ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

#49
МАРТ/2026

Заместитель министра финансов Индии, Глава делагации Индии в ФАТФ и ЕАГ

ДИВАКАР МИСРА:

«Технологии искусственного интеллекта открывают новую главу в эволюции киберпреступности и становятся фактором, влияющим на баланс сил между правоохранителями и преступниками»

ЮРИЙ ЧИХАНЧИН
Директор Росфинмониторинга,
председатель редакционного совета

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Развитие информационно-коммуникационных технологий, повышение доступности электронных сервисов и платформ предопределяют вовлечение все большего числа пользователей в цифровую среду. Инновации делают жизнь человека проще и комфортнее, но при этом становятся привлекательными для злоумышленников.

Организованные группы, зачастую имеющие трансграничный характер, совершают хищения в виртуальном пространстве, используя вредоносное программное обеспечение, специальную технику, мобильную связь и электронные средства платежей. Все шире информационно-коммуникационные технологии применяются для незаконного оборота наркотических средств, финансирования террористической и экстремистской деятельности, вербовки новых членов радикальных группировок.

Рост числа преступлений, совершаемых с использованием цифровых технологий, вызывает серьезную озабоченность государственных структур во всем мире. Сегодня мы активно работаем по целому ряду направлений — с законодательными и правоохранительными органами, организациями кредитно-финансовой сферы, научным и экспертным сообществом, некоммерческим сектором.

В частности, в Российской Федерации создана государственная информационная система «Антифрод», которая призвана обеспечить оперативное взаимодействие банков, операторов связи, цифровых платформ и правоохранительных органов для выявления и пресечения мошеннических действий. Расширяются возможности применения Единой биометрической системы, завершена апробация процессов внедрения и практического использования в рамках комплаенс-процедур финансовых институтов цифрового сервиса «Прозрачный блокчейн».

Масштабная цифровизация государственного управления, внедрение технологий искусственного интеллекта и другие меры, направленные на обеспечение безопасного использования технологий в сфере ПОД/ФТ, реализуются во многих странах.

При этом очевидно, что цифровой прогресс продолжит ускоряться. И уже в недалеком будущем появятся технологии, которые значительно превзойдут возможности существующих систем. В связи с этим крайне важно своевременно прогнозировать вызовы и угрозы, встающие перед участниками антиотмывочной системы, и принимать превентивные меры для их минимизации.

О том, как используются цифровые инструменты для обеспечения финансовой безопасности государства, общества и личности, о новых вызовах и угрозах, в том числе связанных с применением искусственного интеллекта, читатели смогут узнать из материалов этого выпуска журнала.

СОДЕРЖАНИЕ

6 ДИВАКАР МИСРА:
«По мере эволюции угроз кибербезопасности должны опережающими темпами развиваться и механизмы защиты»

9 АНТОН ЛИСИЦЫН
Устойчивость финансовой безопасности в эпоху цифровизации угроз

Код финансовой безопасности: ведомственный ответ на эволюцию киберугроз

14 ЖАНАТ ЭЛИМАНОВ
Квантовые технологии как фактор риска для финансовой системы

17 БОГДАН ШАБЛЯ
Цифровые платформы и инструменты — новые решения в сфере финансовой безопасности (Платформа «Антидроп»)

21 РУСЛАН ДЖУМАДИЛОВ
Защита от мошенничества с помощью антифрод-систем в Кыргызской Республике

23 ЮНУСИ БЕЖАН МАХМАДЮСУФЗОДА
Большие данные под контролем: как автоматизация меняет качество финансового мониторинга в Таджикистане

26 АЗАТ АЛМАНБЕТОВ
Налоговый контроль как элемент системы финансовой безопасности государства: роль цифровых инструментов

30 ИБРАХИМ АРИФИН
От децентрализации к эксплуатации: рост использования криптовалюты в финансовых преступлениях с применением кибертехнологий и вызовы для управления рисками в банковском секторе

33 СЕРГЕЙ КОНДРАТЬЕВ, АРТЕМ ЧОЗГИЯН
Киберпатрулирование и мониторинг даркнета: как правоохранительные органы используют ИКТ для выявления и пресечения финансовых преступлений в темной сети

35 МЕЛАЙЕ ТИМОТИ ФЕМИ
Противодействие финансовым преступлениям с использованием новых технологий в Западной Африке

38 ДМИТРИЙ СПИРЕВ
Блокировка противоправного контента. Системы мониторинга и выявления

40 Жизненная ситуация «Защита от мошенников в сети»

6 ДИВАКАР МИСРА:
«По мере эволюции угроз кибербезопасности должны опережающими темпами развиваться и механизмы защиты»

9 АНТОН ЛИСИЦЫН:
Устойчивость финансовой безопасности в эпоху цифровизации угроз

14 ЖАНАТ ЭЛИМАНОВ
Квантовые технологии как фактор риска для финансовой системы

35 МЕЛАЙЕ ТИМОТИ ФЕМИ:
Противодействие финансовым преступлениям с использованием новых технологий в Западной Африке

76 Медиапрививка от обмана:
ВЛАДИМИР ТОДОРОВ
о роли документального кино в профилактике мошенничества

ИИ как драйвер комплаенса. Частный сектор в авангарде цифровой трансформации

43 ГАЛИНА КУЗНЕЦОВА
Искусственный интеллект в комплаенсе как инструмент устойчивости антиотмывочной системы

45 ЭДУАРД ИГНАТЬЕВ
Искусственный интеллект в комплаенсе Сбербанка: зрелая система выявления и расследования подозрительных операций

48 ХУРРАМ РИЗОЕВ
Чат-боты и виртуальные помощники для защиты клиентов от мошенничества: опыт банков и финансовых организаций

50 ТАТЬЯНА САНЖИЕВА
«Ответственная игра» и законодательные меры самоограничения: цифровые технологии как инструмент повышения финансовой безопасности в регулируемой индустрии развлечений

53 АЛЕКСАНДР ГАТИН
Искусственный интеллект как оружие. Гонка алгоритмов и новая граница финансового суверенитета

Лаборатория безопасности. Научный ответ на новые риски

58 СЕРГЕЙ ЛУЦЕНКО
Информационная безопасность в банковском секторе

62 ОЛЕГ ИВАНОВ, АНДРЕЙ ЛЕОНИДОВ
Методы искусственного интеллекта в контексте задач в сфере ПОД/ФТ

66 ВЛАДИСЛАВ ГЕНЕРАЛОВ, ЛЮДМИЛА МАКАРОВА
Фактчекинг в сфере финансовой безопасности: научно-образовательные траектории противодействия недостоверной информации

71 МАРИНА ШЕМЯКИНА
Урок по финансовой безопасности: от внеурочной инициативы к международному образовательному проекту

Особый взгляд

76 ВЛАДИМИР ТОДОРОВ
Медиапрививка от обмана: о роли документального кино в профилактике мошенничества

Перекресток культур

79 Деньги как элемент культуры: памятные монеты и банкноты стран Евразийской группы

Новости антиотмывочной системы

81 МЕХИКО: в Мексике прошла Пленарная сессия Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ)

81 АСТАНА: обучение для экспертов-оценщиков Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ)

81 ВЕНА: Глобальный саммит по проблеме мошенничества

81 ТАШКЕНТ: в Узбекистане обсудили меры по борьбе с финансированием терроризма

81 МОСКВА: состоялось заседание организационного комитета VI Международной олимпиады по финансовой безопасности

81
Деньги как элемент культуры: памятные монеты и банкноты стран Евразийской группы

ДИВАКАР МИСРА:
«ПО МЕРЕ ЭВОЛЮЦИИ УГРОЗ КИБЕРБЕЗОПАСНОСТИ ДОЛЖНЫ ОПЕРЕЖАЮЩИМИ ТЕМПАМИ РАЗВИВАТЬСЯ И МЕХАНИЗМЫ ЗАЩИТЫ»

Индия стала одной из крупнейших в мире экосистем стартапов, особенно в таких сферах, как финтех, ИИ и кибербезопасность, отмечает Глава делегации Индии в ФАТФ/ЕАГ, заместитель министра финансов Индии Дивакар Мисра. В стране продолжают развиваться новые платежные инструменты и вместе с ними сервисы по противодействию мошенничеству, разработанные с применением новых технологий. В интервью для журнала «Финансовая безопасность» г-н Мисра рассказал о подходе Индии к цифровизации экономики и сферы госуправления, регулированию виртуальных активов и вопросам финансовой безопасности.

— Индия является одним из мировых лидеров в области цифровизации экономики и внедрения новых технологий в различных сферах. Расскажите, пожалуйста, о работе в этом направлении. Каких результатов уже удалось достичь?

— Цифровая трансформация Индии осуществляется в рамках долгосрочной стратегии, ориентированной на инклюзивное и безопасное развитие. За последнее десятилетие в стране была сформирована так называемая цифровая публичная инфраструктура (DPI) — масштабируемая экосистема цифровых решений, обеспечивающих идентификацию, проведение платежей и обмен данными. К числу ее ключевых элементов относятся Aadhaar (цифровая идентификация), Unified Payments Interface (UPI), обеспечивающая проведение платежей в режиме реального времени, DigiLocker — система безопасного хранения документов, а также механизм Account Aggregator для обмена данными на основе согласия пользователя. Эти системы функционируют в общенациональном масштабе и отличаются высокой степенью совместимости.

Достигнутые результаты весьма значительны. Ежемесячно в Ин-

дии обрабатываются миллиарды операций с использованием цифровых платежных инструментов в режиме реального времени. Существенно расширился охват финансовыми услугами: банковские счета, цифровая идентификация и мобильная связь стали доступны даже в отдаленных районах страны. Система прямых государственных выплат (DBT) позволила сократить потери при распределении социальных выплат и повысить прозрачность этого процесса. Системы налогового администрирования, включая сеть GSTN, повысили эффективность управления государственными доходами. Цифровые платформы государственных закупок, в свою очередь, способствовали росту эффективности и подотчетности при расходовании бюджетных средств. В целом цифровизация позволила снизить транзакционные издержки, повысить качество предоставления государственных услуг и укрепить финансовую дисциплину.

— Насколько актуальны угрозы кибербезопасности для Индии? Какие риски вы могли бы выделить?

— Угрозы в сфере кибербезопасности чрезвычайно актуальны для Индии, как и для всех стран с развитой цифровой экономикой. По мере расширения цифровых сервисов возрастает и потенциальная поверхность атаки. К числу основных рисков относятся фишинг, программы-вымогатели, кража персональных данных, мошенничество с платежами, несанкционированный доступ к учетным записям, вредоносное программное обеспечение и утечки данных. Существенную роль играет и социальная инженерия. Все чаще киберпреступники используют инструменты искусственного интеллекта (ИИ) для совершенствования мошеннических схем. С учетом системной значимости финансового сектора Индия рассматривает кибербезопасность как один из ключевых элементов финансовой стабильности. Регуляторы устанавливают требования к формированию систем киберустойчивости, проведению регулярных аудитов, представлению отчетности об инцидентах и обеспечению непрерывности деятельности. Индийская группа реагирования на компьютерные чрезвычайные ситуации (CERT-In) координирует реагирование на инциденты на национальном уровне. Важным элементом защиты выступают и информационно-просветительские кампании для населения, поскольку многие мошеннические схемы эксплуатируют не столько технические уязвимости, сколько поведенческие особенности людей.

«За последнее десятилетие в стране была сформирована так называемая цифровая публичная инфраструктура (DPI) — масштабируемая экосистема цифровых решений, обеспечивающих идентификацию, проведение платежей и обмен данными.

— Существует и обратная сторона широкого внедрения новых технологий: они могут оказаться в руках злоумышленников. Возможно ли эффективно противодействовать киберпреступникам? Как в Индии борются с дипфейками? Какие инструменты используются для противодействия мошенничеству в целом?

— Хотя преступники действительно используют новые технологии в противоправных целях, эффективное противодействие им не только возможно, но и необходимо. Подход Индии основан на сочетании технологических решений, нормативного регулирования и повышения осведомленности населения. Финансовые организации широко применяют многофакторную аутентификацию, привязку устройств, системы оценки транзакционных рисков и поведенческую аналитику на основе ИИ для выявления аномалий в режиме реального времени. Банки ведут круглосуточный мониторинг мошеннических операций. Созданы централизованный портал для сообщений о киберпреступлениях и горячая линия, позволяющие оперативно сообщать о фактах мошенничества и блокировать незаконные транзакции. Раннее реагирование позволяет существенно сократить финансовые потери.

Дипфейки представляют собой новую глобальную угрозу. В Индии противодействие им осуществляется путем развития цифровой криминалистики, внедрения систем обнаружения на основе ИИ, ужесточения требований к платформам в части надлежащей проверки размещаемого контента, а также проведения информационных кампаний среди граждан. Ключевой принцип заключается в обеспечении адаптивной устойчивости: по мере эволюции угроз должны опережающими темпами развиваться и механизмы защиты.

— Можете ли вы поделиться лучшими практиками внедрения ИИ в сфере государственного управления? Насколько цифровизация изменила сектор государственных услуг?

— Искусственный интеллект в Индии все активнее внедряет-

ся в систему государственного управления, в частности в таких сферах, как выявление мошенничества, налоговая аналитика, мониторинг социальных программ, рассмотрение обращений граждан и автоматический перевод между языками. Одной из ключевых передовых практик является разработка ИИ-решений на базе совместимой цифровой публичной инфраструктуры, а не в рамках изолированных систем. Такой подход обеспечивает масштабируемость и эффективность.

Цифровизация существенно трансформировала систему государственных услуг. Граждане получили возможность в онлайн-режиме оформлять сертификаты, лицензии, пользоваться судебными сервисами, получать доступ к медицинским данным и социальным выплатам. Триада JAM — банковские счета Jan Dhan, цифровая идентификация Aadhaar и мобильная связь — позволила осуществлять прямые государственные выплаты в общенациональном масштабе. Это позволило сократить число посредников, повысить прозрачность и улучшить адресность социальной поддержки. ИИ также применяется в регуляторных и надзорных технологиях (SupTech), обеспечивая риск-ориентированный мониторинг финансового сектора в соответствии с международными стандартами ПОД/ФТ.

— Внедрение технологий ИИ требует совершенствования правовой базы. Как вы видите дальнейший вектор развития законодательства в этой сфере? Какие пробелы еще необходимо устранить?

— Подход Индии заключается в обеспечении баланса между инновациями, ответственностью и безопасностью. Последние законодательные инициативы сосредоточены на защите данных, установлении требований в сфере кибербезопасности, обеспечении ответственного поведения цифровых платформ и предупреждении злоупотреблений. Регуляторная философия строится на риск-ориентированном и технологически нейтральном подходе.

В перспективе особое внимание следует уделить вопросам прозрачности алгоритмов, ответственности за ущерб, причиненный системами ИИ, трансграничного управления данными и гармонизации национального регулирования с международными стандартами. Цель состоит не в избыточном регулировании, а в формировании «умного» регулирования, позволяющего поддерживать инновации при одновременном обеспечении доверия, безопасности и защиты прав.

— Какова позиция Индии в отношении регулирования виртуальных активов? Как осуществляется мониторинг и контроль в этой сфере с учетом рисков легализации преступных доходов и финансирования терроризма?

— Индия признает как инновационный потенциал виртуальных активов, так и связанные с ними риски. Поставщики услуг, связанных с виртуальными активами, подпадают под требования в области противодействия легализации преступных доходов и финансированию терроризма в соответствии со стандартами Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ). Они обязаны проводить надлежащую проверку клиентов, хранить документы, направлять сообщения о подозрительных операциях и соблюдать так называемое правило передачи информации (Travel Rule). В этой сфере созданы механизмы регистрации и контроля за соблюдением установленных требований, обеспечивающие надлежащий надзор.

С учетом трансграничного характера виртуальных активов особое значение приобретает международное сотрудничество, позволяющее предотвращать регуляторный арбитраж. Индия поддерживает скоординированный глобальный подход, который обеспечивает равные условия регулирования и одновременно снижает риски легализации преступных доходов, финансирования терроризма и финансирования распространения оружия массового уничтожения. Цель состоит в интеграции таких инструментов в прозрачную и подотчетную финансовую систему, а не в ограничении инноваций.

— Находится ли инновационная деятельность в руках молодых специалистов? Какую поддержку могут получить ИТ-компании и стартапы в Индии?

— Да, инновации в Индии во многом формируются молодыми специалистами и динамично развивающейся экосистемой стартапов. Государственные инициативы, такие как Startup India и Digital India, предусматривают поддержку инкубационных программ, упрощение процедур соблюдения регуляторных требований, расширение доступа к финансированию и интеграцию с цифровой публичной инфраструктурой через открытые API.

Индия стала одной из крупнейших в мире экосистем стартапов, особенно в таких сферах, как финтех, ИИ и кибербезопасность. Партнерство между государством и частным сектором, сотрудничество с научно-исследовательскими учреждениями и программы развития профессиональных навыков дополнительно укрепляют эту экосистему. Цифровая публичная инфраструктура играет важную роль, снижая барьеры входа на рынок и позволяя стартапам масштабировать инновационные решения уже на ранних этапах развития.

