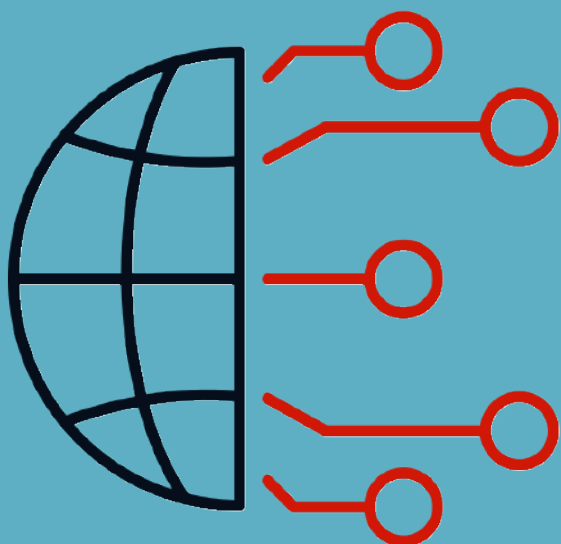




ПЕРСПЕКТИВНЫЙ ОБЗОР

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ДИПФЕЙКИ

ИХ ВЛИЯНИЕ НА ОТМЫВАНИЕ ДОХОДОВ,
ФИНАНСИРОВАНИЕ ТЕРРОРИЗМА И ФИНАНСИРОВАНИЕ
РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО
УНИЧТОЖЕНИЯ



Контекст

Настоящий обзор предлагает перспективный, ориентированный на будущее взгляд на текущие и потенциальные риски и тенденции, связанные с искусственным интеллектом (ИИ). Он является частью поэтапного подхода ФАТФ к изучению формирующихся технологий и направлен на выявление и объяснение развивающихся рисков и уязвимостей, связанных с ИИ, через призму противодействия отмыванию доходов, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ). Отчёт также призван повысить осведомлённость национальных органов власти, финансовых учреждений, поставщиков услуг виртуальных активов, определённых нефинансовых предприятий и профессий, а также других заинтересованных сторон и содействовать разработке эффективных регуляторных и операционных мер реагирования в рамках системы ПОД/ФТ/ФРОМУ. В документе рассматривается пересечение ИИ (включая дипфейки) с рядом Рекомендаций ФАТФ и ставится цель стимулировать дискуссию, углубить понимание проблематики и продемонстрировать приверженность ФАТФ продвижению обсуждения новых тем и формированию перспективного, ориентированного на будущее диалога по данному развивающемуся вопросу.

Введение

Искусственный интеллект является разрушительной силой. Он трансформирует многие аспекты современной жизни — от того, как мы работаем и общаемся, до того, как осуществляется управление и регулирование. Однако, как и любые мощные инструменты, при неправомерном использовании ИИ столь же трансформационен — и опасен. Сформировались два параллельных нарратива: (1) ИИ может использоваться для повышения эффективности правоохранительной деятельности, превентивных мер и комплаенс-процессов; (2) ИИ становится мощным новым инструментом для отмывателей доходов, финансистов терроризма и лиц, уклоняющихся от санкций, позволяя им с возрастающей степенью изощрённости обходить существующие механизмы противодействия отмыванию денег (ОД), финансированию терроризма (ФТ) и финансированию распространения оружия массового уничтожения (ФРОМУ).

Настоящий документ основан на материалах круглого стола, проведённого в рамках заседаний Рабочей группы и Пленарного заседания ФАТФ в июне 2025 года, на которых рассматривалась данная тематика. В нём анализируется усиливающееся пересечение ИИ с ОД, ФТ и ФРОМУ в двух частях:

Часть I посвящена **ИИ-дипфейкам** и, опираясь на недавние экспертные обсуждения ФАТФ о вызовах и возможностях ИИ, используется как аналитическая призма для изучения более широких уязвимостей в превентивных системах подотчетных субъектов в сфере ПОД/ФТ/ФРОМУ, таких как ФУ, ПУВА и УНФПП.

Часть II расширяет обзор и **рассматривает иные формирующиеся риски и тенденции**, связанные с ИИ. Основываясь на текущих исследованиях и экспертном диалоге, она даёт обзор развития за пределами дипфейков с целью прогнозирования потенциальных будущих вызовов.

Раздел I: Дипфейки, искусственный интеллект и ОД/ФТ/ФРОМУ

Стремительно меняющийся ландшафт

Если ранее дипфейки были редким явлением, то сегодня они применяются всё более широко. Дипфейки, созданные с использованием ИИ, представляют собой синтетические материалы — как правило, видео, изображения или аудиозаписи, — сформированные с применением методов искусственного интеллекта, в особенности глубокого обучения, с целью убедительно имитировать внешний облик, голос или действия реальных людей¹. Такие материалы могут использоваться для выдачи себя за другое лицо, распространения дезинформации, а также для содействия мошенничеству и иной незаконной деятельности. Если ранее дипфейки были редким явлением, то сегодня они получают всё более широкое распространение и позволяют эффективно обходить традиционные меры контроля ПОД/ФТ/ФРОМУ и манипулировать системами для совершения отмывания денег, финансирования терроризма, финансирования распространения оружия массового уничтожения, а также предикатных преступлений, таких как мошенничество.

Дипфейки, усиленные ИИ, формируют изменяющуюся угрозу для совершения множества преступлений. В контексте ОД, ФТ и ФРОМУ преступники могут использовать дипфейки для обхода превентивных мер ПОД, ФТ и ФРОМУ, в частности систем надлежащей проверки, включая цифровую идентификацию личности. Сложные и высокоорганизованные субъекты могут применять ИИ-генерированные дипфейки в рамках комплексных схем мошенничества с ценными бумагами. Эти технологии также используются в схемах мошенничества в отношении потребителей, фишинговых атаках, финансовой эксплуатации уязвимых групп населения (например, пожилых людей), романтических онлайн-мошенничествах, а также в онлайн-эксплуатации детей сексуального характера².

