».

Исходя из Федерального закона от 07 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Закон 115-ФЗ), при оказании аудиторских услуг аудиторские организации, индивидуальные аудиторы обязаны уведомлять Росфинмониторинг о любых основаниях полагать, что сделки или финансовые операции аудируемого лица осуществляются или могут быть осуществлены в целях ПОД/ФТ.

Обязанность уведомлять Росфинмониторинг также распространяется на аудиторские организации и индивидуальных аудиторов в случаях, когда при оказании прочих связанных с аудиторской деятельностью услуг они готовят или осуществляют от имени или по поручению своего клиента следующие операции с денежными средствами или иным имуществом:

- сделки с недвижимым имуществом;
- управление денежными средствами, ценными бумагами или иным имуществом клиента;
- управление банковскими счетами или счетами ценных бумаг;
- привлечение денежных средств для создания или обеспечения деятельности юридических лиц и иных организаций, иностранных юридических лиц и иностранных структур без образования юридического лица, а равно для управления ими;
- создание или обеспечение деятельности юридических лиц и иных организаций, иностранных юридических лиц и иностранных структур без образования юридического лица, а равно управление ими;
- купля-продажа юридических лиц, иностранных юридических лиц и иностранных структур без образования юридического лица.

### **2. ИТ организации и организация контроля в сфере ПОД/ФТ/ФРОМУ**

Исходя из сложившейся практики ИТ-организация – это организация, которая занимается информационными технологиями и предоставляет широкий спектр услуг по поддержке компьютерных систем и сетей. ИТ-организации занимаются разработкой компьютерного программного обеспечения (ПО), баз данных, различных информационных ресурсов, приложений, компьютерных игр; оказывают техническую поддержку пользователям этих ресурсов и т.д.

В соответствии с Постановлением Правительства Российской Федерации от 30 сентября 2022 года № 1729 перечень видов деятельности в области информационных технологий утвержден Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 11 мая 2023 года № 449.

Государственная аккредитация организаций, осуществляющих деятельность в области информационных технологий, проводится с целью оказания таким организациям государственной поддержки.

Виды деятельности, связанные с использованием вычислительной техники и информационных технологий, приведены в разд. 62 - 63 ОКВЭД 2. Из них к видам деятельности, которые организация должна осуществлять для получения государственной аккредитации, относятся следующие:

- 62.01 "Разработка компьютерного программного обеспечения";
- 62.02 "Деятельность консультативная и работы в области компьютерных технологий";
- 62.02.1 "Деятельность по планированию, проектированию компьютерных систем";
- 62.02.4 "Деятельность по подготовке компьютерных систем к эксплуатации";
- 62.03.13 "Деятельность по сопровождению компьютерных систем";
- 62.09 "Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая";
- 63.11.1 "Деятельность по созданию и использованию баз данных и информационных ресурсов".

К мерам господдержки относятся:

- 1) возможность применять пониженную ставку по налогу на прибыль (п. 1.15 ст. 284 НК РФ);
- 2) возможность уплачивать страховые взносы по единым пониженным тарифам (пп. 3 п. 1, п. 2.2-1 ст. 427 НК РФ).

Также к мерам господдержки относятся льготное кредитование и предоставление грантов аккредитованным ИТ-организациям. Из федерального бюджета ежегодно выделяются средства для предоставления грантов на перспективные разработки отечественных ИТ-решений.

Постановлением Правительства Российской Федерации от 5 декабря 2019 года № 1598 утверждены Правила предоставления из федерального бюджета субсидий в целях обеспечения льготного кредитования проектов по цифровой трансформации, реализуемых на основе российских решений в сфере информационных технологий. Например, аккредитованные ИТ-организации могут получить льготные кредиты если они обеспечивают разработку программных продуктов, программного обеспечения, сервисов и платформенных решений в сфере информационных технологий.

### **3. Национальная оценка рисков**

Результаты национальной оценки рисков ОД/ФТ/ФРОМУ (далее – НОР) содержат ключевые риски, угрозы и уязвимости, характерные для Российской Федерации. Эти результаты изложены в Отчетах о национальной оценке рисков легализации (отмывания) преступных доходов и Отчетах о национальной оценке рисков финансирования терроризма, размещенных на официальном Интернет-сайте Росфинмониторинга.

В отчете о НОР преступления в сфере информационно-коммуникационных технологий отнесены к ключевым угрозам. В НОР подчеркивается, что развитие информационных технологий является одной из приоритетных задач обеспечения государственной политики во всех сферах деятельности. Однако по мере развития информатизации возрастают и угрозы совершения преступлений в киберпространстве. При этом среди деяний в указанной сфере НОР выделяет получение неправомерного доступа к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Целями совершения таких преступлений является взлом систем информационной безопасности и хищение персональных данных и платежных реквизитов, а также распространение противоправной информации.

Результаты НОР могут быть использованы в процессе получения аудитором понимания аудируемого лица и его окружения, в частности, для выявления и оценки соответствующих рисков и планирования ответных действий. Основные уязвимые места и риски ОД/ФТ/ЭК/ФРОМУ, описанные в результатах НОР, целесообразно использовать в качестве индикаторов для определения областей повышенного аудиторского риска при планировании аудита и идентификации рисков, которые требуют особого внимания.

НОР не содержит специфических рисков, угроз и уязвимостей, связанных именно с ИТ-организациями. Однако при изучении деятельности аудируемого лица, относящегося к ИТ-организациям, следует обратить внимание на описанные в результатах НОР угрозы в сфере осуществления переводов под видом оплаты услуг и займов, в сфере бюджетных отношений, в сфере трансграничных переводов, а также в области коррупционных нарушений.