УСТОЙЧИВОСТЬ ФИНАНСОВОЙ БЕЗОПАСНОСТИ В ЭПОХУ ЦИФРОВИЗАЦИИ УГРОЗ

Развитие цифровых технологий оказывает значительное влияние на структуру основных угроз финансовой безопасности государства. Ключевое значение приобретают изменения в среде функционирования национальных систем, особенно в части технологической инфраструктуры национальных платежных систем и кибербезопасности. Цифровизация мировой экономики создает новые риски и требует комплексного подхода к обеспечению устойчивости финансовых институтов перед лицом современных киберугроз.

АНТОН ЛИСИЦЫН
Заместитель директора Федеральной службы по финансовому мониторингу

Еще десять лет назад типичный образ киберпреступника ассоциировался с технически одаренным энтузиастом, действующим в одиночку. Сегодня современная киберпреступность представляет собой распределенную экосистему. Конвенция ООН против киберпреступности, открытая для подписания 25 октября 2025 года и собравшая к настоящему моменту 74 подписанта, стала признанием на высшем международном уровне того факта, что ИКТ-преступность — угроза глобального масштаба, требующая координированного ответа.

Отдельный фокус сегодня на одном из ключевых трендов — формировании организованной «экономики киберпреступности» в финансовом секторе: ее архитектуре, влиянии на финансовую систему России и связи с национальной системой ПОД/ФТ.

В мире, где кибератаки на финансовые системы (и государственного, и частного сектора) происходят каждые 39 секунд (данные IBM 2025), цифровая устойчивость уже не модный тренд, а вопрос выживания и сохранения возможности стабильного функционирования.

Масштабы теневой ИКТ-экономики поражают. По оценкам компании F6, в 2025 году в публичный доступ попало более 760 млн строк с данными граждан России. Управление «К» МВД России зафиксировало свыше 380 тысяч киберпреступлений по статье о мошенничестве, потерпевшими стали 344,4 тысячи человек.

Массовые утечки данных, рост числа дипфейк-атак и телефонного мошенничества подрывают доверие граждан к цифровым финансовым сервисам. Это создает системный риск для цифровизации финансового сектора — стратегического приоритета государственной политики.

Для Росфинмониторинга это означает, что мы рискуем не только данными, но и национальной безопасностью — согласно экспертным данным один час простоя AML-системы (ЕИС Росфинмониторинга) обходится в 500 млн рублей (по данным за 2022 год).

Все это предъявляет принципиально новые требования к национальной системе противодействия отмыванию доходов и финансированию терроризма и заставляет регуляторов выстраивать цифровую оборону нового поколения.

«В 2025–2026 годах ФАТФ усиливает внимание к рискам, связанным с виртуальными активами, финансированием распространения оружия массового уничтожения через киберпреступность и миграцией криптосервисов в слаборегулируемые юрисдикции.

КИБЕРПРЕСТУПНОСТЬ И СИСТЕМА ПОД/ФТ: ТОЧКИ ПЕРЕСЕЧЕНИЯ

ФАТФ в специальном отчете о программах-вымогателях прямо указывает: атаки программ-вымогателей и иные киберпреступления должны быть квалифицированы как предикатные преступления для целей противодействия отмыванию средств. Выкупы практически всегда выплачиваются в виртуальных активах, а последующее отмывание осуществляется через миксеры, DEX-платформы и анонимные кошельки. Это означает, что каждый инцидент ИКТ-мошенничества порождает цепочку финансовых операций, подлежащих контролю в рамках системы ПОД/ФТ.

В 2025–2026 годах ФАТФ усиливает внимание к рискам, связанным с виртуальными активами, финансированием распространения оружия массового уничтожения через киберпреступность (в частности, атакам на криптовалютные платформы, включая хищение 1,5 млрд долларов с платформы ByBit в феврале 2025 года) и миграцией криптосервисов в слаборегулируемые юрисдикции.

Государственный ответ на эскалацию ИКТ-преступности в финансовой сфере оформлен в виде масштабного законодательного пакета «Антифрод 2.0», принятого Государственной Думой в первом чтении 9 февраля 2026 года. Основная дата вступления в силу — 1 сентября 2026 года, с поэтапным введением отдельных норм в 2027–2028 годах.

Одним из ключевых элементов нового пакета является предложение о введении обязательной привязки банковских счетов граждан к их индивидуальному налоговому номеру (ИНН), что должно повысить точность идентификации владельцев счетов и предотвратить случаи использования подложных документов для оформления платежей и переводов. Помимо этого планируется ввести ряд других мер, включая:

- ограничение количества банковских карт, которыми может владеть одно физическое лицо (не более пяти в одном банке и не более двадцати во всей банковской системе);
- создание единой системы учета платежных карт, позволяющей отслеживать движение средств и выявлять подозрительные операции;
- ужесточение требований к идентификации клиентов банками, включая необходимость предоставления заграничного паспорта иностранцами при открытии счетов и получении карт.

При разработке законопроекта учитывался важнейший аспект — поддержание разумного баланса между повышением уровня безопасности и сохранением удобства для граждан. Таким образом, проведенная работа ярко иллюстрирует намерение российского государства создать эффективные инструменты профилактики и обнаружения киберпреступлений, способствующие повышению финансовой защищенности и общей стабильности общества.

Этот амбициозный проект предполагает внесение существенных поправок в целый ряд основополагающих нормативных актов, включая Федеральные законы № 115-ФЗ о противодействии легализации преступных доходов, о Центральном банке (№ 86-ФЗ), о связи (№ 126-ФЗ), о защите персональных данных (№ 152-ФЗ), а также о национальной платежной системе (№ 161-ФЗ), Едином портале государственных услуг и Единой биометрической системе. Комплексный характер вносимых изменений подчеркивает серьезность подхода государства к решению проблем, возникающих в результате быстрого распространения высокотехнологичных видов мошенничества.

НАПРАВЛЕНИЯ РАЗВИТИЯ ЦИФРОВОЙ УСТОЙЧИВОСТИ ПОД/ФТ

Организованная киберпреступность в финансовом секторе — это не будущее, а настоящее. Она уже структурирована как индустрия с собственными маркетплейсами, сервисной моделью, специализацией и механизмами доверия. Ее масштабы — сотни миллиардов рублей ущерба ежегодно только в России, триллионы рублей предотвращенного ущерба — свидетельствуют о системной угрозе финансовой стабильности.

Однако ключевой вызов ближайших лет — это гонка технологий. Генеративный ИИ, дипфейк, Web3-инструменты и модель Cybercrime-as-a-Service снижают порог входа для преступников и повышают качество атак. Российская государственная система на сегодняшний день имеет возможность не просто реагировать на угрозы, но и выстроить проак-

тивную систему защиты финансового суверенитета в цифровую эпоху. Успех будет зависеть от скорости внедрения технологий, качества межведомственного взаимодействия, а также от финансовой грамотности самих граждан.

Что такое цифровая устойчивость для нас?

Цифровая устойчивость — это способность систем Росфинмониторинга непрерывно выявлять, предотвращать и реагировать на угрозы в реальном времени.

Росфинмониторинг определил цифровую трансформацию национальной системы ПОД/ФТ как стратегический приоритет на 2024–2026 годы. Это отражено в официальной декларации «Стратегические цели Росфинмониторинга на 2024–2026 годы». Среди задач:

- развитие цифровых сервисов в сфере ПОД/ФТ;
- повышение эффективности аналитических инструментов;
- совершенствование информационных технологий финансового мониторинга;
- развитие оценки рисков и кадрового потенциала.

Сегодня можно с уверенностью говорить, что в последние годы единая информационная система ведомства прошла путь от простого инструмента сбора и обработки данных до полноценного цифрового пространства, обеспечивающего всестороннюю поддержку работы сотрудников и выполнение стратегических задач Службы.

Процесс построения цифровой экосистемы сопровождался разработкой инновационных решений. Одной из первых успешных инициатив стало внедрение в 2025 году собственной языковой модели искусственного интеллекта, ориентированной на выявление признаков финансовых нарушений. Благодаря этому сотрудники получили мощный инструмент анализа большого объема данных, помогающий выявить потенциально опасные схемы и минимизировать человеческий фактор в процессе принятия решений.

Сегодня единая информационная система Росфинмониторинга успешно функционирует как самостоятельная экосистема, охватывающая широкий спектр функций и возможностей, обеспечивающая взаимодействие с различными ведомственными системами и базами данных, позволяя оперативно получать информацию и анализировать ее на предмет наличия признаков отмывания денег и финансирования терроризма.

Дальнейшие шаги предполагают интеграцию с международными партнерами, расширение функционала системы и применение перспективных технологий машинного обучения и искусственного интеллекта. Важным направлением развития экосистемы становится работа Международного центра оценки рисков (МЦОР).

«Российская государственная система на сегодняшний день имеет возможность не просто реагировать на угрозы, но и выстроить проактивную систему защиты финансового суверенитета в цифровую эпоху. Успех будет зависеть от скорости внедрения технологий, качества межведомственного взаимодействия, а также от финансовой грамотности самих граждан.

МЦОР играет ключевую роль в изучении глобальных тенденций и актуальных угроз финансовой безопасности и служит своего рода связующим звеном между российским государством и странами СНГ в борьбе с незаконными финансовыми потоками. Взаимодействие с иностранными партнерами позволяет аккумулировать знания и лучшие практики, делая систему предупреждения и раскрытия финансовых преступлений еще эффективнее.

В стремительном развитии ИКТ, которые преобразуют привычные бизнес-процессы и создают новую парадигму доверительного взаимодействия в цифровой экономике, особенно выделяется роль блокчейна, существенно повлиявшего на сферы бизнеса и обеспечение надежности финансовых операций.

Блокчейн произвел настоящую революцию в сфере безопасности и прозрачности криптовалютных сделок. Технология гарантирует надежность и доступность информации о каждой транзакции, включая адрес отправителя и получателя, сумму перевода и точное время операции. Но при этом она оставляет открытым ключевой вопрос — анонимность пользователей, чьи личные данные остаются неизвестными широкой публике.

Именно для преодоления этой проблемы Росфинмониторинг совместно с иными участниками на национальном и наднациональном уровнях начал применять специализированный сервис «Прозрачный блокчейн». Основанный на принципе «разметки», этот инструмент позволяет идентифицировать участников криптовалютного рынка, наблюдать за их активностью и выстраивать связь между криптокошельками. Благодаря такому подходу эффективно проводится мониторинг криптовалютных транзакций, что особенно актуально в ходе подготовки законодательного регулирования оборота криптовалюты.

Несмотря на то, что «Прозрачный блокчейн» появился относительно недавно, он уже занял важное место в цифровой инфраструктуре Росфинмониторинга. Подтверждением тому могут служить успешные примеры совместной работы Росфинмониторинга и правоохранительных органов, направленные на пресечение использования криптовалют в незаконных операциях.

В целях укрепления цифровой устойчивости для безопасного обмена чувствительной информацией с зарубежными партнерами Росфинмониторинг создал собственную уникальную защищенную систему обмена данными.

Обычные каналы связи и стандартные протоколы обмена информацией легко поддаются взломам и манипуляциям, подвергая риску конфиденциальные данные, касающиеся финансовой разведки и борьбы с организованной преступностью. Сегодня Росфинмониторинг при коммуникациях с зарубежными партнерами может гарантировать максимальную защиту данных и исключить компрометацию информации.

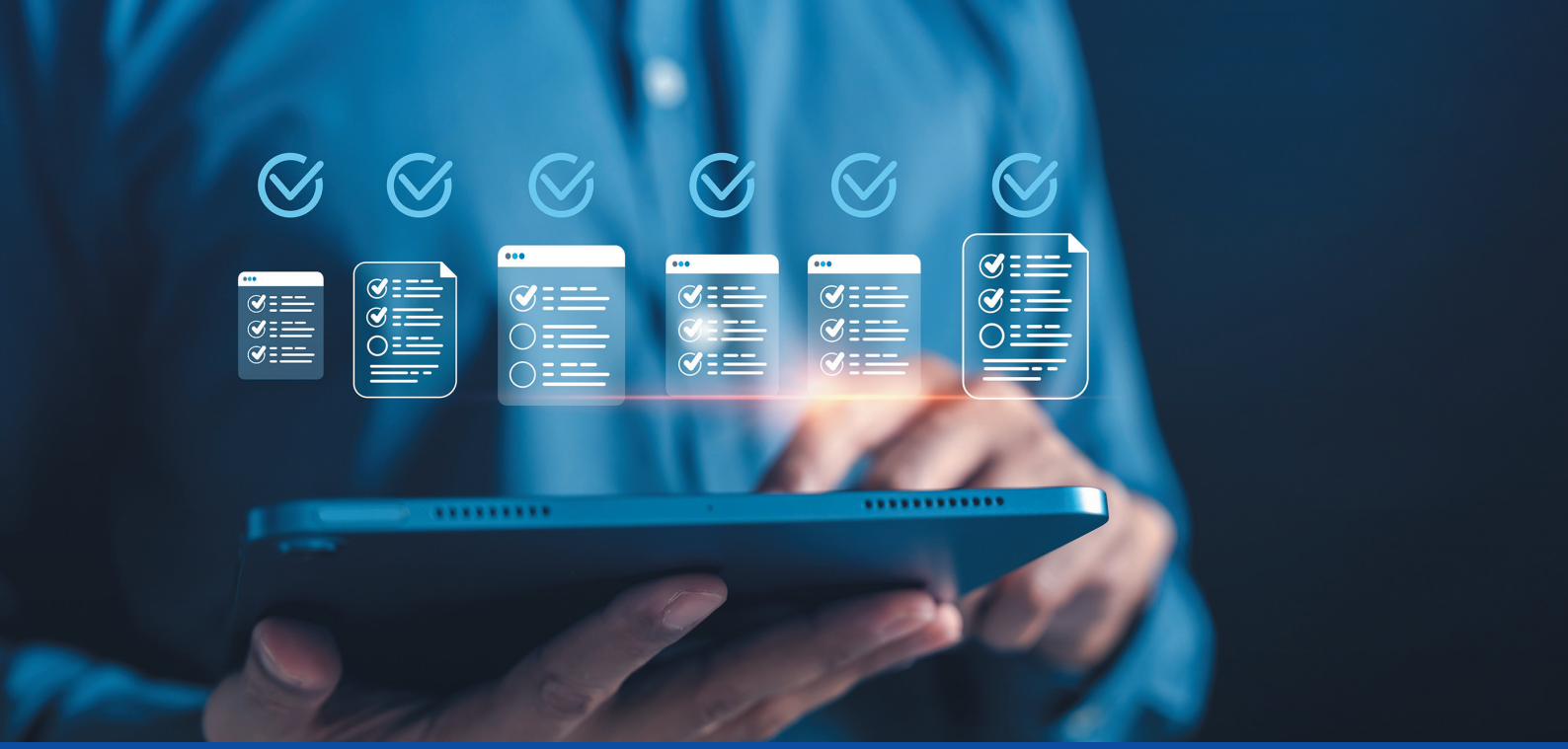
В ближайшее время Росфинмониторинг намерен расширить круг участников защищенной системы в интересах улучшения качества международного сотрудничества и создания устойчивого механизма для противодействия глобальным финансовым преступлениям.

Помимо технического прогресса, остро встает проблема подготовки профессиональных кадров, способных эффективно бороться с новыми формами криминала.

В условиях, когда киберпреступность предлагает «вакансии» с минимальным порогом входа благодаря модели Cybercrime-as-a-Service, государство и бизнес сталкиваются с дефицитом квалифицированных кадров в сфере кибербезопасности и финансовой разведки. Международная олимпиада по финансовой безопасности, проводимая по поручению Президента Российской Федерации Росфинмониторингом совместно с ведомствами и организациями-партнерами (в 2025 году — участники из 40 стран, платформа «Содружество» с 260 тысячами пользователей из 120 стран), — один из инструментов решения этой задачи, но масштаб проблемы требует системного подхода к подготовке специалистов на стыке ИТ, финансов и права.

Останется ли финансовый мониторинг «нервной системой» экономики, зависит от того, насколько решительно и системно мы сумеем выстроить контур цифровой устойчивости. В эпоху, когда атаки — каждые 39 секунд, а объемы криптопреступлений измеряются сотнями миллиардов долларов, другого выбора у нас уже нет.

«В целях укрепления цифровой устойчивости для безопасного обмена чувствительной информацией с зарубежными партнерами Росфинмониторинг создал собственную уникальную защищенную систему обмена данными.