Риски, связанные с дипфейками, стремительно возрастают. Дипфейки, создаваемые с использованием ИИ, позволяют преступникам масштабно реализовывать всё более изощрённые мошеннические схемы. Ещё недавно создание дипфейков требовало значительных технических знаний и ресурсов. Однако развитие ИИ-технологий и их широкая доступность радикально снизили порог входа. В настоящее время любой человек, имеющий смартфон и доступ к интернету, способен в течение нескольких минут создать убедительный дипфейк, что формирует острые операционные и регуляторные вызовы для подотчетных субъектов и для государств в борьбе с ОД, ФТ и ФРОМУ.

Использование дипфейков для обхода превентивных мер

Рекомендации 10 и 22 из 40 [Рекомендаций ФАТФ](#) требуют от компетентных органов обеспечить, чтобы ФУ, ПУВА и УНФПП применяли меры по надлежащей проверке клиентов (НПК), позволяющие осуществлять эффективные проверки и идентифицировать клиентов с использованием «надёжных документов, данных или информации из независимых источников (идентификационные данные)». По мере того как инструменты создания синтетических медиа становятся всё более совершенными и доступными, они открывают новые возможности для организованных преступных групп³. Дипфейки могут использоваться для выдачи себя за других лиц, манипулирования биометрической аутентификацией или поддержки схем социальной инженерии, тем самым многократно усиливая эффективность существующих методов обхода процедур НПК и иных протоколов безопасности, предназначенных для защиты банков и УНФПП от рисков ОД, ФТ и ФРОМУ. Их адаптивность к самым различным контекстам делает дипфейки универсальным инструментом кибер-поддерживаемой преступности и отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения, и представляет все более значимый вызов для правоохранительных органов (аутентификация доказательств, судебные процедуры, идентификация жертв, криминалистика и др.)⁴.

Используя возможности маскировки, манипулирования и анонимизации идентичности, преступники всё активнее применяют дипфейки для наращивания сложности, масштаба и охвата своей деятель-

¹ В настоящее время не существует универсального, общепринятого определения термина «дипфейки», однако в общем понимании под ним подразумевается синтетический аудиовизуальный контент — видеозаписи, изображения и голосовые записи, — созданный с целью имитации реальных лиц. См., например: Счётная палата США (Government Accountability Office), 2020 г.: «Научно-технологический обзор: дипфейки» (Science and Tech Spotlight: Deepfakes). (GAO-20-379SP, Deepfakes).

³ См. отчёт ФАТФ: «Выявление, пресечение и расследование онлайн-сексуальной эксплуатации детей» <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html>

³ Bateman, Jon. «Дипфейки и синтетические медиа в финансовой системе: оценка сценариев угроз». Carnegie Endowment for International Peace, 8 июля 2020 г., [веб-публикация](#).

⁴ INTERPOL. 2024. «За пределами иллюзий: разоблачение угрозы синтетических медиа для правоохранительных органов», [веб-публикация](#).

ности. Опыт правоохранительных органов ряда стран, принимавших участие в круглом столе, дополнительно подтверждает эти опасения, приводя конкретные примеры того, как дипфейки, сгенерированные с использованием ИИ, активно используются для обхода защитных механизмов и эксплуатации уязвимостей финансовых систем.

Риски, связанные с дипфейками, усиливаются в трёх ключевых областях:

- 1) **возрастающая зависимость от биометрической верификации**, при которой широкое внедрение распознавания лиц и процедур ЗСК на основе видеосвязи создаёт возможности для манипуляций с использованием дипфейков;
- 2) **устойчивое отставание во внедрении технологий**, поскольку многие системы ПОД остаются недостаточно подготовленными для выявления синтетического контента, а комплаенс-механизмы до сих пор не учитывают данные уязвимости; и
- 3) **проблема трансграничной сложности**, при которой взаимосвязанность глобальных финансовых систем усложняет цифровую идентификацию и признание удалённой верификации личности, позволяя преступникам эксплуатировать слабые места режимов противодействия отмыванию денег.

Эти риски затрагивают финансовый сектор, прежде всего банки и провайдеров платёжных услуг, а также более широкий финансовый рынок и УНФПП, особенно в условиях, когда услуги (финансовые, юридические и иные) и другие виды деятельности (такие как азартные игры, онлайн-игры и т. п.) всё чаще осуществляются полностью в онлайн-среде. Ускорение цифровизации после пандемии COVID-19 также способствовало дополнительному росту числа финансовых и коммерческих взаимодействий, происходящих в цифровом пространстве. Кроме того, широкая доступность систем ИИ усилила риск их «двойного назначения», позволив как высококвалифицированным, так и менее опытным субъектам использовать эти технологии способами, формирующими различные по характеру угрозы:

Вставка 0.1. Угроза двойного использования ИИ при атаках низкой и высокой сложности – (Европол)

Европол обратил внимание на использование своего «инновационного хаба», что перекликается с другими обсуждениями так называемой «гонки вооружений» в сфере ИИ между правоохранительными органами и преступниками, реализующими профессионализированные схемы отмывания денег (ОД).

Говоря о тенденциях и формирующихся рисках, Европол подчеркнул, что искусственный интеллект эксплуатируется в мошеннических целях по двум направлениям: как низкоквалифицированными преступниками, использующими возможности дипфейков, усиленных ИИ, для лёгкого совершения правонарушений; так и высококвалифицированными, профессионализированными субъектами, действующими в рамках схем отмывания денег и мошенничества в интересах организованной преступности, что создаёт мультипликативный эффект преступной деятельности.

