



Доклад ФАТФ

Кибермошенничество

Цифровизация и риски отмывания денег,
финансирования терроризма и финансирования
распространения оружия массового уничтожения



Февраль, 2026



Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) — независимый межправительственный орган, который разрабатывает и продвигает политику, направленную на защиту глобальной финансовой системы от отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ признаны глобальным стандартом в сфере противодействия отмыванию доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения. Для получения дополнительной информации о ФАТФ посетите сайт: www.fatf-gafi.org.

Настоящий документ и/или любые включенные в него карты не затрагивают статус или суверенитет какой-либо территории, делимитацию международных границ и рубежей, а также наименование любой территории, города или района.

Неофициальный перевод выполнен МУМЦФМ

Ссылка для цитирования:

ФАТФ – (2026), Кибермошенничество — цифровизация и риски отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения, ФАТФ, Париж, Франция, www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html

© 2026 ФАТФ/ОЭСР. Все права защищены.

Никакое воспроизведение или перевод данной публикации не допускается без предварительного письменного разрешения. Заявки на получение такого разрешения, полностью или частично в отношении данной публикации, следует направлять в:

Секретариат ФАТФ, 2 rue André Pascal 75775 Paris Cedex 16, Франция; e-mail: contact@fatf-gafi.org

Предпосылки

Настоящий документ является результатом продолжающейся работы ФАТФ по оценке рисков, возникающих в связи с цифровизацией, прогнозированию и повышению осведомленности о текущих и потенциальных рисках и угрозах, связанных с кибермошенничеством, а также рассмотрению необходимости дальнейших действий. Документ отражает поэтапный подход ФАТФ, направленный на выявление и разъяснение текущих рисков и уязвимостей ОД/ФТ/ФРОМУ в области новых технологий.

Документ предназначен для повышения осведомленности компетентных органов, финансовых учреждений (ФУ), провайдеров услуг виртуальных активов (ПУВА), установленных нефинансовых предприятий и профессий (УНФПП) и других заинтересованных сторон, а также для содействия разработке эффективных регуляторных и операционных мер реагирования в рамках глобальной системы ПОД/ФТ/ФРОМУ. В документе рассматривается взаимосвязь кибермошенничества с рядом Рекомендаций ФАТФ и демонстрируется приверженность ФАТФ стимулированию обсуждения новых тем и развитию перспективного взаимодействия по данной проблематике.

Введение

Кибермошенничество стало одной из наиболее распространенных и разрушительных форм преступлений, приносящих значительные объемы незаконных доходов посредством обмана людей по всему миру. Быстрое внедрение цифровых технологических инноваций во время и после пандемии COVID-19 ускорило развитие мошенничества, обеспечив более быстрое перемещение денежных средств и появление все более сложных схем социальной инженерии. С одной стороны, новые технологии повышают эффективность экономики и финансовых систем по всему миру, развивают инновации и расширяют финансовую доступность. С другой стороны, цифровые технологические инновации существенно расширили масштабы, скорость и сложность мошенничества, все чаще позволяя злоумышленникам действовать трансгранично и использовать цифровые платформы, системы мгновенных платежей и новые технологии.

Часть I: Растущая угроза и последствия кибермошенничества

Мошенничество в цифрах: быстро растущая угроза

В рамках продолжающейся работы ФАТФ по оценке рисков представители правоохранительных органов, подразделений финансовой разведки (ПФР), органов, формирующих политику, и другие эксперты в сфере незаконных финансов продолжают анализировать мошенничество и обмениваться примерами из практики и данными, демонстрирующими масштаб и эволюционирующий характер кибермошенничества в их юрисдикциях. В совокупности эти материалы формируют тревожную картину того, как кибермошенничество усиливается и адаптируется в различных регионах.

Сто пятьдесят шесть, или 90% оцененных юрисдикций¹, прямо указывают мошенничество как значительный риск отмывания денег. Масштабы мошенничества продолжают расти. Например, только в Сингапуре число случаев кибермошенничества (мошеннических схем) увеличилось на 61% за два года². В Соединенном Королевстве мошенничество в настоящее время составляет более 40% всех преступлений. В ряде стран оценивается, что до 15% взрослого населения становились жертвами кибермошенничества, что подчеркивает широкий масштаб и растущий характер этой угрозы. Хотя общий объем потерь от мошенничества, включая ущерб, причиненный физическим лицам, предприятиям и государственным финансам, невозможно точно определить, только в Соединенных Штатах Америки он составляет как минимум десятки миллиардов долларов ежегодно.

Факторы, способствующие кибермошенничеству

Технологические инновации стали движущей силой экономического и социального прогресса. Однако эти же инновации снизили порог входа, расширили охват и позволили кибермошенникам расширить свою деятельность. Многие финансовые и нефинансовые услуги стремительно перешли в онлайн-среду в период пандемии COVID-19.