КОД ФИНАНСОВОЙ БЕЗОПАСНОСТИ: ВЕДОМСТВЕННЫЙ ОТВЕТ НА ЭВОЛЮЦИЮ КИБЕРУГРОЗ

14 **ЖАНАТ ЭЛИМАНОВ**
Квантовые технологии как фактор риска для финансовой системы

17 **БОГДАН ШАБЛЯ**
Цифровые платформы и инструменты — новые решения в сфере финансовой безопасности (Платформа «Антидроп»)

21 **РУСЛАН ДЖУМАДИЛОВ**
Защита от мошенничества с помощью антифрод-систем в Кыргызской Республике

23 **ЮНУСИ БЕЖАН МАХМАДЮСУФЗОДА**
Большие данные под контролем: как автоматизация меняет качество финансового мониторинга в Таджикистане

26 **АЗАТ АЛМАНБЕТОВ**
Налоговый контроль как элемент системы финансовой безопасности государства: роль цифровых инструментов

30 **ИБРАХИМ АРИФИН**
От децентрализации к эксплуатации: рост использования криптовалюты в финансовых преступлениях с применением кибертехнологий и вызовы для управления рисками в банковском секторе

33 **СЕРГЕЙ КОНДРАТЬЕВ, АРТЕМ ЧОЗГИЯН**
Киберпатрулирование и мониторинг даркнета: как правоохранительные органы используют ИКТ для выявления и пресечения финансовых преступлений в темной сети

35 **МЕЛАЙЕ ТИМОТИ ФЕМИ**
Противодействие финансовым преступлениям с использованием новых технологий в Западной Африке

38 **ДМИТРИЙ СПИРЕВ**
Блокировка противоправного контента. Системы мониторинга и выявления

40 Жизненная ситуация «Защита от мошенников в сети»

КВАНТОВЫЕ ТЕХНОЛОГИИ КАК ФАКТОР РИСКА ДЛЯ ФИНАНСОВОЙ СИСТЕМЫ

Финансовая система и рынок цифровых активов в последние годы быстро меняются под влиянием цифровизации. Параллельно развивается новое технологическое направление — квантовые вычисления. В будущем такие технологии могут значительно увеличить вычислительные возможности и изменить способы обработки данных.

ЖАНАТ ЭЛИМАНОВ
Председатель Агентства Республики Казахстан по финансовому мониторингу

Квантовые технологии позволяют решать задачи, которые для традиционных компьютеров остаются крайне сложными. Однако их развитие может создать новые риски для финансовой инфраструктуры. Поэтому уже сейчас важно оценивать возможное влияние квантовых вычислений на устойчивость финансовой системы, рынок цифровых активов и работу механизмов ПОД/ФТ/ФРОМУ.

КВАНТОВЫЕ ТЕХНОЛОГИИ И ИХ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Современные системы защиты данных в банковской сфере и на рынке цифровых активов основаны на криптографических алгоритмах. Их взлом требует значительных вычислительных ресурсов.

Поэтому при появлении достаточно мощных квантовых компьютеров существующие механизмы криптографической защиты могут оказаться уязвимыми.

Для финансовых организаций и участников рынка цифровых активов это формирует новые технологические и операционные риски.

ОСНОВНЫЕ РИСКИ ДЛЯ ФИНАНСОВОЙ СИСТЕМЫ

Компрометация криптографической инфраструктуры

Финансовая система широко использует криптографию. Она

лежит в основе электронных подписей, защищенных каналов связи, инфраструктуры открытых ключей и систем аутентификации пользователей. Эти механизмы обеспечивают безопасность платежей и надежный обмен информацией между финансовыми организациями.

Если устойчивость криптографических алгоритмов будет нарушена, это может привести к несанкционированному доступу к финансовым системам и подделке цифровых транзакций.

Дополнительный риск связан со стратегией, известной как harvest now, decrypt later (с англ. «собери сейчас, расшифруй позже» — используемый в сфере кибербезопасности термин тактики злоумышленников. — *Прим. ред.*). Она предполагает, что злоумышленники могут уже сегодня сохранять зашифрованные данные, рассчитывая расшифровать их в будущем, когда появятся более мощные вычислительные технологии.

УГРОЗЫ ДЛЯ СИСТЕМ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ

Современные финансовые сервисы активно используют удаленную идентификацию клиентов и электронные подписи. Эти инструменты позволяют подтверждать личность пользователей при проведении финансовых операций.

Если криптографические ключи окажутся скомпрометированными, злоумышленники могут подделывать цифровую идентификацию. Это создает дополнительные возможности для финансового мошенничества и может позволить обходить процедуры KYC.

РИСКИ ДЛЯ РЫНКА ЦИФРОВЫХ АКТИВОВ

Рынок цифровых активов во многом основан на криптографических технологиях. Безопасность большинства блокчейн-сетей обеспечивается механизмами цифровых подписей и хеш-функций.

Компрометация криптографических ключей

Право владения цифровыми активами подтверждается закрытыми ключами. Именно они позволяют пользователю управлять средствами в криптовалютных кошельках.

Если в будущем квантовые компьютеры смогут эффективно взламывать используемые алгоритмы защиты, может возникнуть риск несанкционированного доступа к кошелькам и утраты цифровых активов.

Возможность обхода механизмов финансового мониторинга

Ослабление криптографической защиты может осложнить отслеживание транзакций и идентификацию участников операций. В таких условиях финансовым организациям будет сложнее выявлять подозрительные операции, что создает дополнительные риски для систем ПОД/ФТ/ФРОМУ.

Влияние квантовых угроз на систему ПОД/ФТ/ФРОМУ

Эффективность системы ПОД/ФТ/ФРОМУ напрямую зависит от достоверности данных и надежной защиты информационных систем. Не менее важна безопасность обмена информацией между финансовыми организациями и ПФР.

Квантовые угрозы могут повлиять на:

- безопасность хранения данных о клиентах и бенефициарных владельцах;
- защиту отчетности о подозрительных операциях;
- надежность обмена информацией между ПФР и финансовыми организациями;
- эффективность аналитических систем выявления финансовых преступлений.

В долгосрочной перспективе это может потребовать модернизации технологической инфраструктуры финансового мониторинга.

МЕРЫ ПО МИНИМИЗАЦИИ РИСКОВ

Внедрение постквантовой криптографии

Одним из способов снижения рисков является внедрение криптографических алгоритмов, устойчивых к атакам квантовых компьютеров. Такие алгоритмы разрабатываются с учетом возможностей как традиционных, так и квантовых вычислительных технологий.

«Эффективность системы ПОД/ФТ/ФРОМУ напрямую зависит от достоверности данных и надежной защиты информационных систем. Не менее важна безопасность обмена информацией между финансовыми организациями и ПФР.

Криптографическая инвентаризация

Финансовым организациям важно оценить, какие криптографические алгоритмы используются в их системах и какие из них могут потребовать модернизации. Это позволит заранее подготовиться к переходу на более устойчивые технологии защиты.

Развитие криптографической гибкости

Криптографическая гибкость означает, что используемые алгоритмы защиты можно при необходимости быстро заменить. Это позволяет финансовым организациям быстрее адаптироваться к новым технологическим изменениям.

Совершенствование регулирования рынка цифровых активов

Регуляторам важно учитывать возможные квантовые угрозы при формировании требований к инфраструктуре цифровых активов. В частности, это касается требований к защите криптографических механизмов и безопасному хранению ключей.

Международное сотрудничество

Финансовые рынки и рынок цифровых активов имеют международный характер. Поэтому противодействие квантовым угрозам требует координации усилий государств. Важную роль в этом играет совместная разработка стандартов безопасности и обмен опытом между регуляторами и финансовыми организациями.

ЗАКЛЮЧЕНИЕ

Квантовые технологии могут заметно повлиять на развитие мировой экономики и финансовых рынков. Вместе с новыми возможностями они создают риски для информационной безопасности, финансовой инфраструктуры и рынка цифровых активов.

Для национальных систем ПОД/ФТ/ФРОМУ развитие квантовых технологий означает необходимость заранее готовиться к возможным изменениям в сфере защиты данных и финансовых коммуникаций. Важную роль здесь могут сыграть внедрение постквантовой криптографии, развитие криптографической гибкости и совершенствование регуляторных подходов.

Своевременное реагирование на новые технологические вызовы позволит сохранить устойчивость финансовой системы и обеспечить эффективную работу механизмов противодействия финансовым преступлениям.

«Финансовым организациям важно оценить, какие криптографические алгоритмы используются в их системах и какие из них могут потребовать модернизации. Это позволит заранее подготовиться к переходу на более устойчивые технологии защиты.

ЦИФРОВЫЕ ПЛАТФОРМЫ И ИНСТРУМЕНТЫ — НОВЫЕ РЕШЕНИЯ В СФЕРЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ (ПЛАТФОРМА «АНТИДРОП»)

Масштабное применение дропов стало угрозой для финансовой системы страны. Десятки тысяч людей, независимо от того, осознают они это или нет, становятся участниками подобных схем. Анализ применения банками комплаенс-процедур демонстрирует, что сочетание технологических решений и скоординированного подхода позволяет существенно снизить объемы подозрительных операций.

Цифровым платформам и ИТ-инструментам отводится центральная роль в обеспечении финансовой безопасности. С их помощью удается получить полное представление о ситуации, сократить количество ошибок и обеспечить защиту как финансовых учреждений, так и их обычных клиентов.

Проектируемая Платформа «Антидроп» может стать еще одним примером того, как цифровая трансформация способна работать в интересах экономики страны и устойчивости финансовой системы.

БОГДАН ШАБЛЯ
Руководитель Службы финансового мониторинга и валютного контроля Банка России

Финансовая система стремительно цифровизируется. Платежи становятся мгновенными, банковские услуги и взаимодействие клиентов с финансовыми организациями — дистанционными и почти полностью в режиме онлайн. Однако те же технологии, которые делают финансовые сервисы удобными и доступными, активно используют и организаторы теневого бизнеса. Одним из ключевых инструментов нелегальных расчетов стало использование так называемых дропов — подставных физических лиц, на счета которых переводятся средства, связанные с незаконной деятельностью.

Здесь хотелось бы уточнить понятийный аппарат, использующийся для определения дропов. В Уголовном кодексе Российской Федерации[1] операции дропа квалифицируются как осуществление из корыстной заинтересованности клиентом оператора по переводу денежных средств неправомерных операций с использованием электронного средства платежа, предоставленного ему

[1] Часть 4 статьи 187 Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ.

оператором по переводу денежных средств, по указанию другого лица и (или) в интересах такого лица.

В понимании финансового мониторинга понятие «дроп» несколько шире — это физические лица — клиенты банков, по счетам которых проводятся подозрительные операции. Совокупность таких признаков, как транзитный характер операций, значительные объемы P2P-переводов[2], концентрация операций в короткие временные интервалы, отсутствие заработной платы и иных источников доходов, а также платежей по обеспечению жизнедеятельности физического лица может говорить о том, что операции требуют повышенного внимания со стороны банка на предмет управления счетом третьим лицом. Но важно подчеркнуть, что решение об отнесении к подозрительным операциям должно проверяться и подтверждаться уполномоченным сотрудником банка.

По данным Банка России, в стране в 2025 году ежемесячно открывались десятки тысяч счетов дропов, а в пике — до 100 тысяч счетов.

Масштаб проблемы очевиден: использование дропов стало системным явлением, обеспечивающим расчеты нелегальных онлайн-казино, анонимных криптообменников, наркошопов, финансовых пирамид и других незаконных структур.

При этом, несмотря на рост числа вовлекаемых граждан, объемы операций по счетам дропов за последний год удалось снизить более чем в три раза. Это стало результатом комплексной работы регулятора и банков, а также внедрения цифровых инструментов мониторинга.

Ужесточение контроля привело к тому, что срок жизни карты дропа сократился с нескольких месяцев до часов и минут. Банки внедряют онлайн-мониторинг, анализируют количество входящих переводов, блокируют подозрительные операции в режиме реального времени. В результате злоумышленникам приходится буквально выжимать из карт максимум — караулить поступление средств у банкомата, чтобы успеть их обналичить до блокировки.

Но теневой бизнес адаптируется. Распространенной практикой стало дробление операций и открытие счетов в десятках банков одновременно. Один дроп может иметь карты в 30–40 банках, а переводы распределяются небольшими суммами, чтобы не вызывать подозрений. Для каждого банка в отдельности такая активность может выглядеть относительно чистой. Однако в масштабе всей банковской системы картина иная.

Именно здесь становится очевидным несовершенство фрагментарного подхода. Без централизованного обмена данными банки видят лишь часть пазла.

Введение уголовной ответственности для дропов — также важный шаг в борьбе с ними. На раннем этапе мониторинг специализированных интернет-ресурсов организаторов теневых расчетов показал, что часть из них уже отказалась от использования карт дропов после объявления о новой норме об уголовной ответственности.

Очевидно, что уголовные меры — это не только инструмент наказания, но и мера, направленная на создание эффекта превенции или предупреждения новых преступлений. Ее задача не только наказать организаторов теневых расчетов, но и в явном виде предупредить общество и не допустить его криминализации.

Задача финансовых организаций и контролирующих органов, с другой стороны, состоит в том, чтобы счета дропов стали экономически невыгодным, технологически сложным инструментом и чтобы финансовая система не использовалась для проведения подозрительных операций.

Стратегия противодействия должна быть направлена не на тотальные блокировки, а на снижение экономической эффективности дропперской деятельности, когда эксплуатация счетов дропа становится сопряженной с высокими финансовыми издержками, перекрывающими выгоду от их использования. Такой подход позволит не просто блокировать от-

«Стратегия противодействия должна быть направлена не на тотальные блокировки, а на снижение экономической эффективности дропперской деятельности, когда эксплуатация счетов дропа становится сопряженной с высокими финансовыми издержками, перекрывающими выгоду от их использования. Такой подход позволит не просто блокировать отдельные случаи, а сделать всю модель дропперства нецелесообразной для теневого бизнеса.

[2] Переводы между физическими лицами, например с карты на карту, со счета на счет.

дельные случаи, а сделать всю модель дропперства нецелесообразной для теневого бизнеса.

И здесь на первый план выходят цифровые платформы, так как борьба с дропами также требует новых системных решений. Таким решением становится создание единой цифровой Платформы «Антидроп» Банка России.

Положительный опыт внедрения в 2022 году Платформы «Знай своего клиента» в комплаенс банков в части оценки рисков юридических лиц и индивидуальных предпринимателей — пример того, что создание цифровых платформ на базе Банка России возможно и в отношении подозрительных операций клиентов банков — физических лиц.

На данный момент архитектура Платформы «Антидроп» определена. Алгоритмы платформы будут основаны на анализе больших данных, а именно платежной информации, открытых источников информации и данных, находящихся в распоряжении Банка России как мегарегулятора, с использованием моделей оценки риска и технологий машинного обучения.

В качестве ключевого идентификатора для связки платежных данных и их ассоциации с клиентами кредитных организаций предполагается использовать индивидуальный номер налогоплательщика. Банки обеспечат наличие этого реквизита по всем счетам клиентов. Это создаст единое пространство для сопоставления данных.

Признаки подозрительных операций планируется сформировать на основе имеющейся методологии Банка России и кредитных организаций по выявлению дропов, а их перечень будет утвержден Советом директоров Центрального банка Российской Федерации.

МИРОВОЙ ОПЫТ СОЗДАНИЯ ЦИФРОВЫХ ПЛАТФОРМ / СЕРВИСОВ ДЛЯ АНАЛИТИКИ РИСКОВ, ОБМЕНА ДАННЫМИ И МОНИТОРИНГА ТРАНЗАКЦИЙ

Платформы для обмена данными и аналитики в финансовой системе:

Банк России

РОССИЯ:
ПЛАТФОРМА «ЗНАЙ СВОЕГО КЛИЕНТА» БАНКА РОССИИ

Сервис, с помощью которого кредитные организации получают информацию об уровне риска вовлеченности в проведение подозрительных операций их клиентов (юридических лиц и индивидуальных предпринимателей). Информацию платформы банки могут использовать при реализации процедур противолегализационного контроля.

КЫРГЫЗСКАЯ РЕСПУБЛИКА:
АНТИФРОД-СИСТЕМА

Комплекс организационных, технологических и аналитических мер, направленных на борьбу с мошенниками.

TMNL

НИДЕРЛАНДЫ:
TRANSACTION MONITORING NETHERLANDS (TMNL)

TMNL — совместная инициатива крупнейших банков Нидерландов, которая строит единый контур выявления «необычных паттернов» и подозрительных транзакций.

MAS

СИНГАПУР:
COSMIC (MAS)

Денежно-кредитное управление Сингапура (MAS) в апреле 2024 года запустило цифровую платформу COSMIC для совместного обмена кейсами/информацией по отмыванию денег и финансированию терроризма между банками.

Сервисы для аналитики операций в криптовалютах:

ПРОЗРАЧНЫЙ БЛОКЧЕЙН — СЕРВИС РОСФИНМОНИТОРИНГА

Состоит из аналитических инструментов для мониторинга криптовалютных операций (транзакций), анализа финансовых потоков в криптовалюте и проведения расследований в сфере обращения криптовалют в целях противодействия отмыванию доходов, полученных преступным путем, финансированию терроризма и распространению оружия массового уничтожения.

Chainalysis

CHAINALYSIS

Позиционирует себя как blockchain data platform для госорганов, криптобизнеса и финансовых институтов.

ELLIPTIC

ELLIPTIC

Решение по риск-менеджменту, скринингу, расследованиям для компаний и финансового сектора.

«Еще одной важной задачей создания централизованной платформы является сокращение количества «технических» блокировок. Сегодня банки нередко перестраховываются из-за нехватки информации. Централизованный обмен данными позволит точнее выделять действительно рисковых клиентов и снизить нагрузку на добросовестных граждан.

Модели Платформы «Антидроп» подсветят в выборке ту часть клиентов, по которым выявлены признаки проведения подозрительных операций. Далее эти признаки будут подтверждаться аналитиками.

Таким образом, окончательная оценка пройдет ручную верификацию. По каждому клиенту аналитики сформируют мотивированное суждение и в ежедневном режиме — перечень идентификаторов клиентов с высоким риском проведения подозрительных операций.

Использование данных платформы планируется сделать рекомендательным, поскольку, согласно требованиям ФАТФ, решение об оценке рисков клиента всегда должно оставаться за банками. Такой подход сохраняет баланс между централизованным анализом данных и ответственностью кредитных организаций.