- **Низкоквалифицированные правонарушители** всё чаще извлекают выгоду из широкой доступности готовых ИИ-инструментов, которые позволяют им осуществлять сложные преступные действия без необходимости обладать продвинутыми техническими навыками. Эти технологии — часто воспринимаемые как универсальные приложения — включают инструменты ИИ и дипфейков, легко доступные и пригодные к использованию без специализированной подготовки. Преступники могут применять их для широкого спектра незаконных целей, включая фишинг и мошенничество, создание синтетических изображений для материалов сексуальной эксплуатации детей, выдачу себя за других лиц с целью обхода систем безопасности, а также иные формы обмана.
- **Высококвалифицированные киберпреступники** используют ИИ для наращивания своих возможностей — посредством автоматизации сложных методов атак и быстрого выявления уязвимостей в компьютерных системах. Одновременно экспертный уровень применения ИИ и технологий дипфейков позволяет реализовывать более изощрённые методы имитации личности. Так, профессионалы способны воспроизводить отпечатки пальцев, поведение браузера и учётные данные для входа в системы с целью захвата аккаунтов. Вредоносное программное обеспечение класса «инфоботов» может копировать ключевые элементы цифровой идентичности жертвы, помогая злоумышленникам обходить двухфакторную аутентификацию и иные меры безопасности для сохранения несанкционированного доступа.

Появляются и новые виды киберпреступности, основанные на использовании ИИ, в частности атаки типа «тайпсквоттинг», которые эксплуатируют ошибки, допускаемые ИИ-ассистентами для написания кода. Такие ассистенты иногда предлагают программные пакеты, которые фактически не существуют. Злоумышленники отслеживают подобные рекомендации и, когда видят, что вымышленное название пакета предлагается неоднократно, создают реальный — но вредоносный — пакет с этим именем и загружают его в публичные репозитории. Если разработчики доверяются ИИ и используют предложенный код без проверки пакета, в их системы может быть незаметно установлено вредоносное программное обеспечение, что приводит к компрометации цепочки поставок программного обеспечения.

Экспертное использование ИИ также усиливает уже существующие угрозы за счёт автоматизации преступных процессов. Киберпреступные сети применяют алгоритмы машинного обучения для поиска уязвимостей в целевых системах. Это позволяет им существенно масштабировать атаки, одновременно снижая потребность в участии человека.

Данная динамика двойного использования расширяет ландшафт угроз, поскольку ИИ позволяет более широкому кругу субъектов действовать с большей эффективностью, точностью и масштабом воздействия.

Следующее кейс-исследование демонстрирует различный характер воздействия дипфейков, созданных с использованием ИИ, и применения синтетических идентичностей, наглядно показывая возрастающую сложность процессов аутентификации в рамках НПК. Оно подчёркивает сохраняющуюся ключевую роль человеческой экспертизы и технологической компетентности в выявлении несоответствий, которые автоматизированные системы могут не распознать.

Вставка 0.2. Кейс-исследования: синтетическая идентичность с использованием дипфейков на основе ИИ

Технологии ИИ всё активнее интегрируются в финансовые услуги с целью повышения качества клиентского обслуживания и уровня безопасности. Однако те же самые технологии используются преступными субъектами для реализации сложных мошеннических схем. Одна из формирующихся тактик, зафиксированная в одной из юрисдикций, заключается в сборе похищенных документов, удостоверяющих личность, и создании «гибридных» синтетических идентичностей, объединяющих элементы информации как жертв, так и подозреваемых лиц. Эти сфабрикованные идентичности используются для открытия банковских счетов, обхода механизмов НПК, а также систем распознавания лиц, что существенно повышает риски мошенничества, кражи личных данных и иных предикатных преступлений.

Органы власти данной юрисдикции представили два показательных случая, иллюстрирующих неправомерное использование ИИ и технологий дипфейков:

- **Кейс 1: мошенничество с использованием дипфейков в формате видеоконференции**

Преступники использовали дипфейки, сгенерированные с применением ИИ, для имитации видеоконференции с участием международной консалтинговой компании. Выдавая себя за высшее руководство, они дали указание финансовому директору компании перевести 25 млн долларов США на фиктивный проектный счёт. Часть средств удалось своевременно заморозить, при этом расследование по установлению местонахождения оставшихся активов продолжается.

- **Кейс 2: мошенническая схема романтического и инвестиционного характера**

Полиция выявила мошеннический кол-центр, управляемый высококвалифицированными лицами. Данный центр организовывал романтические мошенничества, вовлекая жертв в фиктивные инвестиции в криптоактивы и иные обманные схемы.

Компетентные органы пояснили, каким образом изображения дипфейков и синтетические идентичности использовались для обхода процедур НПК. В ответ полиция внедрила многоуровневую стратегию противодействия финансовым преступлениям с использованием дипфейков, включающую следующие меры:

Превентивные меры на этапе НПК

- внедрение передовых инструментов верификации личности, включая расширенные проверки «присутствия в реальном времени» с применением аппаратных и иных форм биометрической аутентификации в сочетании с более продвинутыми механизмами многофакторной аутентификации.

- Усиление протоколов ЗСК за счёт внедрения систем выявления рисков на основе ИИ.

Следственные меры

- интеграция традиционных следственных методов (например, финансово-экономической экспертизы, сбора разведывательной информации) с передовыми технологиями, такими как:
 - криминалистические инструменты на основе ИИ
 - программное обеспечение для выявления дипфейков
 - аналитика блокчейна для отслеживания потоков виртуальных активов
- создание специализированных подразделений по борьбе с киберпреступностью для демонтажа трансграничных преступных сетей и отслеживания незаконной финансовой деятельности
- назначение специализированных прокуроров и внедрение усиленных мер наказания за финансовые преступления, совершённые с использованием технологий.

Эти случаи подчёркивают сохраняющуюся важность человеческой экспертизы при выявлении аномалий, которые автоматизированные системы могут не обнаружить. В ответ финансовые учреждения начали сотрудничать с академическими организациями и отраслевыми партнёрами с целью:

- обмена разведывательной и аналитической информацией
- тестирования методологий выявления нарушений
- углубления понимания развивающихся технологических рисков.

Рассмотренные случаи также подчёркивают критическую роль государственно-частного партнёрства в поддержании устойчивости к формирующимся угрозам и в обеспечении развития мер противодействия синхронно с технологическими достижениями.