Как отмечается в совместной публикации ФАТФ, Группы «Эгмонт» и ИНТЕРПОЛ за 2023 год [о незаконных финансовых потоках, связанных с кибермошенничеством](#), такие преступления демонстрируют стремительный рост, обусловленный развитием новых технологий, включая искусственный интеллект и технологии «дипфейк» на основе искусственного интеллекта. Эти технологии расширяют возможности преступников использовать фишинговые электронные письма, поддельные веб-сайты, рекламу в социальных сетях, приложения для обмена сообщениями и другие цифровые инструменты для совершения мошенничества дистанционно и в массовом масштабе.

Развитие финансовой инфраструктуры также затруднило борьбу с мошенничеством. Растущее использование виртуальных активов, а также каналов мгновенных и трансграничных платежей при недостаточности специализированных мер по снижению рисков позволяет переводить преступные доходы до их выявления (в случае, если компетентные органы не смогут выявить такие операции и вмешаться в течение очень короткого периода времени).

¹ 176 стран, опубликованных и рассмотренных на момент проведения анализа в июне 2025 года.

² [Ежегодный отчет Сингапура о мошенничестве и киберпреступности за 2024 год](#).

Ситуацию усугубляют и трудности обмена информацией и международного сотрудничества, поскольку компетентные органы и участники частного сектора вынуждены действовать в рамках правовых, процедурных и юрисдикционных ограничений, тогда как преступники не скованы этими обстоятельствами. Например, преступники все чаще требуют оплату непосредственно в криптовалюте или быстро конвертируют полученные средства в криптовалюту, чтобы избежать возврата активов, в то время как отслеживание таких средств требует времени и ресурсов.

Во многих случаях масштабные схемы кибермошенничества осуществляются или поддерживаются транснациональными преступными группировками и управляются через специализированные «мошеннические центры» (или комплексы).

Такие центры часто являются частью более широких преступных систем, где они пересекаются с другими видами преступной деятельности, такими как профессиональные услуги по отмыванию денег, торговля людьми и связанные с ней нарушения прав человека, наркоторговля, а также другие серьезные уголовные преступления³.

Страны отмечают, что все большее число схем кибермошенничества изначально включает механизмы отмывания денег, используя номинальные счета, сети денежных мулов, торговлю банковскими и криптовалютными счетами, а также быстрое перемещение денежных средств через финтех-платформы. Это размывает границы между мошенничеством, незаконными финансовыми услугами и отмыванием денег.

³ Источник: [США и Соединенное Королевство провели крупнейшую в истории операцию против киберпреступных сетей в Юго-Восточной Азии | Министерство финансов США](#).

Часть II: Использование стандартов ФАТФ для противодействия кибермошенничеству

Борьба ФАТФ с кибермошенничеством

В отчете ФАТФ за 2023 год [о незаконных финансовых потоках, связанных с кибермошенничеством](#) было отмечено, что кибермошенничество в последние годы растет в геометрической прогрессии. С этого времени масштаб зарегистрированных случаев мошенничества и их географическое распространение значительно увеличились.

В рамках работы по противодействию кибермошенничеству ФАТФ предпринимает значительные меры, которые могут помочь странам и финансовым учреждениям выявлять и предотвращать происхождение и перевод преступных доходов.

Прозрачность платежей

В ответ на развитие инфраструктуры ОД, включая пиринговые транзакции и децентрализованные финансовые системы, ФАТФ повышает прозрачность платежей. Это имеет ключевое значение для отслеживания преступных доходов от мошенничества (например, через механизмы «подтверждения получателя»), а также для сокращения возможностей преступников перемещать средства анонимно или через нерегулируемых посредников.

Особо важную роль играют партнерства между государственным и частным сектором, между участниками частного сектора, а также между государственными структурами. Они обеспечивают своевременный обмен информацией, разработку типологий, раннее выявление возникающих моделей мошенничества и оперативное реагирование на развивающиеся угрозы ОД.

Совершенствование стандартов возврата активов

В течение последнего десятилетия ФАТФ уделяет приоритетное внимание укреплению механизмов [возврата активов](#) на глобальном уровне, признавая их важность для пресечения преступлений, совершаемых с целью получения прибыли, а также для компенсации жертвам мошенничества⁴.

Обновленные стандарты ФАТФ требуют от стран создания механизмов оперативной приостановки платежей и «заморозки» активов, чтобы предотвратить перевод преступных доходов от кибермошенничества за рубеж. Они также предусматривают применение режимов конфискации без вынесения обвинительного приговора и усиление международного сотрудничества, включая более быструю и эффективную неформальную координацию.