Взаимодействие с банками будет осуществляться ежедневно как в части направления данных о клиентах с признаками проведения подозрительных операций, так и обратной связи от банков в части принятых/отмененных ограничительных мер в отношении клиентов.

Принципиальная особенность концепции — отказ от блокирования денежных средств клиента и отключения дистанционного банковского обслуживания. С развитием качества и скорости аналитики самих банков нет задачи полностью лишить человека доступа к финансовой системе, поскольку гораздо важнее организовать обмен информацией, а не применение мер.

Предлагается ограничивать определенной суммой (например, 30 тысяч рублей в месяц) только те операции, которые критичны для теневых расчетов: массовые входящие P2P-переводы от третьих лиц, внесение наличных в банкоматах, то есть когда у банка нет возможности в моменте подтвердить источник происхождения денежных средств.

В этом случае клиент сохранит возможность получать заработную плату, оплачивать товары и услуги, пользоваться базовыми банковскими сервисами. Такой дифференцированный подход снижает риск «выталкивания» человека в «серую» зону и минимизирует негативный клиентский опыт.

Период действия вводимых банками мер планируется ограничить. В первый раз они будут действовать один календарный год, в случае повторного выявления рисков — три года.

Любая система риск-ориентированного контроля должна предусматривать механизм реабилитации. В рамках Платформы «Антидроп» предполагается, что клиент сможет обратиться в свой банк, предоставить объяснения, а банк в свою очередь проинформировать о принятом решении Банк России. Таким образом, решение о применении и снятии мер полностью остается на стороне банка.

Данный подход делает процедуру прозрачной, а отсутствие избыточной бюрократии — ключевой фактор доверия. Опыт Платформы «Знай своего клиента» показывает, что при корректной настройке доля ошибочных решений может быть минимальной (0,3% реабилитированных клиентов).

Еще одной важной задачей создания централизованной платформы является сокращение количества «технических» блокировок. Сегодня банки нередко перестраховываются из-за нехватки информации. Централизованный обмен данными позволит точнее выделять действительно рисковых клиентов и снизить нагрузку на добросовестных граждан.

Таким образом, цифровая платформа становится не только инструментом борьбы с дропами, но и средством повышения качества комплаенс-процедур.

Дропперство как массовое явление выступает индикатором глубоких изменений в финансовой системе, где теневой и легальный бизнес используют схожие цифровые инструменты. Для эффективного противодействия необходимо системное решение, основанное на современных технологиях и анализе больших данных.

ЗАЩИТА ОТ МОШЕННИЧЕСТВА С ПОМОЩЬЮ АНТИФРОД-СИСТЕМ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

Сегодня антифрод — это не просто набор ограничений на отдельные операции, а система защиты клиента, банка и цифровых каналов обслуживания. Ее задача — своевременно выявлять подозрительную активность, предотвращать мошеннические действия, снижать возможный ущерб и не допускать повторения подобных инцидентов.

РУСЛАН ДЖУМАДИЛОВ
Заместитель председателя Государственной службы финансовой разведки Кыргызской Республики

Если говорить простыми словами, антифрод — это комплекс организационных, технологических и аналитических мер, направленных на борьбу с мошенничеством. В банковской сфере это особенно важно, поскольку злоумышленники используют не только технические уязвимости, но и методы социальной инженерии, заставляя клиентов самостоятельно раскрывать данные карт, подтверждать операции или переводить деньги под ложным предлогом.

На практике наиболее часто встречаются фишинг, компрометация карт, захват учетных записей, использование утекших логинов и паролей, а также мошеннические переводы, инициированные самими клиентами под воздействием обмана. Дополнительную сложность создает высокая скорость операций: после получения доступа к аккаунту или платежным данным злоумышленники стараются как можно быстрее вывести средства через переводы, онлайн-оплату, электронные кошельки или иные каналы.

Именно поэтому современный антифрод обычно строится в двух взаимосвязанных контурах — сессионном и транзакционном. Первый отвечает за доверие к самому входу в систему и поведению пользователя в цифровом канале, второй — за оценку риска уже конкретной операции: перевода, платежа, привязки карты или иного финансового действия. Международные подходы к цифровой аутентификации и

защите платежей исходят именно из такой логики: решение должно приниматься не по одному признаку, а с учетом контекста, риска и характера действия.

«Антифрод — это комплекс организационных, технологических и аналитических мер, направленных на борьбу с мошенничеством.

Сессионный антифрод нужен для того, чтобы выявить риск еще до момента списания денег. Его задача — понять, насколько можно доверять текущей сессии: действительно ли вход выполняет владелец аккаунта, не выглядит ли устройство подозрительно, не отличается ли поведение от обычного профиля клиента. В этой части применяются такие технологии, как многофакторная аутентификация, биометрия на доверенном устройстве, ключи доступа, дактилоскопия устройства, проверка характеристик приложения и устройства, а также риск-ориентированная аутентификация. Последняя оценивает набор сигналов — IP-адрес, геолокацию, время входа, параметры браузера или телефона, а также отклонения в поведении пользователя — и в зависимости от уровня риска либо пропускает действие, либо требует дополнительное подтверждение.

Технологически сессионный антифрод опирается на несколько уровней. Device fingerprinting помогает понять, знакомо ли банку устройство и не изменился ли его цифровой профиль. PKI и криптографические ключи лежат в основе устойчивой аутентификации и позволяют надежно связывать приложение или устройство с доверенным контуром. Биометрия удобна как способ подтверждения действий на уже доверенном устройстве, а не как изолированное решение само по себе. Дополнительно важны контроль целостности мобильного приложения, защита от эмуляторов и подмененной среды, а также безопасное управление сессией: обновление идентификаторов сессии, ограничение времени бездействия и повторная аутентификация после риск-событий. Транзакционный антифрод включается в момент совершения конкретной операции. Здесь система оценивает уже не только пользователя и сессию, но и сам платежный замысел: сумму, получателя, частоту действий, историю подобных операций, тип канала, устройство, а также признаки, характерные для известных мошеннических сценариев.

Основой транзакционного антифрода является мониторинг в реальном времени. На практике используются правила, скоринговые модели и риск-ориентированные сценарии подтверждения. Если операция выглядит типичной и низкорисковой, клиент проходит ее почти без дополнительного трения. Если же система видит отклонения — новый получатель, нетипичная сумма, подозрительный контекст или признаки компрометации — она может запросить усиленное подтверждение, временно ограничить действие или направить событие на дополнительную проверку.

Практика показывает, что наилучший результат дает связка обоих подходов. Рискованная сессия должна повышать риск последующей транзакции, а подозрительная операция в свою очередь должна запускать дополнительную проверку на уровне сессии и клиента. Именно поэтому зрелый антифрод строится как единая система, где сигналы от устройства, канала входа, поведения пользователя и параметров платежа анализируются совместно, а меры защиты применяются адресно — там, где риск действительно повышен.

Таким образом, антифрод сегодня в Кыргызской Республике — это не отдельная проверка и не один защитный механизм, а непрерывный процесс оценки доверия. Сессионный антифрод защищает доступ и цифровую среду клиента, транзакционный — контролирует конкретное движение денег. В сочетании они позволяют кыргызским банкам быстрее выявлять признаки мошенничества, точнее реагировать на подозрительные сценарии и при этом сохранять разумный баланс между безопасностью и удобством клиента.

«Антифрод сегодня в Кыргызской Республике — это не отдельная проверка и не один защитный механизм, а непрерывный процесс оценки доверия. Сессионный антифрод защищает доступ и цифровую среду клиента, транзакционный — контролирует конкретное движение денег.

Большие данные под контролем:

КАК АВТОМАТИЗАЦИЯ МЕНЯЕТ КАЧЕСТВО ФИНАНСОВОГО МОНИТОРИНГА В ТАДЖИКИСТАНЕ

Объем информации, с которым ежедневно работают подразделения финансовой разведки (ПФР), растет экспоненциально. Однако главный вызов современности заключается не в сборе данных, а в их фильтрации: при увеличении потока сообщений о подозрительных операциях (СПО) нередко падает их практическая ценность. Последствие — аналитические ресурсы перегружены, а реальные риски замаскированы информационным шумом.

ЮНУСИ БЕЖАН МАХМАДЮСУФЗОДА
Начальник отдела обработки информации Департамента финансового мониторинга при Национальном банке Таджикистана

ПАРАДОКС ЦИФРОВИЗАЦИИ: ЧЕМ БОЛЬШЕ ДАННЫХ, ТЕМ МЕНЬШЕ ПРОЗРАЧНОСТИ

В соответствии с базовым Законом о противодействии отмыванию доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ) Департамент финансового мониторинга при Национальном банке Таджикистана (ДФМ НБТ) ежедневно получает отчеты об операциях, подлежащих обязательному информированию, а также отчеты о подозрительных сделках. Формирование и направление отчета о подозрительных операциях осуществляется согласно действующему реестру признаков подозрительных операций и сделок, что задает нормативную основу для идентификации и классификации событий, требующих дальнейшей аналитической проверки.

В 2022 году ДФМ НБТ зарегистрировал аномальный рост числа СПО, поступивших от субъектов финансового мониторинга. На первый взгляд, это выглядело как усиление комплаенс-активности банков. Однако стратегический анализ, проведенный нами по итогам 2022 — первого полугодия 2023 года, выявил тревожную тенденцию. Значительная часть этих сообщений носила формальный характер и не содержала обоснованных подозрений, связанных с ОД/ФТ.

Возникли ключевые вопросы: почему банки направляют СПО без хотя бы первичной аналитической проработки? Почему автоматизированные банковские системы (АБС) считаются конеч-

ной инстанцией? И как вернуть аналитику главенствующую роль в процессе принятия решений?

ИСТОЧНИКИ И МЕТОДОЛОГИЯ: МНОГОМЕРНЫЙ АНАЛИЗ

Для ответа на эти вопросы мы инициировали исследование, использовав принципы анализа разных источников, рекомендованные ФАТФ и Группой «Эгмонт». Наши аналитики изучили:

- базу данных отчетности по подозрительным операциям (форма № 101);
- алгоритмы автоматического выявления подозрительных операций, встроенные в АБС банков;
- результаты выездных проверок и наши собственные аналитические заключения.

Методологический подход объединял количественный анализ (распределение СПО по банкам и критериям) и качественную оценку (соответствие реестру признаков подозрительных операций и сделок, наличие аналитической логики).

Результаты показали, что проблема носит системный характер и усугубилась ослаблением надзорного влияния в период моратория на проверки в 2022 году.

ОТЧЕТ СПО: ИСТОРИЯ ЛОЖНЫХ СРАБАТЫВАНИЙ

Исследование выявило системный характер проблемы: так, 30% банков направили в ДФМ около 73% общего объема СПО. Столь высокая доля свидетельствовала не о повышенной криминогенности их клиентов, а о серьезных сбоях в логике работы их программного обеспечения.

Наибольший объем необоснованных сообщений был сформирован по трем типовым критериям.

1. Переводы без открытия счета от нерезидентов.
2. Операции через страны, ошибочно классифицированные как «зоны высокого риска».
3. Множественные операции, не соответствующие официальному доходу клиента.

Итоги анализа показали, что около 60% всех СПО, направленных по этим критериям, были сгенерированы автоматически и отправлены в ДФМ НБТ без какого-либо участия аналитика. Комплаенс-службы подменили понятие «операция может быть подозрительной» понятием «операция обязательно подозрительна», что снизило аналитическое качество отчетности.

Были случаи, когда сообщения направлялись на каждый трансграничный перевод, не учитывая контекст: гражданство отправителя, социально-экономический смысл операции (например, регулярные переводы мигрантов) или наличие подтверждающих документов.

ПРОБЛЕМА, ЗНАКОМАЯ ВСЕМУ РЕГИОНУ

Выявленная проблема — не уникальная для Таджикистана: она характерна для многих государств региона, переживающих активный этап цифровизации финансового сектора. В ходе анализа мы обращались к опыту коллег по Евразийской группе по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ) и консультировались со специалистами Международного учебно-методического центра финансового мониторинга (МУМЦФМ).

Исследования, проводившиеся МУМЦФМ совместно с ведущими научными институтами еще в начале 2010-х годов, показали: никакой алгоритм не способен полностью заменить профессиональное суждение аналитика. Алгоритмы эффективны для отсечения очевидных шаблонных операций, но гибкое распознавание сложных схем отмывания требует опыта и риск-ориентированного мышления.

Особую ценность в этом контексте приобретают образовательные проекты. Выпуск базового учебного пособия «Особенности национальных систем ПОД/ФТ государств Евразийского региона», третий том которого посвящен именно Таджикистану, стал важным вкладом в формирование нового поколения специалистов, которые понимают: слепое доверие к машине — это профессиональная некомпетентность.

«Выпуск базового учебного пособия «Особенности национальных систем ПОД/ФТ государств Евразийского региона», третий том которого посвящен именно Таджикистану, стал важным вкладом в формирование нового поколения специалистов, которые понимают: слепое доверие к машине — это профессиональная некомпетентность.

СТРАТЕГИЧЕСКИЕ ВЫВОДЫ: СИСТЕМНЫЙ СБОЙ

По итогам анализа ДФМ НБТ сформулировал ключевые выводы, которые легли в основу нашей новой политики.

Вывод первый. Резкий рост количества СПО в 2022 году не отражал реального увеличения рисков ОД/ФТ. Он был вызван институциональными и процедурными факторами: ослаблением надзора, кадровым дефицитом в комплаенс-службах и низким качеством алгоритмов АБС.

Вывод второй. Произошло опасное смещение ответственности. Автоматизированные системы и алгоритмы стали восприниматься сотрудниками как самостоятельный инструмент принятия решений, что привело к снижению роли профессионального аналитического суждения. Ключевое значение имеет участие специалиста, а машина должна лишь помогать ему обрабатывать большие массивы данных.

Вывод третий. Перегрузка наших аналитических ресурсов из-за массового потока формальных сообщений негативно сказалась на эффективности обработки действительно рискованных операций.

ПРИНЯТЫЕ МЕРЫ: НАСТРОЙКА СИСТЕМЫ

На основе результатов анализа ДФМ НБТ реализован комплекс мер, охвативших методологические, технологические и кадровые аспекты.

Методологические разъяснения

В адрес кредитных организаций были направлены инструкции, особо подчеркивающие, что критерии подозрительности носят оценочный характер и не являются безусловным основанием для направления СПО. Выявление признака должно служить основанием для углубленного анализа, а не для автоматического отчета.

Корректировка автоматизации и новая форма для комплаенса

Появилась необходимость отмены практики автоматической отправки СПО, сформированных АБС. Была создана специальная форма для заполнения СПО именно для комплаенса, где указываются причины подозрительности. Исключение сделано лишь для операций, связанных с финансированием терроризма. Банки обязаны пересмотреть алгоритмы с целью исключения ложноположительных срабатываний и обеспечить обязательное участие ответственных сотрудников комплаенс-служб в процессе принятия решений о направлении сообщений.

Кадровые меры

ДФМ НБТ рекомендовал увеличить численность комплаенс-служб в проблемных организациях и обеспечить повышение квалификации сотрудников в части корректной интерпретации критериев подозрительности и применения риск-ориентированного подхода.

МЕЖДУНАРОДНОЕ ИЗМЕРЕНИЕ: В КОНТЕКСТЕ ЕАГ

ДФМ НБТ работал в координации с партнерами по Евразийской группе. Приоритетные направления сегодня — оценка рисков, применение риск-ориентированного подхода и взаимодействие с правоохранительными органами.

Опыт ДФМ НБТ, где по итогам стратегического анализа были скорректированы подходы к автоматизации и усилена роль профессионального суждения, может быть полезен для всего региона. Именно поэтому ДФМ НБТ активно делится им на площадках ЕАГ и СРПФР (Совет руководителей подразделений финансовой разведки государств — участников СНГ) и участвует в подготовке совместных образовательных программ.

Принятые нами меры уже начинают приносить результаты. Сокращение доли необоснованных СПО позволяет нашему аналитическому подразделению фокусироваться на действительно сложных кейсах, требующих глубокого погружения и межведомственного взаимодействия.

Налоговый контроль как элемент системы финансовой безопасности государства: РОЛЬ ЦИФРОВЫХ ИНСТРУМЕНТОВ

В статье рассматривается взаимосвязь налоговых правонарушений и процессов легализации преступных доходов. Уклонение от уплаты налогов анализируется как один из первичных этапов формирования теневого капитала, который впоследствии может вовлекаться в схемы отмывания денежных средств.

На основе практики налогового администрирования Кыргызской Республики показано значение цифровых инструментов контроля — прежде всего информационных систем «Электронный счет-фактура» и «Салык Күзөт» — при выявлении разрывов в товарных цепочках и фиктивного документооборота.

Обосновывается, что цифровизация налогового администрирования формирует механизм раннего выявления финансовых аномалий и становится важным элементом системы противодействия легализации преступных доходов.

Особое внимание уделено аналитическим индикаторам подозрительных операций, финансовому мониторингу и межведомственному обмену информацией как факторам повышения эффективности финансового контроля и укрепления финансовой безопасности государства.