В 2020 году ФАТФ выпустила специальные [Руководящие принципы по цифровой идентификации](#), призванные отреагировать на стремительный рост цифровых и онлайн-платежей, а также на перенос финансовых услуг в цифровое пространство. Эти принципы были направлены на устранение формирующихся уязвимостей, связанных с дистанционным приемом клиентов на обслуживание и процедурами НПК, и предусматривали применение «информированного риск-ориентированного подхода к использованию систем цифровой идентификации» с тем, чтобы финансовые и иные услуги, подпадающие под Стандарты ФАТФ, обеспечивали надлежащий и стандартизированный уровень надёжности процедур ЗСК и НПК. В условиях текущего развития угроз для организаций как никогда важно внедрять устойчивую систему НПК, учитывающую новый ландшафт рисков посредством данного информированного риск-ориентированного подхода.

Противодействие угрозам, связанным с дипфейками на основе ИИ

Выявление и надлежащие практики для финансовых учреждений и подотчётных субъектов

Непредсказуемый и динамично развивающийся характер угроз, основанных на использовании ИИ, требует стратегического предвидения, инноваций и межсекторного взаимодействия. Быстрая эволюция дипфейков на основе ИИ подпитывает постоянную технологическую «гонку вооружений», вынуждая организации осуществлять значительные инвестиции в передовые инструменты выявления и в специализированную экспертизу, в том числе с привлечением внешних поставщиков технологических решений. Расширение цифровых услуг требует мер безопасности, которые одновременно являются масштабируемыми и непрерывными, обеспечивая высокий уровень защиты без подрыва пользовательского опыта, при одновременном обеспечении и повышении доступности финансовых услуг. При этом организациям необходимо ориентироваться в сложной регуляторной среде, находя баланс между эффективностью и соблюдением требований в области конфиденциальности, согласия и подотчётности.

Разграничение подлинного и сфальсифицированного контента сегодня требует развитой технической экспертизы. Эффективность выявления также может быть повышена за счёт внедрения технологических инструментов поддержки, способных обнаруживать несоответствия в видео- и аудиоматериалах, усиления многоуровневых механизмов верификации, а также обучения комплаенс-подразделений в тесном взаимодействии с поставщиками технологических услуг. Приведённое ниже кейс-исследование демонстрирует, каким образом органы власти могут использовать различные источники для выявления дипфейков, созданных с применением ИИ, и связанных с ними мошеннических схем:

Вставка 0.3. Выявление мошенничества на рынке ценных бумаг с использованием дипфейков на основе ИИ

В одной из стран случай так называемого «глубокого мошенничества» был выявлен на основе совокупности источников, включая сообщения от банков, ПУВА, а также обращения общественности (в форме судебных жалоб), поступившие в подразделение финансовой разведки (ПФР).

В ходе проведения операционного и стратегического анализа ПФР выявило сложную мошенническую схему с использованием ИИ и технологий дипфейков, применённых для создания реалистичного видеосюжета — «дипфейкового» новостного репортажа с участием известных телеведущих авторитетных новостных каналов, якобы освещающих первичное публичное размещение акций фиктивной компании. В дипфейках также были задействованы другие широко известные лица из деловой и академической среды.

Злоумышленники использовали данные синтетические видеоматериалы в рамках двух отдельных схем инвестиционного и биржевого мошенничества, действуя от имени конкретных корпораций, включая одно государственное предприятие.

Расследование показало, что программное обеспечение, использованное в данном инциденте, было приобретено у иностранного поставщика, а интернет-инфраструктура, задействованная в схеме, находилась в одной из европейских юрисдикций за пределами страны. С делом были связаны два крупных финансовых учреждения, при этом, согласно национальной оценке рисков, как банковские каналы, так и механизмы, связанные с криптоактивами, характеризуются как каналы с повышенным уровнем риска.

Компетентные органы отследили движение средств и активность преступников. Доходы от мошенничества аккумулировались на центральном счёте, после чего переводились в виртуальные активы (ВА) с использованием некастодиальных кошельков. Для прохождения НПК при аутентификации кошельков виртуальных активов также применялись дипфейки. Идентификация конечных бенефициарных владельцев данных кошельков и счетов была дополнительно осложнена применением методов сокрытия, включая использование синтетической цифровой идентичности при регистрации у провайдера кошельков виртуальных активов (что, в свою очередь, попадает под иностранные санкции).

Участвующие в расследовании органы особо отметили применение новых технологий — таких как верификация контента, специализированное обучение и специальное программное обеспечение для выявления дипфейков. Также была подчеркнута необходимость для ПФР и иных компетентных органов осуществлять постоянный мониторинг и адаптацию к изменяющимся рискам с целью эффективного противодействия угрозам, связанным с внедрением новых технологий.

ИИ может также использоваться подотчетными субъектами для повышения эффективности и усиления мер НПК. По мере того как искусственный интеллект всё глубже интегрируется в финансовые услуги, растущее число финансовых учреждений демонстрирует наглядный пример его трансформационного потенциала. ИИ может органично интегрироваться в ключевые банковские функции. Такой встроенный технологический подход позволяет им оперативно адаптироваться к формирующимся рискам и возможностям, что делает их ключевыми участниками будущего государственно-частного сотрудничества и диалога в сфере финансовых услуг с использованием ИИ.

Надлежащие практики правоохранительных органов:

Стремительное технологическое развитие ИИ создаёт множество вызовов для правоохранительных органов, подчёркивая необходимость формирования устойчивых внутренних компетенций, проведения углублённого обучения и обеспечения непрерывного технологического развития для эффективно-го предотвращения, выявления и реагирования на преступления, совершаемые с использованием ИИ.

Следующее кейс-исследование демонстрирует, каким образом национальные органы реагируют на рост кибермошенничества, основанного на применении ИИ. Эти изменения обусловили внедрение комплекса контрмер — от расширенной биометрической верификации и усиленного мониторинга транзакций до законодательных реформ и кампаний по повышению общественной осведомлённости, — по мере того как органы власти и финансовые учреждения стремятся адаптироваться к меняющемуся характеру угроз.

Вставка 0.4. Кейс-исследование: дипфейки в кибермошенничестве

Недавние сообщения национальных органов одной из юрисдикций указывают на резкий рост инцидентов кибермошенничества, связанных с использованием технологий ИИ. Такие атаки часто переплетаются с традиционными методами, включая фишинг, социальную инженерию и иные формы цифрового обмана.