При приеме на обслуживание ИТ-организации, в процессе получения понимания её деятельности и системы внутреннего контроля, необходимо оценить, насколько риски, описанные в результатах НОР, присущи деятельности аудируемого лица, и выделить значительные виды операций и области, в которых возможно появления рисков ОД/ФТ/ЭК/ФРОМУ. Риски ОД/ФТ/ЭК/ФРОМУ, включенные в группы высокого, повышенного и умеренного риска в результатах НОР, следует отнести к ключевым областям аудита.

#### **4. Принятие и продолжение отношений с клиентом, изучение клиента, выявление подозрительных операций**

Аудитор должен рассмотреть вопрос, является ли значимой для выявления рисков ОД/ФТ информация, полученная при выполнении аудитором процедуры принятия или продолжения отношений с клиентом. Оценка честности и деловой репутации клиента или потенциального клиента проводится на основании общедоступной информации (например, в сети Интернет); информации, полученной из предыдущего опыта его работы с клиентом; также возможно направление запросов лицам, которые, по мнению аудитора, могут владеть информацией о деловой репутации клиента.

Помимо предусмотренных МСА процедур до приема на обслуживание нового клиента или до начала очередного задания с ранее принятым клиентом необходимо провести процедуры по **идентификации** клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев, а также необходимо проверить достоверность сведений, т.е. провести их верификацию.

Кроме того, следует убедиться, что клиент, его бенефициарные владельцы, выгодоприобретатели, представители клиента не включены в следующие перечни в личном кабинете аудиторской организации на официальном сайте Росфинмониторинга:

- Перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму;
- Перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к распространению оружия массового уничтожения;
- Перечень лиц, в отношении которых действует решение межведомственной комиссии по противодействию финансированию терроризма о замораживании (блокировании) принадлежащих им денежных средств или иного имущества (далее – Перечни).

К признакам необычных сделок, выявляемых при оказании аудиторских услуг ИТ-организациям, обычно можно отнести следующие:

**1101** Запутанный или необычный характер сделки, не имеющей очевидного экономического смысла или очевидной законной цели;

**1189** Совершение операций (сделок) с юридическим лицом или индивидуальным предпринимателем, период деятельности которых с даты государственной регистрации составляет менее 1 года;

**1290** Совершение операции (сделки) по поручению клиента в случае, когда клиент, учредитель или выгодоприобретатель является участником федеральных, региональных либо муниципальных целевых программ или национальных проектов;

**1291** Совершение операции (сделки) по поручению клиента в случае, если имеются основания полагать, что клиент, учредитель, бенефициарный владелец или выгодоприобретатель является получателем субсидий, грантов или иных видов государственной поддержки за счет средств федерального бюджета, бюджета субъекта РФ или муниципального бюджета;

**1390** Совершение операции (сделки) в случае, когда клиент, его контрагент, представитель клиента, бенефициарный владелец, выгодоприобретатель или учредитель клиента зарегистрирован в государстве или на территории, предоставляющем(щей) льготный режим налогообложения и (или) не предусматривающем(щей) раскрытия и предоставления информации при проведении финансовых операций (офшорной зоне) либо его счет открыт в банке, зарегистрированном в указанном государстве или на указанной территории;

**1590** Предоставление или получение займа, процентная ставка по которому ниже ставки рефинансирования, устанавливаемой Банком России;

**1591** Получение займа от нерезидента и (или) предоставление займа нерезиденту;

**1804** В договоре (контракте) предусмотрены экспорт резидентом товаров (работ, услуг), либо платежи по импорту товаров (работ, услуг) в пользу нерезидента, зарегистрированного в государстве или на территории, предоставляющем(щей) льготный режим налогообложения и (или) не предусматривающем(щей) раскрытия и предоставления информации при проведении финансовых операций (офшорной зоне);

**1882** Перечисление денежных средств в адрес нерезидента по внешнеторговым сделкам, связанным с оказанием информационно-консультативных и маркетинговых услуг, передачей результатов интеллектуальной деятельности, в том числе исключительных прав на них, и других видов услуг нематериального характера;

**1883** Перечисление денежных средств в адрес нерезидентов в рамках платежей за пользование исключительными правами на программные продукты, товарные знаки, ноу-хау;

**4901** Операции (в том числе со связанными сторонами), выходящие за рамки обычной деятельности, или со связанными сторонами, которые не аудируются или аудируются другой аудиторской организацией, в том числе приводящие к выводу средств и активов аудируемого лица;

**4905** Завышение или занижение сумм в счетах за товары и услуги.

## **5. Уведомление Росфинмониторинга**

Аудиторским организациям, индивидуальным аудиторам при оказании аудиторских услуг ИТ-организациям при возникновении любых оснований полагать, что сделки или финансовые операции аудируемого лица могли или могут быть осуществлены в целях ОД/ФТ/ЭК/ФРОМУ, в соответствии с п. 2.1 ст. 7.1 Закона 115-ФЗ и п. 3.2 ч.2 ст. 13 Федерального закона от 30 декабря 2008 года № 307-ФЗ «Об аудиторской деятельности» необходимо уведомить об этом Росфинмониторинг.

**Председатель Комитета по противодействию коррупции и легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма СРО ААС**

**К.Ю.Н.**

**В.В. Бутовский**