АЗАТ АЛМАНБЕТОВ
Заместитель председателя Государственной налоговой службы при Кабинете Министров Кыргызской Республики

В правовой системе Кыргызской Республики налоговые преступления рассматриваются как классические предикатные деяния. Согласно национальному законодательству в сфере противодействия легализации преступных доходов и международным стандартам Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) сокрытие доходов от налогообложения является одним из источников формирования незаконных финансовых активов.

Для дальнейшего использования таких средств в легальном секторе экономики, как правило, требуется их последующая легализация, включающая этапы размещения, расслоения и интеграции. Без прохождения этих процедур использование средств, полученных незаконным путем, остается рискованным для бенефициаров компаний.

Актуальность темы усиливается масштабной цифровизацией налогового администрирования в Кыргызской Республике, активно развивающейся с 2025 года. В стране внедрены и успешно работают электронные счета-фактуры, онлайн контрольно-кассовая техника и системы мониторинга движения товаров.

Эти инструменты позволяют выявлять разрывы в цепочках добавленной стоимости. Подобные разрывы нередко используются не только для минимизации налоговых обязательств, но и для транзита денежных средств с целью их последующей легализации.

В этих условиях налоговый контроль постепенно выходит за рамки исключительно фискаль-

ной функции и становится элементом системы финансовой безопасности государства, позволяя выявлять незаконные финансовые потоки на ранних этапах их формирования.

Настоящая статья посвящена анализу взаимосвязи налоговых правонарушений и процессов легализации преступных доходов, а также оценке роли цифровых инструментов налогового администрирования в выявлении финансовых аномалий и подозрительных операций.

Налоговые правонарушения рассматриваются не только как фискальные нарушения, но и как один из ключевых предикатных механизмов формирования теневого капитала, вовлекаемого в схемы легализации преступных доходов. Особое внимание уделяется анализу возможностей цифровых систем налогового контроля в выявлении транзитных финансовых потоков и фиктивного документооборота.

НАЛОГОВЫЕ СХЕМЫ КАК ИСТОЧНИК ФОРМИРОВАНИЯ ТЕНЕВОГО КАПИТАЛА

В современной экономике Кыргызской Республики одним из основных источников формирования теневого капитала остаются схемы уклонения от уплаты налогов. Наиболее распространенными среди них являются использование фиктивного документооборота и искусственное дробление бизнеса.

Субъекты предпринимательства могут использовать электронные счета-фактуры от сомнительных поставщиков для необоснованного зачета налога на добавленную стоимость и завышения расходов.

В подобных ситуациях налоговое правонарушение проявляется в минимизации налоговых обязательств. Однако финансовая составляющая операций фактически представляет собой транзит денежных средств на счета фиктивных компаний с последующим их обналичиванием.

Таким образом, неуплаченные налоги трансформируются в незаконные финансовые ресурсы, которые впоследствии нуждаются в легализации.

Другой распространенной схемой является искусственное разделение крупного предприятия на несколько взаимосвязанных субъектов, применяющих льготные налоговые режимы.

Такая модель позволяет снизить налоговую нагрузку и аккумулировать неучтенную прибыль на счетах аффилированных лиц. С точки зрения механизмов легализации преступных доходов это может соответствовать этапу размещения финансовых средств.

> **«Налоговый контроль постепенно выходит за рамки исключительно фискальной функции и становится элементом системы финансовой безопасности государства, позволяя выявлять незаконные финансовые потоки на ранних этапах их формирования.**

АНАЛИТИЧЕСКИЕ ИНДИКАТОРЫ ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЙ

В связи с этим особое значение приобретает система аналитических индикаторов, позволяющих выявлять признаки подобных финансовых схем.

В процессе налогового администрирования используются аналитические индикаторы, позволяющие выявлять взаимосвязь между налоговыми правонарушениями и возможной легализацией преступных доходов.

К числу наиболее значимых индикаторов относятся:

- несоразмерность налоговой нагрузки и оборотов, когда при значительном росте оборота налоговые выплаты остаются минимальными;
- аномалии в структуре дебиторской и кредиторской задолженности, включая значительное увеличение обязательств перед сомнительными контрагентами;
- транзитный характер движения денежных средств, при котором поступившие средства в короткие сроки перечисляются другим субъектам без очевидного экономического смысла;
- несоответствие финансовых операций профилю деятельности компании, например проведение крупных операций при отсутствии необходимых ресурсов.

Использование подобных индикаторов позволяет выявлять компании, вовлеченные в транзитные финансовые схемы.

ФИНАНСОВЫЙ МОНИТОРИНГ И АНАЛИЗ ПОДОЗРИТЕЛЬНЫХ ОПЕРАЦИЙ

Финансовый мониторинг является важным элементом системы противодействия легализации

преступных доходов. Налоговые органы участвуют в выявлении подозрительных операций путем анализа финансово-хозяйственной деятельности налогоплательщиков.

В рамках такой аналитической работы проводится:

- анализ крупных денежных операций;
- контроль транзакций, не соответствующих профилю деятельности налогоплательщика;
- мониторинг операций с наличными денежными средствами;
- выявление возможных схем вывода капитала за рубеж;
- анализ трансграничных финансовых операций.

Следует отметить, что органы налоговой службы Кыргызской Республики не имеют доступа к банковским операциям налогоплательщиков в режиме реального времени. Взаимодействие с банковскими учреждениями осуществляется в соответствии со статьей 146 Налогового кодекса Кыргызской Республики.

В целях реализации данной нормы 4 июля 2024 года было принято постановление Кабинета Министров Кыргызской Республики № 363, которым утвержден порядок предоставления банками и платежными организациями информации органам налоговой службы.

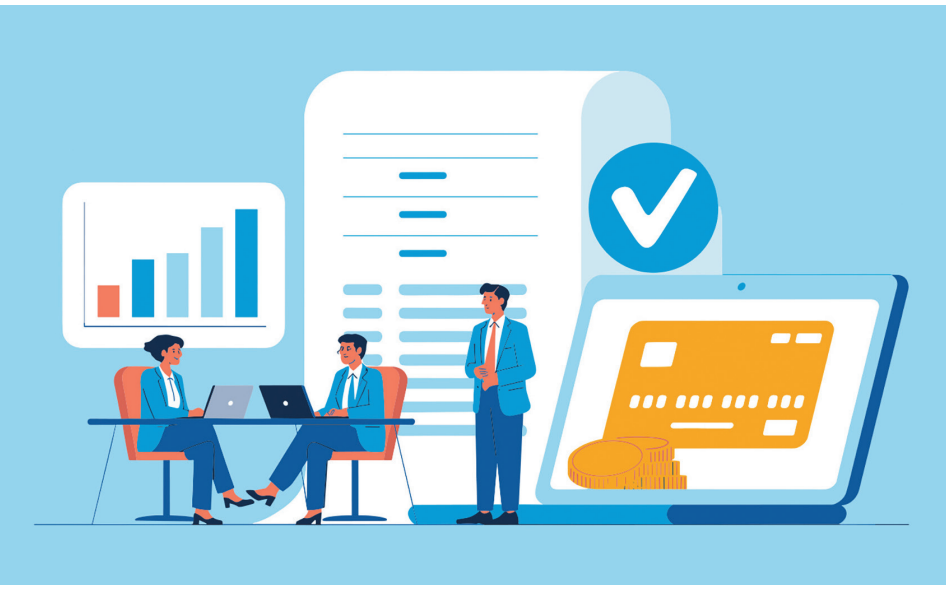
Для реализации этого механизма в системе «Кабинет инспектора» разработан модуль «Взаимодействие с банками», позволяющий формировать официальные запросы в коммерческие банки для получения информации по счетам налогоплательщиков.

Банки обязаны предоставлять информацию в течение пяти рабочих дней. При этом сведения об операциях по счетам организаций и индивидуальных предпринимателей могут предоставляться только в предусмотренных законодательством случаях:

- при проведении выездной налоговой проверки;
- при проведении камеральной проверки на основании решения налогового органа;
- при ликвидации юридического лица либо прекращении деятельности индивидуального предпринимателя.

Помимо банковской информации, налоговые органы проводят аналитическую работу на основе данных электронных счетов-фактур, таможенных деклараций, сопроводительных накладных и налоговой отчетности.

Сопоставление этих сведений позволяет выявлять несоответствия в финансово-хозяйственной деятельности налогоплательщиков и потенциальные налоговые риски.



ВЫЯВЛЕНИЕ И ПРЕСЕЧЕНИЕ СХЕМ УКЛОНЕНИЯ ОТ НАЛОГОВ И ЛЕГАЛИЗАЦИИ ДОХОДОВ

Одной из ключевых задач налоговых органов является обеспечение полноты и своевременности поступления налогов в бюджет, а также контроль за соблюдением налогового законодательства.

Анализ финансово-хозяйственной деятельности налогоплательщиков проводится на основе данных налоговой отчетности, электронных счетов-фактур, таможенных деклараций и других информационных ресурсов.

Одной из наиболее распространенных схем является использование фиктивных компаний, через которые оформляются мнимые сделки и электронные счета-фактуры.

Как правило, такие организации не ведут реальной хозяйственной деятельности и используются исключительно для оформления фиктивных договоров на поставку товаров или оказание услуг. На основании этих документов формируются расходы и налоговые вычеты, не имеющие фактического экономического содержания.

В результате формируется цепочка взаимосвязанных операций, позволяющая искусственно увеличивать расходы, уменьшать налоговую базу и затруднять выявление конечных получателей денежных средств.

Еще одной распространенной схемой является искусственное распределение единой хозяйственной деятельности между несколькими взаимосвязанными субъектами.

Нередко в подобных схемах регистрируется несколько индивидуальных предпринимателей, применяющих упрощенную систему налогообложения на основе единого налога со ставкой 0%, при которой годовой оборот не должен превышать установленный лимит в 15 млн сомов.

Фактически деятельность осуществляется как единый бизнес, однако формальное распределение оборота между несколькими субъектами позволяет сохранять льготный налоговый режим и снижать налоговые обязательства.

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ И РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

Развитие цифровых технологий существенно расширило возможности выявления подобных финансовых схем.

Одним из ключевых факторов повышения эффективности налогового администрирования стала цифровизация налогового контроля.

▸ **Одной из используемых систем является автоматизированная система контроля НДС,** предназначенная для анализа отчетности по налогу на добавленную стоимость и проведения камеральных проверок.

Система обеспечивает:

- поиск расхождений по НДС;
- визуально-сетевой анализ хозяйственных связей;
- анализ цепочек поставок;
- формирование аналитических отчетов;
- оценку налоговых рисков;
- формирование досье налогоплательщика.

Модуль «Сравнительный анализ» позволяет сопоставлять данные первичных документов и налоговой отчетности, автоматически выявляя отклонения между фактическими операциями и отраженными в отчетности показателями.

Дополнительные аналитические возможности предоставляет информационная система «Салык Күзөт», предназначенная для объединения данных различных государственных информационных ресурсов и формирования комплексной аналитики налоговых рисков.

В рамках межведомственного взаимодействия налоговые органы также осуществляют электронный обмен данными с рядом уполномоченных государственных органов.

Сопоставление сведений о собственности, транспортных средствах, внешнеэкономических операциях и регистрационных данных налогоплательщиков с информацией налоговой отчетности и электронных счетов-фактур существенно расширяет возможности выявления налоговых рисков.

Проведенное исследование показывает, что налоговые правонарушения могут выступать одним из ключевых источников формирования незаконных финансовых ресурсов, которые в дальнейшем вовлекаются в процессы легализации преступных доходов.

Анализ практики налогового администрирования свидетельствует, что уклонение от уплаты налогов нередко сопровождается использованием фиктивного документооборота, транзитных финансовых операций и технических компаний. Подобные механизмы позволяют формировать теневые финансовые потоки, которые впоследствии требуют легализации для их использования в легальном секторе экономики.

Развитие цифровых технологий существенно расширило возможности выявления подобных схем. Использование информационных систем налогового контроля, включая информационные системы «Электронный счет-фактура» и «Салык Күзөт», позволяет выявлять разрывы в цепочках поставок, признаки бестоварных операций и транзитных финансовых потоков на ранних этапах их формирования.

В этих условиях налоговое администрирование приобретает дополнительное значение как инструмент обеспечения финансовой прозрачности и укрепления финансовой безопасности государства.

Повышение эффективности противодействия легализации преступных доходов требует дальнейшего развития аналитических инструментов налогового контроля, расширения межведомственного обмена информацией и совершенствования риск-ориентированных методов анализа финансовых операций.

«Модуль «Сравнительный анализ» позволяет сопоставлять данные первичных документов и налоговой отчетности, автоматически выявляя отклонения между фактическими операциями и отраженными в отчетности показателями.

От децентрализации к эксплуатации:

РОСТ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТЫ В ФИНАНСОВЫХ ПРЕСТУПЛЕНИЯХ С ПРИМЕНЕНИЕМ КИБЕРТЕХНОЛОГИЙ И ВЫЗОВЫ ДЛЯ УПРАВЛЕНИЯ РИСКАМИ В БАНКОВСКОМ СЕКТОРЕ

Криптовалюта может рассматриваться как альтернативная форма валюты, обеспечивающая более высокую степень автономии и контроля за счет минимизации участия государств и центральных банков и тем самым позволяющая формировать децентрализованную экономическую систему. Одной из ключевых целей такой децентрализованной природы является создание системы расчетов, которая работает быстро, с минимальными затратами и не требует участия доверенных третьих сторон.

ИБРАХИМ АРИФИН
Директорат по правовым вопросам и регулированию, подразделение финансовой разведки Индонезии (PPATK)

Изначально биткоин создавался в конструктивных целях — как электронная платежная система, позволяющая проводить расчеты напрямую между сторонами без участия доверенных посредников. Благодаря использованию криптографического подтверждения и децентрализованных механизмов система была задумана как инструмент обеспечения безопасности, прозрачности и защиты от мошеннических действий в цифровых транзакциях[1].

Однако по мере развития использование этой технологии не всегда соответствовало ее первоначальным целям. Те самые характеристики, которые обеспечивают эффективность и гибкость расчетов, отдельные участники начали использовать для сокрытия финансовых потоков и содействия различным формам финансовых преступлений. В результате инновация, изначально призванная укрепить целостность платежных систем, на практике создала новые вызовы для предупреждения и пресечения преступной деятельности.

РОСТ ЧИСЛА ВЗЛОМОВ БАНКОВСКИХ СЧЕТОВ И СМЕЩЕНИЕ К КРИПТОВАЛЮТНЫМ ПОТОКАМ

Мошенничество с использованием кибертехнологий стало одной из наиболее распространенных и разрушительных форм преступности в мире, генерируя значительные объемы преступных доходов за счет эксплуатации жертв в различных юрисдикциях[2]. За последние три года банковский сектор Индонезии столкнулся с существенным ростом кибератак в форме неправомерного доступа, что привело к масштабным фи-

[1] Накамото С. (2008) Биткоин: одноранговая электронная платежная система.

[2] ФАТФ (2026). Мошенничество с использованием кибертехнологий: цифровизация и риски отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения. Париж: Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ).

нансовым потерям. Совокупный ущерб по нескольким выявленным делам достиг примерно 300 млрд индонезийских рупий. Эта цифра отражает не только масштаб экономического вреда, но и свидетельствует о росте как возможностей, так и операционных моделей финансовой преступности, основанной на технологиях.

Случай, произошедший в конце февраля 2026 года, является наиболее свежей иллюстрацией этого явления. Около 6 тысяч клиентских счетов были неправомерно доступны, в результате чего в течение относительно короткого срока было незаконно переведено около 143 млрд индонезийских рупий[3]. Помимо финансового ущерба, инцидент нарушил и работу цифрового банковского обслуживания: сервисы мобильного банка были временно недоступны, что потребовало изменения механизмов проведения операций.

Дальнейшее расследование выявило серьезные признаки того, что часть преступных доходов была переведена на счета, аффилированные с криптокошельками. Этот паттерн не является единичным. Годом ранее аналогичный взлом банковских счетов привел к потерям примерно на 119 млрд[4] индонезийских рупий, а двумя годами ранее сопоставимый случай причинил ущерб примерно на 21 млрд индонезийских рупий. В совокупности эти инциденты демонстрируют устойчивую тенденцию: банковский сектор становится точкой входа для преступной деятельности, которая затем перемещается в криптоэкосистему.

Кроме того, факты, установленные в ходе судебных разбирательств, указывают на то, что привлеченные к ответственности и осужденные лица не были интеллектуальными организаторами этих преступлений. Как правило, задержанные выполняли ограниченные функции, например, предоставляли номинальные счета, использовавшиеся для получения и перевода преступных доходов. Это свидетельствует о существовании более сложной организованной преступной структуры с четким распределением ролей между техническими исполнителями, посредниками при проведении транзакций и основными виновными лицами, которые в значительной степени остаются неустановленными.

Сравнительный анализ этих дел выявляет устойчивую операционную модель. Во-первых, преступники используют большое количество номинальных счетов в качестве первоначальных хранилищ для средств, полученных в результате неправомерного доступа (этап размещения в контексте легализации преступных доходов). Во-вторых, аккумулированные средства быстро конвертируются в криптоактивы, прежде всего в стейблкоины, в рамках этапа расслоения. Такая конвертация осуществляется с использованием различных механизмов, включая пиринговые (P2P) схемы и криптобиржевые платформы, что позволяет быстро переводить средства через границы.