Особую обеспокоенность вызывает возрастающее использование голосовых дипфейков и манипулированного видеоконтента, которые применяются для выдачи себя за других лиц и введения в заблуждение как финансовых учреждений, так и потребителей.

Органы власти характеризуют текущую ситуацию как «технологическую гонку вооружений», в рамках которой как регуляторы, так и подотчетные субъекты стремятся не отставать от стремительно развивающихся возможностей ИИ. В ответ был внедрён ряд ключевых мер:

- ФУ рекомендуется внедрять передовые системы биометрической идентификации и расширенные формы проверок «присутствия в реальном времени» (например, совмещённое использование аппаратных средств, пассивных и активных методов подтверждения присутствия) для подтверждения подлинности пользователей и предотвращения подмены личности с использованием ИИ;
- ПФР усиливают системы мониторинга транзакций и применяют аналитические методы обработки данных для выявления подозрительных шаблонов, связанных с мошенничеством на основе ИИ;
- правоохранительные органы инициировали технологические реформы, включая создание специализированных подразделений по борьбе с киберпреступностью, ориентированных на расследование и противодействие угрозам, связанным с использованием ИИ;
- во всех секторах приоритетное внимание уделяется кампаниям по повышению осведомлённости, направленным на информирование заинтересованных сторон и широкой общественности о рисках и признаках мошенничества с применением ИИ.

Юрисдикция также проводит пересмотр своего уголовного законодательства с целью формального признания использования инструментов ИИ в преступной деятельности. Предлагаемые поправки предусматривают квалификацию такого использования как самостоятельной формы преступности и, потенциально, как отягчающего обстоятельства при назначении наказания, что отражает серьёзность и высокий уровень технологической сложности данных преступлений.

Некоторые подразделения финансовой разведки (ПФР) разработали наилучшие практики для оказания помощи подотчетным субъектам в выявлении дипфейков в финансовой деятельности, уделяя особое внимание поведенческим и транзакционным аномалиям⁵. К ключевым индикаторам относятся подозрительные схемы, такие как скоординированная активность, быстрые транзакции на вновь открытые счета и немедленное снятие средств сразу после их зачисления. ПФР также отслеживают несогласованности — такие как несоответствия между IP-адресами и профилями клиентов либо использование одного и того же устройства разными контрагентами, — а также необычно высокие объёмы транзакций, независимо от того, связаны ли они с получателями повышенного риска или проявляются в повышенной доле возвратных операций и отклонённых платежей. Эти практики способствуют укреплению систем выявления мошенничества с использованием ИИ.

Вместе с тем в условиях стремительно меняющейся среды методы выявления могут быстро устаревать. В связи с этим участники круглого стола ФАТФ в июне 2025 года подчеркнули важность партнёрств между государственными органами, частным сектором⁶ и операционными подразде-

⁵ См., например: предупреждение Сеть по борьбе с финансовыми преступлениями США «О мошеннических схемах с использованием дипфейк-медиа, нацеленных на финансовые учреждения» <https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial>; см. также: подразделение финансовой разведки Люксембурга (CRF) — «Трендовое предупреждение № 1: использование дипфейков и ИИ для обхода мер ПОД/ФТ».

⁶ Включая поставщиков технологических услуг.

лениями. С учётом данной тенденции критически возрастает потребность в подготовленных специалистах по расследованиям, а также в узкопрофильных экспертных свидетелях, обладающих соответствующей технологической компетенцией.

Формирование пула квалифицированных экспертов и экспертных свидетелей является необходимым первым шагом. Прокуроры также должны проходить специализированную подготовку — не только по вопросам применения ИИ, но и в части выявления и нейтрализации подделок, сгенерированных с использованием ИИ, в ходе разбирательств по делам о мошенничестве.

Создание устойчивых государственно-частных партнёрств в сочетании с взаимодействием с аналитическими центрами и локальными профессиональными сетями является незаменимым условием для обмена знаниями, распространения надлежащих практик и повышения возможностей по выявлению нарушений. Укрепление этих связей имеет ключевое значение для наращивания коллективного потенциала противодействия мошенничеству, основанному на использовании ИИ.

Для эффективного противодействия возрастающей угрозе дипфейков, создаваемых с применением ИИ, финансовые учреждения и правоохранительные органы должны не только усиливать возможности выявления, но и использовать ИИ в качестве проактивного инструмента. Инновационные решения — такие как верификация контента на основе ИИ, биометрический анализ и выявление поведенческих аномалий — позволяют в режиме, близком к реальному времени, идентифицировать синтетические медиа и мошеннические идентичности. Интеграция ИИ в процессы НПК, мониторинга транзакций и следственно-аналитические рабочие процессы способствует повышению устойчивости к мошенничеству с использованием дипфейков.

Раздел II. Перспективный обзор: генеративный ИИ и ОД — эволюция уязвимостей ОД/ФТ/ФРОМУ

Генеративный ИИ, ИИ-агенты, общий искусственный интеллект и ОД/ФТ/ФРОМУ

В настоящем Разделе II представлен краткий первичный перспективный анализ формирующихся тенденций и рисков, связанных с неправомерным использованием ИИ, который акцентирует внимание на эволюционирующих вызовах для правоохранительных и операционных органов, таких как подразделения финансовой разведки. В рамках ускоренного перспективного обзора выделяется несколько различных форм технологий ИИ (классифицированных по способу применения), создающих новые риски для ОД, ФТ и ФРОМУ, в частности за счёт использования следующих инструментов:

- 1) **Дискриминативные / предиктивные модели**⁷, применяющие алгоритмы, основанные на данных, для выявления закономерностей и формирования прогнозов; такие модели могут использоваться преступниками, финансистами терроризма и субъектами ФРОМУ для обхода традиционных систем выявления либо автоматизации незаконной финансовой деятельности.
- 2) **Генеративный ИИ**, способный создавать реалистичный синтетический контент (см., например, раздел о дипфейках выше), поддельные документы или иные артефакты, способствующие мошенничеству и введению в заблуждение, в том числе с использованием диффузионных моделей для генерации изображений и видео.
- 3) **ИИ-агенты** — автономные системы, способные принимать решения и осуществлять действия без участия человека, что потенциально позволяет масштабировать финансовые манипуляции или мошеннические схемы.