В совокупности эти меры повышают способность стран выявлять, пресекать и обеспечивать возврат активов, полученных в результате мошенничества и других финансовых преступлений.

¹ См. Руководство 2025 года по возврату активов: <https://www.fatf-gafi.org/en/publications/Methodsandtrends/asset-recovery-guidance-best-practices-2025.html>

Регулирование виртуальных активов

По мере того, как более широкое использование цифровых и более быстрых способов платежей создает дополнительные возможности для мошенников причинять ущерб потребителям, мониторинг ФАТФ для выявления новых рисков становится особенно важным.

В 2019 году ФАТФ внедрила глобальные [стандарты в отношении виртуальных активов и выпустила руководство](#) по регулированию ПУВА с применением мер ПОД/ФТ, включая требования по установлению и проверке личности клиента и отслеживанию транзакций, чтобы обеспечить согласованность информации, требуемой в платежных сообщениях.

С тех пор ФАТФ уделяет внимание выполнению этих требований юрисдикциями, особенно теми, где сектор ПУВА имеет существенное значение. Это делается, в том числе, чтобы снизить возможности использования виртуальных активов для кибермошенничества и обеспечить преследование таких злоупотреблений в рамках системы уголовного правосудия.

Поскольку преступники используют пробелы и различия в реализации стандартов ФАТФ в разных юрисдикциях, ФАТФ будет уделять особое внимание ускорению глобального соблюдения стандартов.

Выявление бенефициарной собственности

Профессиональные участники мошеннической деятельности используют подставные компании для сокрытия преступных доходов и имущества. ФАТФ является мировым лидером по внедрению международных стандартов в отношении бенефициарной собственности таких видов юридических структур.

В марте 2022 года ФАТФ пересмотрела свои стандарты в отношении бенефициарной собственности, обязав страны применять риск-ориентированный и многоуровневый подход к сбору и использованию [информации о бенефициарных собственниках юридических лиц](#).

Национальные и международные партнерства

Механизмы национальной координации и сотрудничества возникли из необходимости более быстрого обмена информацией, совместной работы государственного и частного сектора для достижения общей цели и реагирования на растущую эпидемию кибермошенничества. Национальные центры по борьбе с мошенничеством обладают многими характеристиками и полномочиями, аналогичными национальным центрам или режимам координации в сфере ПОД/ФТ/ФРОМУ.

Помимо координации внутри своей страны, национальные органы также демонстрируют готовность работать с международными партнерами для выявления лиц, совершающих мошенничество за рубежом, а также для отслеживания и возврата активов от преступной деятельности. Эффективное межведомственное сотрудничество через границы может существенно повысить эффективность выявления и пресечения транснациональных сетей мошенничества и мошеннических схем.

Использование передовых технологий

Учитывая огромный масштаб и сложность мошеннических транзакций, страны инвестируют в технологические решения, позволяющие опережать развитие кибермошенничества.

Некоторые ПФР и банки внедрили модели машинного обучения для анализа данных о транзакциях и выявления аномалий, связанных с мошенничеством и другими формами финансовых преступлений. Другие разработали системы оценки рисков платежей, позволяющие выявлять платежи высокого риска в режиме реального времени на основе характеристик, соответствующих известным моделям мошенничества.

Недавние изменения ФАТФ в требованиях к прозрачности платежей также стимулируют применение механизмов проверки на мошенничество в платежных процессах.

Заключение

Кибермошенничество значительно расширилось по охвату и масштабам и в настоящее время затрагивает практически каждого человека в мире. Признавая развитие этих угроз, ФАТФ намерена в ближайшие годы уделять особое внимание проблеме мошенничества. Это включает продолжение анализа новых тенденций, таких как рост и распространение по всему миру числа «центров мошенничества», а также определение мер по укреплению возможностей стран реагировать на эпидемию мошенничества путем использования инструментов ФАТФ.

ФАТФ поддерживает согласованность усилий в борьбе с кибермошенничеством. Благодаря Глобальной сети ФАТФ более 200 юрисдикций применяют инструменты ПОД/ФТ, которые не позволяют деньгам попадать в руки к мошенникам, а в случае если, мошенники все же завладели деньгами, помогают вернуть эти средства.

Дальнейшее противодействие современным вызовам кибермошенничества требует международной сплоченности. ФАТФ играет ключевую роль в поддержке более эффективного внедрения глобальных стандартов, направленных на усиление международных усилий по борьбе с мошенничеством, включая международное сотрудничество, возврат активов, оперативный обмен информацией между национальными, международными партнерами, адаптацию к динамичной среде рисков кибермошенничества и укрепление коллективной решимости и практических действий.



Февраль 2026

www.fatf-gafi.org