Свежие данные дополнительно подчеркивают возрастающую роль стейблкоинов в противоправной деятельности. Стейблкоины все чаще используются для легализации преступных доходов, финансирования терроризма и финансирования распространения оружия массового уничтожения. По имеющимся оценкам, в последние годы на них приходилась значительная доля противоправных транзакций с виртуальными активами. Недавний случай взлома банковских счетов также указывает на высокую вероятность сохранения этой тенденции[5].

С практической точки зрения такие схемы создают серьезные трудности для правоохранительных органов и подразделений финансовой разведки при розыске активов, их заморозке и конфискации. Скорость перемещения средств в сочетании с многоуровневой структурой транзакций приводит к крайне узкому временному окну между совершением преступления и возможностью вмешательства властей. Во многих случаях средства уже успевают попасть в криптоэкосистему еще до того, как можно принять действенные меры принуждения.

Таким образом, изложенные выше обстоятельства показывают, что преступность, связанная с банковским сектором, претерпела фундаментальную трансформацию. Modus operandi (с лат. «образ действия». — *Прим. ред.*) больше

«Около 6 тысяч клиентских счетов были неправомерно доступны, в результате чего в течение относительно короткого срока было незаконно переведено около 143 млрд индонезийских рупий.

[3] ANTARA News Jambi (2026) // Полиция зафиксировала убытки Банка Джамби в размере 143 млрд индонезийских рупий в результате взлома системы.

[4] Nusantara Abadi News (2025) // Предполагаемый взлом на сумму 100 млрд индонезийских рупий в Bank Jatim: обвиняемый Абдул Рахим подал возражение, судебное разбирательство обостряется.

[5] ФАТФ (2026) Целевой доклад о стейблкоинах и некастодиальных кошельках — пиринговые (P2P) транзакции. Париж: Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ).

не заканчивается неправомерным завладением средствами, а превратился в технологически интегрированный процесс, направленный на системное сокрытие происхождения преступных доходов и усложнение правоприменительных действий. Высокая скорость транзакций и ликвидность криптоактивов создают значительные вызовы не только для Индонезии, но и для юрисдикций по всему миру, поскольку преступники все активнее используют эти инструменты, чтобы маскировать противоправные средства и придавать им видимость легитимности[6].

МЕРЫ БАНКОВСКОГО СЕКТОРА ПО СНИЖЕНИЮ РИСКОВ, СВЯЗАННЫХ С ФИНАНСОВЫМИ ПРЕСТУПЛЕНИЯМИ С ИСПОЛЬЗОВАНИЕМ КРИПТОАКТИВОВ

Исходя из моделей, выявленных в различных делах о взломе банковских счетов, очевидно, что modus operandi преступников носит структурированный и повторяющийся характер. В этих условиях банки как организации, действующие на основе принципа банковской осмотрительности, должны не только реагировать постфактум, но и проактивно предвосхищать риски, особенно те, которые уже приобрели достаточно четкие признаки.

С учетом этого банковский сектор может предпринять несколько конкретных шагов для усиления снижения рисков на стыке киберпреступности и использования криптоактивов.

Во-первых, банкам необходимо разработать и внедрить специальные риск-индикаторы для выявления транзакций, связанных с высокорискованной деятельностью в сфере криптоактивов. Такие индикаторы должны не только фиксировать транзакционные аномалии, но и выявлять модели конвертации средств из банковской системы в криптоэкосистему. К релевантным параметрам могут относиться высокочастотные транзакции в короткие промежутки времени, использование нескольких счетов со сходными клиентскими профилями, а также потоки средств, направляемые в адрес конкретных организаций или криптоплатформ. В этой связи для обеспечения комплексного мониторинга транзакций крайне важно расширять обмен информацией между банками и провайдерами криптосервисов.

Во-вторых, критически важно усилить механизмы «Знай своего клиента» (ЗСК), чтобы закрыть уязвимость, связанную с использованием номинальных счетов. Эмпирические данные показывают, что успешность этапа расслоения во многом зависит от наличия счетов, не отражающих реального бенефициарного собственника (владельца). Технологическое развитие, включая злоупотребление цифровой идентификацией и технологиями дипфейков, еще больше повышает этот риск. Поэтому банкам необходимо усиливать процедуры верификации личности и постоянную надлежащую проверку клиентов (НПК). Это особенно важно, поскольку доступность данных о криптокошельках теряет эффективность, если счета, используемые как точки входа в криптоэкосистему, открыты по недействительным или заимствованным данным.

В-третьих, необходимо укреплять механизмы раннего вмешательства посредством внедрения мер по замораживанию подозрительных транзакций в режиме реального времени. Одной из ключевых проблем, выявленных в этих делах, является крайне узкий временной интервал между самим взломом и быстрым перемещением средств через несколько уровней, включая их конвертацию в криптоактивы. В таких условиях решающим фактором становится скорость реагирования. Банки должны обладать возможностью автоматизированного выявления подозрительных транзакций с последующей немедленной временной заморозкой при эффективной координации с компетентными органами. Такой подход позволяет вмешаться до того, как средства будут переведены в более сложные и менее отслеживаемые системы.

Для сравнения, международная практика показывает, что некоторые финансовые учреждения уже применяют более прогрессивные подходы, ограничивая транзакции, направляемые на высокорискованные криптоплатформы. Это демонстрирует, что снижение рисков не ограничивается выявлением, а включает и прямой контроль за потоками средств в критических точках.

В заключение следует отметить, что работа по снижению рисков в банковском секторе должна вестись комплексно и охватывать предупреждение, выявление и реагирование. Эти три элемента должны действовать одновременно, поскольку природа финансовой преступности развилась, начав активно использовать скорость и сложность современных цифровых финансовых систем.

[6] Арифин И., Юстисия О., Анданте Р. // Стейблкоины: новый инструмент для легализации преступных доходов? Оптимизация роли режима ПОД/ФТ в противодействии неправомерному использованию стейблкоинов, журнал «Финансовая безопасность», № 47, декабрь, 2025.

КИБЕРПАТРУЛИРОВАНИЕ И МОНИТОРИНГ ДАРКНЕТА:

как правоохранительные органы используют ИКТ для выявления и пресечения финансовых преступлений в темной сети

СЕРГЕЙ КОНДРАТЬЕВ

Старший оперуполномоченный по особо важным делам отдела по противодействию имущественным преступлениям, совершенным в сфере компьютерной информации, Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России, подполковник полиции

АРТЕМ ЧОЗГИЯН

Оперуполномоченный отдела по противодействию имущественным преступлениям, совершенным в сфере компьютерной информации, Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России, лейтенант полиции

Массовые финансовые преступления уже давно перестали быть делом отдельных мошенников-энтузиастов. Сегодня их совершают организованные группы и даже целые преступные сообщества, действующие по отработанным схемам и использующие передовые информационно-коммуникационные технологии. Особую тревогу вызывает тот факт, что значительную долю таких преступлений на территории Российской Федерации совершают участники транснациональных преступных формирований, находящихся за пределами Российской Федерации, которые не только владеют высокотехнологичными инструментами кибератак, но и имеют отлаженную инфраструктуру для вывода похищенных средств.

Одним из ключевых инструментов обогащения преступников является использование ресурсов даркнета. Именно в этом анонимизированном сегменте интернета размещаются предложения о «бизнес-проектах», под видом которых вербуются российские граждане, готовые выступить в роли пособников и обеспечить локальную поддержку на территории нашей страны для инфраструктуры, обеспечивающей вывод значительных денежных средств за границу.

В этом же сегменте при желании можно отыскать предложения о

«Одним из эффективных методов, применяемых УБК МВД России в технологическом противостоянии, стало киберпатрулирование — систематическая, непрерывная деятельность по мониторингу, анализу и контролю противоправной активности в цифровой среде, включая даркнет.

продаже банковских карт, оформленных на третьих лиц, для использования в противоправной деятельности.

Кроме того, в недрах глубинного интернета скрываются многочисленные тематические сообщества, являющиеся онлайн-площадками для обмена опытом и распространения новых схем мошенничества.

Для противодействия этой угрозе в структуре МВД России существует специализированное подразделение — Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России[1], которое является головным подразделением по борьбе с киберпреступностью.

Одним из эффективных методов, применяемых УБК МВД России в этом технологическом противостоянии, стало киберпатрулирование — систематическая, непрерывная деятельность по мониторингу, анализу и контролю противоправной активности в цифровой среде, включая даркнет.

Эта практика позволяет не просто реагировать на уже совершенные преступления, а выявлять и пресекать их на стадии подготовки.

Особую эффективность киберпатрулированию придает использование специализированного программного обеспечения собственной разработки. Такие системы способны анализировать огромные массивы данных, выявлять скрытые связи между участниками преступных сетей и прогнозировать их дальнейшие действия. Использование высоких технологий придает проактивный характер правоохранительной деятельности УБК МВД России в цифровой среде и создает технологическую платформу, позволяющую действовать на опережение преступников.

Результаты такой системной работы стали очевидны уже в 2025 году: впервые в истории современной России было зафиксировано снижение количества массовых финансовых преступлений, совершаемых с использованием ИКТ. Это достижение напрямую связано с переходом от реактивного реагирования к постоянному, технологически оснащенному мониторингу цифрового пространства.

Таким образом, в условиях, когда финансовая преступность все глубже уходит в цифровую тень, эффективная защита общества и государства возможна только за счет перехода к проактивной модели противодействия. Киберпатрулирование и мониторинг даркнета, осуществляемые УБК МВД России с использованием собственных ИКТ-решений, становятся не просто инструментами раскрытия преступлений, а стратегическим ресурсом обеспечения национальной финансовой безопасности. Достигнутое в 2025 году снижение уровня массовых киберпреступлений — наглядное подтверждение того, что технологически оснащенное правоохранительное присутствие в глубинном интернете способно разрушать преступную инфраструктуру еще до того, как она нанесет ущерб гражданам и экономике страны.

По данным ФКУ «ГИАЦ МВД России» в январе – декабре 2025 года оперативная обстановка на территории Российской Федерации в сфере противоправного использования ИКТ характеризуется снижением на 12,2% зарегистрированных преступлений (с 755 094 до 663 224), а также на 5,3% тяжких и особо тяжких (с 363 375 до 344 181).

Удельный вес противоправных деяний в сфере противоправного использования ИКТ составляет 42,1% общего количества совершенных преступлений.

Основной массив противоправных деяний в сфере ИКТ на 65% сформирован преступлениями против собственности (–12,5%; с 492 594 до 430 981).

Раскрываемость преступлений в сфере ИКТ составила 25,7% (2024 г. — 22,5%).

Отмечается снижение на 5,2% материального ущерба, причиненного противоправными деяниями, совершенными с использованием ИКТ (с 200,1 млрд до 189,6 млрд рублей).

[1] Далее — УБК МВД России.

ПРОТИВОДЕЙСТВИЕ ФИНАНСОВЫМ ПРЕСТУПЛЕНИЯМ С ИСПОЛЬЗОВАНИЕМ НОВЫХ ТЕХНОЛОГИЙ В ЗАПАДНОЙ АФРИКЕ

Африканский континент нередко характеризуют как самый «молодой» на планете. Хотя это утверждение может быть оспорено историками, с точки зрения социально-экономических показателей и темпов догоняющего развития Африка по-прежнему уступает другим регионам мира. Тем не менее данное отставание не является ключевой проблемой. Основная особенность современного этапа развития континента заключается в стремительной технологической экспансии. При условии эффективного применения технологии способны стать тем рычагом, который позволит сократить разрыв между Африкой и развитыми странами, а также выровнять условия в различных юрисдикциях. В настоящей статье основное внимание уделено региону Западной Африки; для иллюстрации ключевых тезисов рассматриваются отдельные примеры из практики различных государств этой части континента.

МЕЛАЙЕ ТИМОТИ ФЕМИ
Глава нигерийского офиса и исполняющий обязанности главы по коммуникациям и адвокации Межправительственной группы по борьбе с отмыванием денег в Западной Африке (ГИАБА)

Новые технологии открывают значительные возможности для экономического роста, повышения скорости проведения операций и внедрения инновационных решений. Однако одновременно они порождают и новые вызовы. К их числу относятся рост киберпреступности, интернет-мошенничество, конвертация похищенных ресурсов в виртуальные активы, кража персональных данных (кража личности), а также использование контента, созданного с применением искусственного интеллекта. Дополнительные риски возникают в связи с высокой степенью анонимности участников финансовых транзакций.

В условиях глобального роста преступной деятельности использование передовых технологий для противодействия ей становится насущной необходимостью. Африка постепенно расширяет внедрение технологических решений в этой сфере. Наблюдается рост использования виртуальных активов. Так, Нигерия занимает второе или третье место в мире по объему использования виртуальных активов (ВА) и провайдеров услуг виртуальных активов (ПУВА). Кения и Южная Африка также входят в число стран с высоким уровнем их использования. Данное явление имеет как преимущества, так и риски. Популяризация подобных инструментов может способствовать росту финансовых преступлений, поскольку они облегчают трансграничное перемещение средств и активов, существенно усложняя отслеживание финансовых потоков. Это, в свою очередь, снижает эффективность фундаментального принципа борьбы с криминальными доходами — «следуй за деньгами». В связи с этим принимаются согласованные меры по использованию технологий для обеспе-

чения соответствия требованиям, выявления рисков, внедрения превентивных мер, а также отслеживания и возврата похищенных активов.

Западная Африка демонстрирует заметный прогресс в использовании искусственного интеллекта (ИИ) для усиления борьбы с финансовыми преступлениями, включая отмывание денег, мошенничество и финансирование терроризма.

ФОРМИРОВАНИЕ ИНСТИТУЦИОНАЛЬНЫХ МЕХАНИЗМОВ

На международном и региональном уровнях разрабатываются масштабные стратегии, обусловленные глобальным осознанием угроз, внутриконтинентальными вызовами и спецификой финансовых преступлений. Фундаментальным этапом стало создание в 1989 году Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ). Впоследствии по ее образцу были сформированы региональные группы. В Африке функционируют четыре такие структуры: Межправительственная группа по борьбе с отмыванием денег в Западной Африке (ГИАБА), Группа по борьбе с отмыванием денег в Восточной и Южной Африке (ЕСААМЛГ), Группа по борьбе с отмыванием денег в Центральной Африке (ГАБАК), Группа разработки финансовых мер борьбы с отмыванием денег на Ближнем Востоке и в Северной Африке (МЕНАФАТФ), деятельность которой распространяется также на страны Ближнего Востока.

В каждой стране континента учреждено подразделение финансовой разведки (ПФР). Несмотря на то что они находятся на разных стадиях институционального развития, значительная часть из них уже входит в международную Группу «Эгмонт». Эти механизмы формируют основу для внедрения мер контроля в финансовом секторе и развития правовой базы. Часто отмечается, что в обществе без закона соблюдение закона теряет смысл. Поэтому многие страны пересмотрели законодательство с учетом современных требований, включая меры по противодействию новым видам финансовых преступлений. Такие реформы позволили определить функции государственного сектора, установить обязанности для частного сектора и вовлечь негосударственных участников, включая гражданское общество и средства массовой информации.

Региональные группы по типу ФАТФ (РГТФ) осуществляют широкий спектр мероприятий, направленных на поддержку стран в противодействии отмыванию денег и финансированию терроризма. Показательным примером является деятельность ГИАБА. Организация выполняет следующие функции:

а) координация стратегий по противодействию отмыванию денег и финансированию терроризма между государствами-членами;

б) проведение взаимной оценки — механизма экспертной оценки, который анализирует соответствие стран международным стандартам. Этот процесс позволяет государствам совершенствовать национальные системы и укреплять институциональный потенциал;

в) некоторые страны региона, включая Нигерию, Гану и Сенегал, внедрили более строгие меры и сформировали институциональные механизмы противодействия серьезным финансовым преступлениям. Благодаря этим усилиям данные государства были исключены из «серого» списка ФАТФ. Это свидетельствует о достигнутом прогрессе в обеспечении соответствия международным требованиям и усилении надзора. В результате повышается эффективность борьбы с финансовыми преступлениями на национальном уровне.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Как отмечалось ранее, страны Африки постепенно внедряют технологические решения для повышения эффективности противодействия финансовым преступлениям.

- Использование ИИ в качестве инструментов обеспечения соответствия
  - Многие финансовые учреждения внедряют системы на основе ИИ для выявления подозрительных транзакций в режиме реального времени. Это позволяет ускорить анализ и повысить точность результатов.
  - Такие системы превосходят традиционные нормативные модели анализа, поскольку способны выявлять скрытые закономерности в операциях мобильных платежей, финтех-сервисов и трансграничных электронных переводов. ИИ может использоваться, например, для классификации сообщений о подозрительных операциях (СПО) и проведения автоматизированного анализа.
- Выявление мошенничества в финтех-сфере
  - Стремительный рост мобильных платежей и цифрового банковского обслуживания приводит к увеличению объема транзакций. ИИ используется для мониторинга таких операций. Системы могут автоматически формировать уведомления и предоставлять первичный аналитический вывод.
  - Модели машинного обучения позволяют выявлять аномалии, снижать риски мошенничества и укреплять доверие потребителей.
  - Для обеспечения единообразия требований комплаенса новые автоматизированные системы помогают проводить

ПРИМЕРЫ ПРЕИМУЩЕСТВ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРЕДОТВРАЩЕНИИ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ (ИСТОЧНИК: FITC)

Проблема	Традиционный подход	Подход с использованием ИИ
Отмывание денег	Ручной аудит, медленная отчетность	Автоматизированное выявление подозрительных финансовых потоков
Мошенничество в финтех	Проверки на основе правил	Адаптивные модели машинного обучения, выявляющие новые схемы мошенничества
Трансграничные платежи	Ограниченный контроль	Мониторинг в режиме реального времени между юрисдикциями
Соответствие	Реактивное применение мер	Проактивное обеспечение соответствия международным стандартам ПОД/ФТ

надлежащую проверку клиента (НПК) в отношении всех новых клиентов финансовых учреждений.

ОСНОВНЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ ИИ

- **Качество и интеграция данных.** Системы ИИ зависят от доступности и стандартизации финансовых данных. В регионе такие данные представлены неравномерно. В результате система может использовать ограниченные массивы информации, что иногда приводит к менее точному отражению реальной ситуации.
- **Наращивание потенциала.** Регуляторы и участники финансового сектора нуждаются в специалистах, способных анализировать результаты работы систем ИИ.
- **Трансграничное сотрудничество.** Преступные сети используют различия между юрисдикциями. Поэтому необходима гармонизация региональных механизмов взаимодействия. Страны должны оперативно выявлять ключевые проблемные направления и совместно принимать меры по их устранению.

Подход Западной Африки сочетает реформы государственной политики (через деятельность ГИАБА и соблюдение стандартов ФАТФ) с технологическими инновациями, включая мониторинг на основе ИИ. Такое сочетание способствует модернизации механизмов противодействия все более сложным финансовым преступлениям.

В 2024 году в Нигерии было зафиксировано значительное увеличение интернет-мошенничества. Число случаев финансового мошенничества выросло на 45% по сравнению с предыдущим годом. Центральный банк Нигерии сообщил, что около 70% финансовых потерь связано с цифровыми каналами, прежде всего с нерегулируемыми платформами виртуальных активов. Комиссия по экономическим и финансовым преступлениям Нигерии зарегистрировала 2588 случаев интернет-мошенничества. Эти данные демонстрируют необходимость применения комплексных мер для противодействия экономическим и финансовым преступлениям. Рост мошенничества с использованием виртуальных активов и сложных инвестиционных схем требует более эффективных инструментов анализа. В этом контексте ИИ может использоваться для обработки больших массивов данных и проведения автоматизированного анализа. Итоговые результаты должны проверяться специалистами, которые принимают решения и формулируют рекомендации.

ЗАКЛЮЧЕНИЕ

При использовании технологий необходимо учитывать как преимущества, так и риски, включая возможные непреднамеренные последствия. Эти аспекты следует принимать во внимание при применении ИИ в борьбе с финансовыми преступлениями. Многие африканские государства уже внедряют новые технологические решения для сбора, анализа и использования данных в целях противодействия финансовым преступлениям.

ЛИТЕРАТУРА

FITC — Fraud and Forgery 2024 2nd Quarter.cdr

БЛОКИРОВКА ПРОТИВОПРАВНОГО КОНТЕНТА. СИСТЕМЫ МОНИТОРИНГА И ВЫЯВЛЕНИЯ

Порядок ограничения доступа к информации в условиях постоянно растущей цифровизации российского общества продолжает оставаться актуальной и общественно значимой проблематикой. Интернет-пространство сегодня является средством для моментального обмена информацией. Важным звеном в цепи регулирования подобных общественных отношений является деятельность органов государственной власти по реализации комплекса правовых механизмов, направленных на ограничение доступа к запрещенной информации.

ДМИТРИЙ СПИРЕВ
Представитель ФГУП «Главный радиочастотный центр», к.ю.н.

Российское законодательство за последнее время значительно расширило перечень оснований для включения в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено (далее — реестр), предусмотренных ст. 15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и другими нормативными правовыми актами[1]. Во многом это связано с углублением механизмов влияния на общественные отношения со стороны противоправных элементов, имеющих в том числе и зарубежное происхождение.

Эффективность деятельности по блокировке и предотвращению распространения противоправного контента в сети Интернет напрямую влияет на состояние стабильности общественных отношений российского общества. Вместе с тем эффективность такой деятельности во многом определяется комплексом факторов, одним из которых является система оперативного обнаружения противоправного контента.

Без своевременного обнаружения публикации с признаками нарушения действующего законодательства невозможны ни ее правовая оценка, ни последующее решение уполномоченного органа об ограничении доступа к информации. Для цифровой среды характерна высокая скорость тиражирования информации. Новость о событии моментально распространяется среди источников регионального, федерального и общемирового уровня. Анализ последних резонансных происшествий, связанных, например, с нападением на учебные заведения, показывает, что момент между преступным деянием и появлением новостных публикаций о нем (в том числе и с признаками нарушения действующего законодательства) неуклонно сокращается.

Один и тот же материал может быть воспроизведен на различных платформах и видеохостингах, в социальных сетях и мессенджерах. Особую сложность создает и использование анонимных аккаунтов, сетей прокси-серверов, распределенных каналов распространения информации.

Отдельного внимания заслуживает феномен мессенджеров, где публикации могут размещаться как в публичных каналах, так и в закрытых группах. Это объективно усложняет выявление противоправных материалов и требует применения специализированных инструментов анализа.

В свою очередь, повышаются и требования к системам обнаружения противоправной информации. Подобные программы позволяют осуществлять мониторинг значительных массивов данных в

[1] Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 (с изм. и доп.) «О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено».

автоматизированном режиме. Такие программные решения должны ориентироваться прежде всего на большие объемы информации российского интернет-пространства, которые собираются целевыми «краулерами» и «парсерами» при помощи заранее заданных оператором мониторинга параметров.

К таким параметрам относятся и лексико-семантические словарные конструкции, список которых можно и нужно варьировать и изменять в зависимости от изменений общественно-политической обстановки в конкретном регионе использования системы выявления противоправных публикаций.

Вместе с тем необходимо учитывать и ограничения такого автоматизированного анализа. Машинные методы обработки текста не обладают и не должны обладать полноценной способностью к правовой оценке выявляемых материалов. Возможны как ложные срабатывания, так и пропуск публикаций, содержащих скрытые признаки противоправности.

К системам мониторинга информационного пространства можно отнести используемые Роскомнадзором системы «Чистый интернет», «Окулус», «Вепрь» и другие. Данные системы позволяют оперативно выявлять материалы с признаками нарушения законодательства Российской Федерации с дальнейшим ограничением доступа к ним.

Средства мониторинга используются в разных областях общественной жизни: СММ, связи с общественностью и органами государственной власти — все это имеет уже созданные механизмы для отслеживания трендов сети «Интернет». В числе таких инструментов анализа телеграм-каналов широко используются специализированные сервисы, которые позволяют создавать подборки статистической информации о каналах, динамике публикаций, охвате аудитории и тематике контента, репостов и перепечаток публикаций нескольких телеграм-каналов.

Подобные инструменты позволяют выявлять резкое увеличение публикационной активности по определенной тематике, отслеживать распространение инфоповодов, а также анализировать взаимосвязи между каналами. Это особенно актуально при мониторинге распространения материалов, ранее признанных запрещенными.

Для более широкого анализа информационного поля применяются и иные автоматизированные системы, которые ориентированы на обработку больших массивов текстовой информации из социальных сетей, блогов, форумов и иных открытых источников. С использованием алгоритмов машинного обучения и лингвистического анализа такие системы позволяют формировать тематические выборки и отчеты по ключевым словам.

Наравне с оперативностью выявления публикаций с признаками противоправной информации высокую значимость имеет и качество выявляемых материалов. Под ним можно понимать как полное или частичное соответствие материалов заданной тематике мониторинга, так и корректность выявленных системами мониторинга ссылок (URL). Дополнительную актуальность проблема корректности выявляемых и собираемых URL-адресов приобретает и в связи с появлением все большего количества баз данных, реестров электронных ресурсов.

Особую сложность при этом представляют аудиовизуальные материалы, для анализа которых необходимо сначала вычленить (расшифровать) текстовую составляющую, а затем проанализировать системой мониторинга. К такому контенту можно относить видеозаписи на мобильных платформах, различный игровой контент, распространяемый в лаунчерах игровых платформ.

Конечным этапом любой системы мониторинга должна быть система ручной перепроверки выявленных материалов, их правовой оценки. Подобная квалификация требует глубокой включенности в контекст публикации, уяснения содержания и формы высказывания, а также сопоставления с действующими критериями запрещенной информации, указанными в ведомственных нормативных правовых актах.

В научном дискурсе все чаще поднимается вопрос о соотношении эффективности блокировки и соблюдения принципов законности и справедливости. С одной стороны, государство обязано обеспечивать защиту общества от противоправного воздействия. С другой стороны, любые ограничения доступа к информации должны быть обоснованными и соответствовать установленным процедурам.

Использование систем мониторинга позволяет повысить управляемость информационных процессов. Однако окончательное решение о блокировке должно приниматься с учетом принципа соразмерности и при наличии достаточных правовых оснований. Именно поэтому экспертный анализ остается неотъемлемым элементом механизма противодействия запрещенному контенту.

В то же время автоматизация не может и не должна полностью заменять юридическую квалификацию со стороны правоприменителя. Должна быть обеспечена корректность квалификации и обоснованность решений о применении мер ограничения доступа.

Дальнейшее развитие систем обнаружения и блокировки противоправного контента должно строиться на интеграции технологических решений и повышении квалификации лиц, дающих оценку выявленным материалам. Подобный комплексный подход предопределяет эффективность правоприменения, соблюдения норм действующего законодательства, а также баланса интересов общества и государства.

Государство для людей

ЖИЗНЕННАЯ СИТУАЦИЯ «ЗАЩИТА ОТ МОШЕННИКОВ В СЕТИ»

НА ПОРТАЛЕ ГОСУСЛУГ

Телефонное мошенничество, фишинг, дипфейки — столкнуться с мошенниками сегодня может каждый. С развитием цифровых технологий появляются новые риски и схемы обмана, которые направлены как на молодежь, так и на пожилых людей. Важным аспектом защиты граждан становится просветительская работа. Разобраться в правилах безопасного поведения в сети помогает жизненная ситуация «Защита от мошенников в сети», разработанная в рамках федерального проекта «Государство для людей». На портале госуслуг пользователи могут найти советы по кибербезопасности и сообщить о подозрительном звонке.

СПОКОЙСТВИЕ И УВЕРЕННОСТЬ В ЛЮБОЙ ЖИЗНЕННОЙ СИТУАЦИИ

В 2024 году на российском интернет-портале госуслуг был запущен каталог «жизненных ситуаций», в котором все справочные материалы сгруппированы по тематическим блокам — жизненным ситуациям. Комплексный подход позволяет пользователям найти всю нужную информацию за пару кликов и сэкономить время получения государственных услуг.

Раздел с жизненными ситуациями разработан в рамках федерального проекта «Государство для людей», который направлен на внедрение принципов и стандартов клиентоцентричности. Миссия проекта: обеспечить достойную жизнь людей, а также спокойствие и уверенность в любой жизненной ситуации, помогая каждому человеку решать свои задачи и оказывая незримую поддержку, когда она требуется. Проект помогает модернизировать подходы к предоставлению госуслуг, снизить бюрократические преграды, улучшить качество сервиса, создать механизмы обратной связи и постоянного информирования граждан о процессах и доступных возможностях.

КАК ОБЕЗОПАСИТЬ СЕБЯ И СВОИХ БЛИЗКИХ?

▸ Жизненная ситуация «Защита от мошенников в сети» содержит советы по кибербезопасности и цифровой гигиене. Сервис включает подробные инструкции, которые помогают гражданам найти ответы на наиболее часто встречающиеся вопросы: Что делать, если мошенники получили доступ к аккаунту на Госуслугах? Куда обратиться, если вы или ваши близкие столкнулись с телефонным мошенничеством?

https://www.gosuslugi.ru/scammer_protection

Жизненная ситуация «Защита от мошенников в сети»

Сегодня злоумышленники все чаще используют новые технологии, в том числе искусственный интеллект, для обмана граждан: дипфейки позволяют подделать голос или изображение, что может ввести в заблуждение даже опытного пользователя сети. Столкнуться с преступной схемой и попасть под влияние мошенников может каждый, и важно помнить о простых правилах безопасности, рассказать своим родственникам и друзьям, как вести себя в такой ситуации.

Одним из популярных механизмов защиты становится кодовое слово. Если вам звонят друзья или близкие с неожиданной новостью и просьбой срочно перевести деньги, важно убедиться, что на другом конце трубки действительно ваш знакомый, а не киберпреступник. Выход из ситуации есть: вы можете задать собеседнику личные уточняющие вопросы или заранее придумать кодовое слово, которое он должен будет назвать при разговоре. Если возникают подозрения, главное правило — кладите трубку.

В жизненной ситуации «Защита от мошенников в сети» собраны все доступные на портале госуслуг

инструменты противодействия киберпреступникам. Здесь пользователь может:

- сообщить о подозрительном звонке;
- установить самозапрет на получение кредита;
- проверить кредитную историю;
- посмотреть список оформленных сим-карт;
- подать жалобу о вредоносном ресурсе.

КИБЕРГРАМОТНОСТЬ ДЛЯ ДЕТЕЙ И ПЕНСИОНЕРОВ

Жизненная ситуация «Защита от мошенников в сети» содержит советы по кибербезопасности, ориентированные на разные возрастные группы: от детей до пожилых людей. С развитием новых технологий и широким распространением мобильного интернета активными пользователями мессенджеров становится все большее число представителей старшего поколения. Для данной целевой группы собраны материалы по теме «Как стать киберграмотным в 60 лет», где пользователи могут найти информацию о самых распространенных фразах злоумышленников и уловках телефонных мошенников, рекомендации по цифровой гигиене и инструкцию, как распознать фишинговые письма и вредоносные ссылки.

Отдельное внимание уделяется профилактике вовлечения молодого поколения в противоправную деятельность. Современные дети много времени проводят в интернете, поэтому важно с ранних лет уделять внимание правилам безопасного поведения в цифровом пространстве. Среди угроз, с которыми могут столкнуться дети в сети: взлом учетной записи, сбор личной информации, фишинг, кибербуллинг и многие другие ситуации. Ответственность в вопросах противодействия вовлечению несовершеннолетних в противоправную деятельность в значительной степени ложится на плечи родителей, которые могут своевременно рассказать ребенку о правилах защиты учетных записей, важности настроек приватности и правилах коммуникации в цифровой среде.

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ — ЭТО ПРОСТО

▸ Из раздела «Что рассказать детям о кибербезопасности» (Жизненная ситуация «Защита от мошенников в сети»):

- Использовать надежные пароли
- Подключить подтверждение входа
- Настроить приватность в соцсетях
- Блокировать пользователей, которые пишут негативные комментарии
- Не переходить по ссылкам из подозрительных сообщений
- Не публиковать в соцсетях информацию, которая может быть полезна преступникам
- Не общаться с незнакомыми людьми
- Не пользоваться важными приложениями при подключении к бесплатному вайфаю
- Не провоцировать агрессию и не отвечать на нее

Ранее в Федеральной службе по финансовому мониторингу отметили рост использования в совершении подозрительных операций платежных инструментов несовершеннолетних. Участниками мошеннических схем нередко становятся школьники или студенты, которые в погоне за «легким заработком» вовлекаются в дропперство и предоставляют свои банковские карты или реквизиты третьим лицам. По данным Росфинмониторинга, в 2025 году объем операций физических лиц с признаками дропов увеличился в 1,7 раза по сравнению с 2024 годом и превысил 90 млрд рублей.

Флагманскими проектами в работе по просвещению молодых людей в вопросах противодействия мошенничеству и цифровой грамотности стали Международная олимпиада по финансовой безопасности и Международное движение по финансовой безопасности. В рамках Олимпиады для школьников и студентов из разных регионов России и зарубежных стран проходят тематические уроки по финансовой безопасности. В 2026 году урок посвящен теме противоправного использования ИИ-технологий, в прошлом году уроки на тему «НЕдетские игры: 2.0. Дроп поневоле» прошли для более 3,5 млн школьников и студентов из разных стран. Материалы уроков доступны на платформе «Содружество» и на сайте Олимпиады на русском, английском и других языках.

Ежегодная Олимпиада I уровня проводится с 2021 года при поддержке Президента России и Правительства Российской Федерации. Финал VI Международной олимпиады по финансовой безопасности пройдет с 27 сентября по 2 октября этого года в Красноярске на площадке Сибирского федерального университета (СФУ). В прошлом году финальный этап объединил представителей 40 стран.

Организаторами выступают Росфинмониторинг, Минобрнауки России, Минпросвещения России и образовательные организации, входящие в состав Международного сетевого института в сфере ПОД/ФТ (МСИ). Координатор — Международный учебно-методический центр финансового мониторинга (МУМЦФМ).