Кроме того, следует учитывать и иные технологии, находящиеся на горизонте развития. К ним относится общий искусственный интеллект — пока теоретическая форма ИИ с широкими, человекоподобными когнитивными способностями, которая в случае реализации может создать непредсказуемые риски, поскольку будет способна стратегически проектировать целостные цепочки отмывания доходов и адаптироваться в режиме реального времени на уровне, потенциально превосходящем возможности человека.

Все перечисленные технологии несут различную степень риска в зависимости от вероятности их использования и масштабов последствий, при этом данные параметры постоянно изменяются по мере дальнейшей эволюции ИИ.

Потенциальные риски (известные неизвестности)

- Как отмечено выше, одним из текущих сценариев с высоким уровнем воздействия является использование **генеративного ИИ** (текстовых, визуальных, видео- и голосовых моделей) для создания чрезвычайно убедительных вымышленных лиц или событий, которые мошенники применяют для побуждения жертв к переводу денежных средств, раскрытию учётных данных либо подтверждению транзакций.
- **Дискриминативный / предиктивный ИИ** также представляет существенный риск за счёт применения алгоритмического имитирования схем, используя которые люди (или ИИ-агенты) обучаются с использованием методов машинного обучения воспроизводить легитимное финансовое поведение с высокой точностью. В перспективе отмыватели доходов могут использовать модели машинного обучения, обученные на обширных массивах данных о типичных клиентских транзакциях (полученных как законным, так и незаконным путём) — например, по выплате заработной платы или торговым расчётам, — для генерации синтетических последовательностей операций, статистически неотличимых от подлинной активности. Это значительно затрудняет выявление незаконных транзакций, поскольку они органично «растворяются» в общем потоке легитимной коммерческой деятельности. В связи с этим обеспечение безопасности информационных систем и защита данных организаций финансового сектора становятся следующими критически важными задачами.
- Ещё одним потенциальным риском с высоким уровнем воздействия является появление полностью автоматизированных цепочек отмывания доходов, управляемых **ИИ-агентами**⁸ и функционирующих при минимальном участии человека. Преступные организации могут задействовать

⁷ Данные модели широко применяются в системах ПОД/противодействия мошенничеству (оценка рисков, прогнозирование сообщений о подозрительных операциях, выявление аномалий), в связи с чем у злоумышленников имеется серьёзный стимул к их атаке или эксплуатации.

⁸ IBM: «Что такое ИИ-агенты?» (What are AI Agents?). <https://www.ibm.com/think/topics/ai-agents>

такие механизмы для масштабирования незаконной финансовой деятельности с высокой скоростью и адаптивностью. Такие агенты могут быть способны выявлять системные уязвимости, перенаправлять транзакции в режиме реального времени с целью уклонения от контроля, а также динамически адаптироваться к комплаенс-механизмам. Для снижения подобных угроз финансовым учреждениям потребуется внедрение передовых систем выявления, способных распознавать и нейтрализовать такие сложные автоматизированные модели поведения⁹.

- Дополнительную обеспокоенность вызывает потенциальное будущее развитие **общего искусственного интеллекта** — формы ИИ с широкими, человекоподобными способностями к рассуждению и принятию решений. Несмотря на то что данный концепт остаётся теоретическим, в случае его использования преступными субъектами он может создавать непредсказуемые и системные риски. Способность такого ИИ к автономному обучению, разработке стратегий и междоменной адаптации может позволить организовывать сложные финансовые преступления, включая трансграничные схемы отмывания доходов, манипулирование финансовыми рынками и эксплуатацию регуляторных пробелов. Отсутствие прозрачности в функционировании подобных систем дополнительно усложнило бы процессы выявления и установления ответственности, что подчёркивает необходимость проактивного обзора перспективы рисков и регуляторной готовности.

Потенциальные сценарии, связанные с использованием ИИ:

ИИ представляет собой многогранную и крайне сложную угрозу для способов, с помощью которых правоохранительные органы противодействуют ОД, ФТ и ФРОМУ. Существует широкий спектр вариантов, при которых ИИ может использоваться злоумышленниками для совершения либо содействия совершению отмывания доходов. Ниже приведены некоторые сценарии (включая несколько, основанных на реальных случаях), иллюстрирующие, каким образом ИИ может применяться для содействия профессиональному отмыванию доходов и уклонения от уголовного преследования.

Сценарий 1: использование генеративного ИИ для автоматизации и облегчения этапа расслоения с целью легализации преступных доходов

Злоумышленники используют совокупность генеративных и агентных систем ИИ для формирования убедительного документального «бумажного следа», поддерживающего сложную мошенническую схему и многоуровневое расслоение средств. Преступники могут генерировать поддельные счета за профессиональные услуги с целью создания незаконной либо внешне правдоподобной фиктивной отчётности, используемой на этапе расслоения средств, полученных в результате мошенничества. В данном случае ИИ применяется для создания документации, вводящей в заблуждение подотчетных субъектов и органы власти (а также аудиторов и иных участников), вследствие чего транзакции или экономическая деятельность выглядят легитимными, тогда как фактически речь идёт о сложной системе расслоения.

Сценарий 2: профессиональное отмывание доходов с использованием ИИ-агентов (отмывание через третьих лиц)

Профессиональный субъект, занимающийся отмыванием доходов, проектирует и создаёт серию ИИ-агентов, которые автоматически выполняют набор задач, таких как осуществление онлайн-покупок, внесение средств на счета и иные действия (например, онлайн-гемблинг, игровые платформы, мелкие покупки). ИИ-боты планируют и исполняют микротранзакции, перемещая денежные средства через цепочки счетов в периоды наименьшего уровня риска. Такая деятельность может дополнительно обеспечиваться использованием мошеннических синтетических либо присвоенных идентичностей, применяемых в рамках сложных операций по расслоению и «смурфингу».

Сценарий 3: использование ИИ-агентов в транснациональном отмывании доходов с привлечением номинальных держателей счетов

Данный сценарий описывает схему ОД, в рамках которой автоматизируются привлечение и управление номинальными держателями счетов (денежными мулами), а также выполнение большого объёма микротранзакций на сотни счетов мулов с целью отмывания значительных сумм (например, через онлайн-игровые или гемблинговые платформы). Для этапа расслоения ИИ-агенты автоматизируют переводы на сотни банковских счетов мулов, что позволяет отмывать миллионы долларов США в месяц через онлайн-игровые и азартные платформы. При проведении проверок злоумышленники также обходят процедуры цифровой идентификации, используя дипфейки, созданные с применением ИИ.

⁹ Передовые подходы к выявлению могут включать: графовую и сетевую аналитику для раскрытия скрытых цепочек отмывания доходов; мониторинг транзакций в режиме реального времени с применением методов машинного обучения и выявления аномалий; адаптивное профилирование клиентов; консорциумный обмен разведывательной и аналитической информацией; устойчивые к противодействию модели машинного обучения с постоянным проведением «красного командирования»; гибридные контуры анализа с участием человека; тестирование поведения ИИ-агентов на синтетических данных; а также управление объяснимым ИИ для обеспечения регуляторного надзора.

Сценарий 4: профессиональный ИИ-консультант для ОД/ФТ и обхода санкций

Специалист по обходу санкций в небольшой компании, оказывающей трастовые и корпоративные услуги, использует профессиональную агентную систему ИИ для исследования, компиляции и практической реализации стратегий обхода целевых финансовых санкций (ЦФС), связанных с контролем ФРОМУ/ФТ, в юрисдикциях с уязвимым регулированием. Используемая архитектура решений сочетает крупные языковые модели с поиском с дополненной выборкой по правовым и регуляторным текстам, структурированные графы знаний по юрисдикциям и корпоративным структурам, а также автоматизированных планирующих агентов. Система автоматически собирает и синтезирует публичные и правовые источники, ранжируя и предлагая оптимальные маршруты движения средств и товаров для уклонения от контроля и надзора.

Связанно с этим, возможно и использование аналогичного агента, сочетающего элементы трёх предыдущих сценариев (например, создание синтетической документации, как в Сценарии 1, и применение ИИ-агентов, как в Сценарии 2), для фальсификации документов при торгово-ориентированном отмывании доходов и обходе санкций — посредством генерации поддельных счетов-фактур и учреждения фиктивных импортно-экспортных компаний с ложной деловой историей в юрисдикциях с ограниченными мерами НПК. Такие системы могут даже создавать поддельные веб-сайты и виртуальных поставщиков — с фиктивными каталогами продукции, транспортными документами и электронной перепиской между несуществующими участниками.

Текущие и будущие вызовы для правоохранительных органов

Интеграция ИИ в финансовые и коммерческие системы создаёт значительные новые риски для режимов ПОД/ФТ/ФРОМУ. Хотя ИИ способен повышать эффективность мониторинга и выявления нарушений, он одновременно наделяет преступные субъекты высокоразвитыми инструментами для сокрытия деятельности, фабрикации документации и эксплуатации регуляторных «слепых зон».

ИИ позволяет формировать транзакционные схемы, максимально приближенные к легитимному поведению, что эффективно обходит традиционные системы мониторинга и выявления со стороны ПФР. Противодействующий ИИ может обучаться распознаванию и избеганию «красных флагов» на основе анализа типологических отчётов, методических рекомендаций и иных регуляторных материалов, целенаправленно уклоняясь от обнаружения. Используя масштабные исторические и публичные наборы данных, такие системы способны вырабатывать адаптивные контрмеры, эволюционирующие в ответ на стратегии правоохранительных органов.

Следственные процессы также уязвимы. Преступные сети могут задействовать ботов на основе ИИ для извлечения регуляторной информации, отчётов взаимной оценки и данных из открытых источников с целью выявления слабых юрисдикций, недостаточно регулируемых секторов и эксплуатируемых пробелов. Такие агенты способны картографировать оптимальные маршруты отмывания доходов, определять зоны с низким риском правоприменения и даже разрабатывать новые методы отмывания посредством координированных «хакатонов» в даркнете или автоматизированных экспериментов. Продвинутое сокрытие — включая синтетические торговые потоки и сети подставных компаний, созданные с использованием ИИ, — могут вводить в заблуждение или задерживать действия правоохранительных органов.

В сфере возврата активов ИИ ускоряет сокрытие и перемещение незаконных средств. Миксеры с поддержкой ИИ, автономные кошельки и динамические системы маршрутизации способны дробить и переводить активы через множество юрисдикций почти в реальном времени. Эти инструменты также могут генерировать убедительную, но мошенническую документацию для сокрытия происхождения средств, существенно усложняя их отслеживание и замораживание.

Наконец, уголовное преследование также сталкивается с уникальными препятствиями. Сложность финансовых преступлений с использованием ИИ может опережать техническое понимание следователей и судов. Массовый объём синтетических или фальсифицированных доказательств способен перегружать органы и размывать цепочку хранения доказательств. Кроме того, «чёрный ящик» многих систем ИИ подрывает доказательственную ценность их результатов, если процессы принятия решений не поддаются ясному объяснению или аудиту.

Хотя описанные выше вызовы демонстрируют возрастающую сложность финансовых преступлений с использованием ИИ, в ряде юрисдикций уже предпринимаются инновационные ответные меры. Приводимый далее пример показывает, каким образом такие инструменты, как генеративный ИИ, могут применяться и для укрепления возможностей выявления и верификации.

Вставка 0.5. Использование ИИ финансовыми учреждениями в качестве инструмента выявления схем

Финансовые учреждения в одной из юрисдикций начали внедрять практики, направленные на снижение рисков, связанных с генеративным ИИ. К таким практикам относятся разработка передовых систем проверки документов и защиты от подделок, а также сотрудничество в рамках отраслевых стандартов, ориентированных на выявление вмешательства в цифровой контент.

В ходе мониторинга транзакций одно финансовое учреждение выявило компанию, демонстрировавшую ряд подозрительных транзакционных схем, включая аномальные объёмы, временные характеристики и суммы операций. Для подтверждения подлинности заявленной хозяйственной деятельности финансовое учреждение запросило у компании соответствующие фотоматериалы, подтверждающие наличие и функционирование её коммерческих помещений. С использованием интеллектуальной системы защиты от подделок в сочетании с анализом больших данных для обработки изображений учреждение установило, что элементы фона на фотографиях витрины и интерьера компании в значительной степени совпадают с поддельным документом, ранее представленным клиентом, классифицированным как субъект с высоким уровнем риска. В результате компания была признана высоковероятно вовлечённой в фиктивную хозяйственную деятельность, а применение ИИ обеспечило раннее выявление мошенничества.

Регуляторные подходы к ИИ

В настоящее время не существует согласованного и подлежащего принудительному применению глобального стандарта регулирования ИИ. Ряд юрисдикций и межправительственных организаций разрабатывают региональные или глобальные руководящие материалы¹⁰. Вместе с тем на данный момент отсутствует всеобъемлющая рамочная модель интеграции ИИ в более широкий регуляторный контур. В то время как некоторые юрисдикции активно формируют правила, направленные на обеспечение безопасного использования ИИ и его соответствие действующим или новым правовым нормам, другие — особенно обладающие ограниченными регуляторными ресурсами и институциональной ёмкостью — с меньшей вероятностью предпринимают подобные шаги.

Предыдущая работа ФАТФ по генеративному ИИ и ОД/ФТ/ФРОМУ

В отчёте ФАТФ за 2021 год [«Возможности и вызовы новых технологий для ПОДФТ»](#) был подчеркнут значительный потенциал ИИ и машинного обучения для поддержки подразделений финансовой разведки, надзорных органов и иных правоохранительных структур. В отчёте отмечалось, что данные технологии способны воспроизводить аналитические процессы, свойственные человеку, и выявлять новые методы обнаружения ОД, ФТ и ФРОМУ, при этом подчёркивалось, что ИИ способен *«повышать возможности участников более эффективно реагировать на риски и выполнять установленные требования»*.

С тех пор ИИ стремительно эволюционировал. Если ранее такие инструменты были доступны преимущественно специализированным организациям, то сегодня они получили широкое распространение, принося значительные выгоды, но одновременно формируя новые и сложные риски при неправомерном использовании. Эти изменения подчёркивают важность постоянного диалога и совместных усилий ФАТФ и более широкого международного сообщества для более глубокого понимания и эффективного реагирования как на возможности, так и на вызовы, связанные с данными технологиями.

¹⁰ См., например, [Акт ЕС об ИИ](#) — правовую рамку регулирования ИИ, направленную на гармонизацию законодательства, разработку набора риск-ориентированных правил в сфере ИИ и формирование «надёжного ИИ». Данный акт запрещает ряд практик в отношении услуг ИИ, предоставляемых платформами.

Китай также принял регуляторные акты и технические стандарты, устанавливающие требования к соблюдению норм поставщиками услуг, включая [Временные меры по управлению услугами генеративного искусственного интеллекта](#).

В 2019 году **Сингапур** стал первой страной, представившей Модельную рамку управления ИИ, а в 2024 году опубликовал проект обновлённой [Модельной рамки управления генеративным ИИ](#).

См. также обновлённые в 2024 году [Принципы открытого ИИ](#) ОЭСР — межправительственный стандарт в области ИИ.

Стандарты ФАТФ в отношении возникающих технологий

ФАТФ приняла широкий и инклюзивный подход к «новым технологиям» (Рекомендация ФАТФ 15), обязывающий подотчетные субъекты выявлять и оценивать риски, связанные с возникающими продуктами и решениями. По мере развития ИИ данный подход создаёт прочную основу для дальнейшего сотрудничества, помогая государствам и заинтересованным сторонам анализировать, каким образом такие технологии, как дипфейки и автономные агенты, формируют новые уязвимости и как этими рисками можно эффективно управлять. Существует возможность для ФАТФ и её глобальных партнёров совместно обеспечивать использование преимуществ ИИ при одновременном управлении сопутствующими рисками в соответствии со Стандартами ФАТФ.

Общие выводы и рекомендации

Искусственный интеллект и технологии дипфейков трансформируют сферу финансовых преступлений, создавая как беспрецедентные риски, так и новые возможности для выявления и предотвращения нарушений. По мере роста доступности и усложнения этих инструментов они ставят под сомнение устойчивость существующих режимов ПОД/ФТ/ФРОМУ, особенно в таких областях, как надлежащая проверка клиентов, верификация личности и мониторинг транзакций. Проведённый ФАТФ перспективный обзор по данной тематике подчёркивает необходимость повышенной бдительности и непрерывных инноваций. Чтобы опережать эволюционирующие угрозы, заинтересованные стороны должны не только усиливать защитные механизмы, но и ответственно использовать ИИ для укрепления целостности глобальной финансовой системы.



Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) является независимым межправительственным органом, разрабатывающим и продвигающим политики, направленные на защиту глобальной финансовой системы от отмывания доходов, финансирования терроризма и финансирования распространения оружия массового уничтожения. Рекомендации ФАТФ признаются глобальным стандартом в сфере ПОД и ФТ.

Дополнительную информацию о деятельности ФАТФ можно найти на официальном сайте: www.ФАТФ-gafi.org.

© 2025 ФАТФ/ОЭСР. Все права защищены.

Ни воспроизведение, ни перевод настоящей публикации полностью или частично не допускаются без предварительного письменного разрешения. Заявки на получение такого разрешения — на воспроизведение или перевод всей публикации либо её части — следует направлять в адрес соответствующего правообладателя contact@ФАТФ-gafi.org.