Подготовила Кристина Татарникова, главный специалист-эксперт пресс-службы Росфинмониторинга

ИИ КАК ДРАЙВЕР КОМПЛАЕНСА. ЧАСТНЫЙ СЕКТОР В АВАНГАРДЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

43 **ГАЛИНА КУЗНЕЦОВА**
Искусственный интеллект в комплаенсе как инструмент устойчивости антиотмывочной системы

45 **ЭДУАРД ИГНАТЬЕВ**
Искусственный интеллект в комплаенсе Сбербанка: зрелая система выявления и расследования подозрительных операций

48 **ХУРРАМ РИЗОЕВ**
Чат-боты и виртуальные помощники для защиты клиентов от мошенничества: опыт банков и финансовых организаций

50 **ТАТЬЯНА САНЖИЕВА**
«Ответственная игра» и законодательные меры самоограничения: цифровые технологии как инструмент повышения финансовой безопасности в регулируемой индустрии развлечений

53 **АЛЕКСАНДР ГАТИН**
Искусственный интеллект как оружие. Гонка алгоритмов и новая граница финансового суверенитета

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КОМПЛАЕНСЕ КАК ИНСТРУМЕНТ УСТОЙЧИВОСТИ АНТИОТМЫВОЧНОЙ СИСТЕМЫ

Стремительное развитие дистанционных финансовых сервисов и цифровых каналов обслуживания сопровождается усложнением схем незаконных операций и мошенничества. Для участников системы ПОД/ФТ это означает необходимость одновременного решения двух задач: обеспечения доступности финансовых услуг и строгого соблюдения требований Федерального закона № 115-ФЗ.

В этих условиях технологии искусственного интеллекта становятся не элементом технологической модернизации, а прикладным инструментом повышения качества внутреннего контроля. В 2025 году ИИ в комплаенсе — это инструмент поддержки специалиста, который ускоряет анализ, структурирует данные и снижает долю рутинных операций при сохранении ключевой роли профессиональных решений на рынке.

ГАЛИНА КУЗНЕЦОВА
Директор департамента комплаенса Т-Банка

ИНТЕЛЛЕКТУАЛЬНАЯ АГРЕГАЦИЯ ДАННЫХ И АВТОМАТИЗАЦИЯ ПРОЦЕССОВ

Одним из ключевых направлений применения ИИ является интеллектуальная агрегация информации по клиенту. На практике это означает формирование целостного профиля, включающего:

- позитивные факторы (длительная история обслуживания, стабильное финансовое поведение, отсутствие ранее выявленных нарушений);
- негативные сигналы (нетипичные транзакции, отклонения от поведенческого профиля, операции с контрагентами повышенного риска);
- историю предыдущих коммуникаций, направленные запросы и полученные пояснения.

Если ранее сотруднику требовалось обращаться к нескольким внутренним системам и сопоставлять данные вручную, то интеллектуальная обработка позволяет сформировать консолидированную картину в течение нескольких минут. Это напрямую влияет на скорость и обоснованность решений.

Существенный практический эффект связан с автоматизацией рутинных процедур в рамках исполнения требований Закона 115-ФЗ. В частности, алгоритмы используются для:

- формирования и направления типовых запросов клиентам;
- автоматической маршрутизации кейсов внутри подразделений;
- контроля сроков исполнения и статусов рассмотрения;
- подготовки шаблонных уведомлений и пояснений.

Фактически автоматизация охватывает этапы первичной обработки сигнала, подготовки запроса документов и сопровождения кейса

до получения ответа клиента. Это снижает операционную нагрузку и минимизирует вероятность ошибок, связанных с человеческим фактором.

НАВИГАЦИЯ В НОРМАТИВНОЙ СРЕДЕ И ПОДДЕРЖКА ПРОФЕССИОНАЛЬНОГО СУЖДЕНИЯ

Современная регуляторная среда характеризуется высокой динамикой. Изменения подзаконных актов, развитие правоприменительной практики и корректировка внутренних регламентов требуют оперативной адаптации.

ИИ используется как интеллектуальный помощник, обеспечивающий быстрый доступ к релевантным положениям законодательства, внутренним инструкциям и методологическим материалам.

Система также может анализировать изменения в нормативной базе и выявлять, какие положения внутренних регламентов требуют корректировки в связи с новым законодательством. Например, при внесении изменений в налоговый кодекс «помощник» оперативно сопоставляет обновленные требования с действующими внутренними инструкциями, определяет участки, где необходимо внести правки, и формирует перечень предлагаемых изменений. Сотрудник осуществляет проверку предложенных корректировок и принимает решение об их утверждении. При рассмотрении нестандартных кейсов система позволяет соотнести параметры операции с действующими требованиями и сформировать основу для обоснования запроса либо решения.

При этом принципиально важно, что итоговая оценка риска клиента, принятие решений о применении ограничительных мер, интерпретация экономического смысла операций и выстраивание диалога с клиентом остаются в зоне ответственности специалиста. Алгоритм формирует аналитическую основу, но не заменяет профессиональное суждение.

ВЛИЯНИЕ АВТОМАТИЗАЦИИ НА КАЧЕСТВО ВЗАИМОДЕЙСТВИЯ С КЛИЕНТАМИ И УСТОЙЧИВОСТЬ СИСТЕМЫ

Практический эффект автоматизации проявляется не только во внутренних процессах, но и во взаимодействии с клиентами. За счет ускоренной агрегации данных и сокращения внутренних согласований решения принимаются быстрее, а запросы формируются без задержек и содержат структурированный перечень необходимых сведений.

Клиент оперативно понимает, какая информация требуется и в каком объеме, что снижает уровень неопределенности и повышает предсказуемость процедур.

Одновременно повышается точность контроля. Более глубокий анализ транзакционного поведения и отклонений от клиентского профиля позволяют сосредоточить внимание на действительно рисковых операциях, снижая количество избыточных запросов в отношении добросовестных клиентов. Это соответствует принципам риск-ориентированного подхода и способствует более рациональному распределению ресурсов подразделений финансового мониторинга.

В условиях роста дистанционного мошенничества технологии ИИ используются и как дополнительный элемент защиты клиентов — за счет выявления нетипичных сценариев поведения и оперативной передачи информации ответственным подразделениям. Тем самым антиотмывочные механизмы интегрируются с задачами противодействия мошенничеству, формируя единую систему защиты.

Таким образом, применение искусственного интеллекта в комплаенсе целесообразно рассматривать не как локальную технологическую модернизацию, а как элемент системного управления комплаенс-рисками. Интеграция интеллектуальных инструментов в процессы ПОД/ФТ позволяет повысить качество риск-ориентированного анализа, обеспечить единообразие подходов и сократить влияние операционных факторов на принятие решений. В условиях роста объема дистанционных операций, модернизации мошеннических схем и усложнения финансовых потоков именно технологическая поддержка становится необходимым условием сохранения управляемости антиотмывочных процедур.

Сочетание алгоритмической обработки данных и экспертной оценки специалиста формирует зрелую модель ПОД/ФТ, в которой автоматизация усиливает, но не подменяет профессиональную ответственность. Такая модель обеспечивает баланс между защитой финансовой системы, соблюдением прав добросовестных клиентов и требованиями законодательства. В условиях стремительной цифровой трансформации и нарастающих технологических рисков именно синергия технологий и компетенций становится основой устойчивого функционирования финансовой инфраструктуры.

«Интеграция интеллектуальных инструментов в процессы ПОД/ФТ позволяет повысить качество риск-ориентированного анализа, обеспечить единообразие подходов и сократить влияние операционных факторов на принятие решений.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КОМПЛАЕНСЕ СБЕРБАНКА:

зрелая система выявления и расследования подозрительных операций

Финансовая среда сегодня быстро адаптируется к потребностям клиентов, предлагая услуги высокого качества и разнообразные финансовые продукты. Это требует от комплаенса решения нескольких задач одновременно: эффективно управлять рисками отмывания денежных средств, точно выявлять подозрительные операции, минимизируя неудобства клиентам, и рационально распределять ресурсы. Использование технологий искусственного интеллекта (ИИ) позволяет решать такие задачи.

ЭДУАРД ИГНАТЬЕВ
Ведущий исследователь данных
ПАО «Сбербанк»

Рассмотрим два этапа в общей системе ПОД/ФТ. Первый этап — выявление операций, обладающих признаками сомнительных. Здесь система работает как фильтр и механизм приоритизации: из потока операций клиентов отбирается ограниченный набор кейсов, на которые действительно стоит обратить внимание. Второй этап — расследование отобранных кейсов. На этом этапе проводится сбор информации, включая документы и пояснения клиента об экономическом смысле операций, анализ и формирование мотивированного суждения. Таким образом, на первом этапе особенно важны скорость, стабильность сигналов и корректная настройка порогов, в расследовании — полнота контекста, достаточность аргументации вывода и воспроизводимость результата.

На этапе выявления операций надежно работают классические модели машинного обучения — скоринговые модели на табличных признаках, построенных на агрегатах по операциям, а также признаках из профиля клиента и его окружения. Мы разделяем множество моделей на два контура, отличные по бизнес-логике и среде исполнения:

- Онлайн-инструменты оперативного реагирования, где оценивается риск транзакции непосредственно в момент ее проведения;
- Пост-режим глубокого ретроспективного анализа. Здесь модели изучают поведение клиента за более длительный период, выявляя сложные схемы.

Высокая точность контролей обеспечивается не выбором «самого сложного алгоритма», а промышленной инженерией: консистентностью данных, мониторингом деградации, управлением изменениями, а также постоянным сбором обратной связи из расследований, что превращает опыт экспертов в новую обучающую выборку.

Эволюция процедур выявления закономерно ведет к моделям, которые видят структуру поведения, а не только статический «срез» признаков. На практике достаточно сильными алгоритмами оказались нейросети, обрабатывающие мультивариативные последовательности событий: модель учится выделять устойчивые паттерны активности клиента и подсвечивать отклонения, которые выглядят нетипично относительно его собственной истории и относительно сопоставимых групп клиентов. В прикладном смысле это позволяет находить новые области риска и поддерживать непрерывное обновление типологий: то, что раньше могло затеряться в «хвосте» распределения, становится заметным и попадает в фокус эксперта. Важно подчеркнуть — такие методы не от-

«ИИ-агент способен находить релевантные фрагменты в большом пакете документов, выделять ключевые тезисы и факты (суммы, даты, предметы договоров, роли сторон), помогать формулировать проверяемые гипотезы и мотивированные суждения.

меняют обучение на разметке из результатов расследований, а дополняют его, обеспечивая приток свежих примеров и снижая зависимость от запаздывающих знаний.

Еще одно направление — графовые методы, в которых ключевым объектом анализа становится сеть связей и операций между клиентами и контрагентами. Здесь технологический выигрыш появляется только при прагматичной постановке задачи. Недостаточно «построить граф»: необходимо качественно определить, какие связи считать значимыми, как агрегировать взаимодействия, как интерпретировать результат и как встроить его в процесс. Там, где данные о связях достаточны, графовый слой усиливает выявление за счет контекстного взгляда на окружение и устойчивых групповых паттернов. Там, где связи шумные или интерпретация неудобна для эксперта, эффект может оказаться ограниченным даже при математически сложной модели. Поэтому зрелая практика — это не гонка за сложностью, а баланс между качеством данных, объяснимостью и операционной применимостью.

Этап расследования долго оставался главным «узким горлышком» автоматизации. Причина проста — здесь преобладают неструктурированные и неоднородные данные. Эксперт сталкивается с многостраничными пакетами документов: сложной иерархией из вложенных папок и архивов, возможными дублями страниц, сканами и фотографиями разных форматов и качества, рукописными текстами пояснений. Существенная часть времени уходит на подготовку материалов: распаковку, структурирование, сбор документов из отдельных страниц, первичную оценку полноты. Затем следует содержательная работа: верификация, перекрестные проверки, сопоставление документов с выпиской, формирование аргументов. Классические алгоритмы здесь практически бессильны, потому что расследование требует не только «оценить риск», а ответить на вопрос — где в материалах кейса находится подтверждение экономического смысла анализируемых операций.

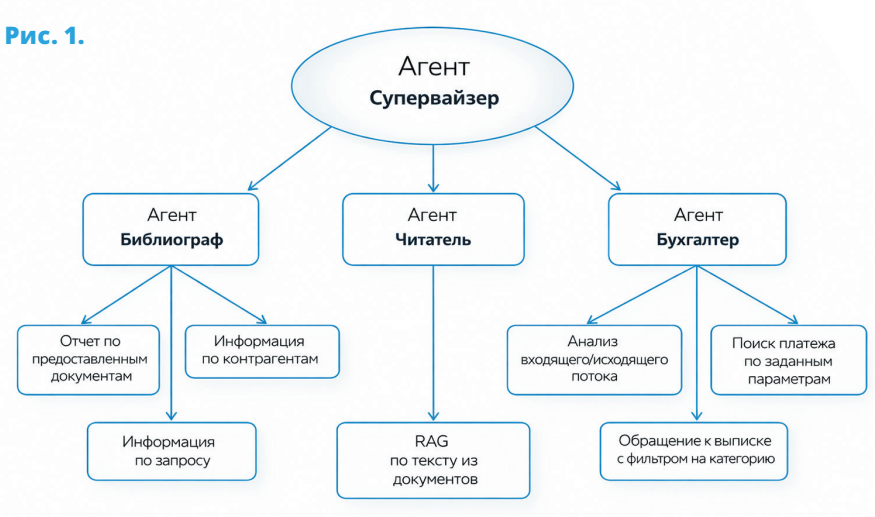
Стремительное развитие генеративного ИИ — больших языковых моделей (LLM) и парадигмы агентов, позволило по-новому организовать работу с такими материалами. Их прикладная польза в расследовании заключается в ускорении навигации, чтения и написания заключений. Например, ИИ-агент способен находить релевантные фрагменты в большом пакете документов, выделять ключевые тезисы и факты (суммы, даты, предметы договоров, роли сторон), помогать формулировать проверяемые гипотезы и мотивированные суждения.

Первым шагом по созданию ИИ-помощника стал запуск конвейера интеллектуальной обработки документов (Intelligent Document Processing, IDP). Данный конвейер превращает разрозненные файлы клиента в пригодный для анализа контент: распаковывает архивы, устраняет дубли, извлекает текст (с применением моделей оптического распознавания), объединяет страницы в единые документы, определяет типы документов, формирует понятные названия и краткие описания, собирает отчет. Результатом становится структурированный пакет документов и база знаний для каждого кейса, готовая к использованию в формате Retrieval Augmented Generation (RAG). Именно данный паттерн позволяет LLM не «галлюцинировать» из своей памяти, а опираться на факты из реальных документов.

Следующим шагом стала разработка мультиагентной системы «Шерлок» на базе нейросети Сбера — GigaChat. Его архитектура спроектирована по принципу распределения задач узкоспециализированным субагентам под управлением «Супервайзера» (рис. 1).

- «Библиограф» отвечает за инвентаризацию пакета докумен-

Рис. 1.



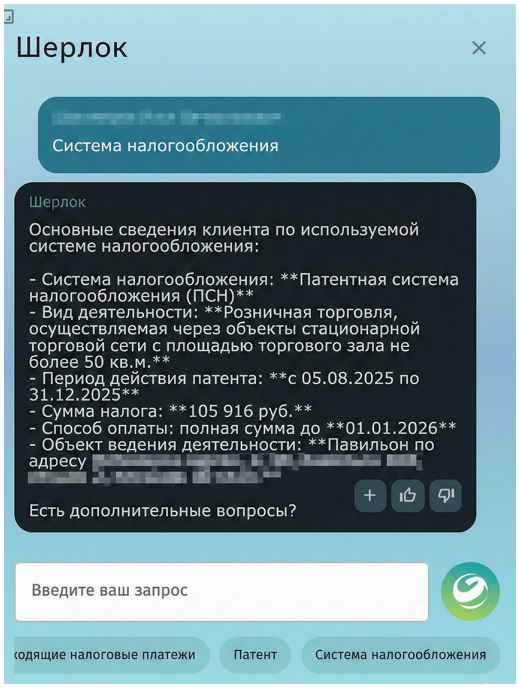
тов: что предоставлено клиентом, чего не хватает, по каким контрагентам есть подтверждения.

- «Читатель» работает с содержанием документов конкретного типа и извлекает нужные факты, опираясь на поисковый индекс документов кейса, который возвращает релевантные фрагменты текста (RAG).
- «Бухгалтер» отвечает за вопросы по выписке, используя специальные инструменты для агрегаций и поиска по потоку банковских операций.

ИИ в ПОД/ФТ превращается из набора разрозненных инструментов в зрелую, контролируемую архитектуру, которая повышает точность выявления, ускоряет расследование и поддерживает воспроизводимое принятие решений.

Важно отметить, что ядром «Шерлока» является не только LLM и логика агентной системы, но и инструменты обращения к данным. Для агентов требуется устойчивый онлайн-доступ к смежным системам, обеспечивающим проведение расследования, в согласованных форматах и с едиными идентификаторами. Каждый логически отделимый блок данных превращается в инструмент агента, который может быть вызван по решению модели для ответа на те или иные вопросы пользователя. Так получается новый специализированный Data API, который должен соответствовать единому стандарту интеграции (Gen AI Ready). Это трудоемкая работа, существенно увеличивающая время и стоимость внедрения.

Рис. 2.



Чтобы снизить порог входа и ускорить работу, наиболее популярные «общие» вопросы дополнительно зашиты в интерфейс в виде готовых подсказок (рис. 2): сотрудник может выбрать их одним кликом или задать свой вопрос в свободной форме. В результате он получает не шаблон с заполненными признаками, а помощника, который соединяет документы, выписку и контекст кейса в единую логику расследования.

Доверие к ИИ в ПОД/ФТ нельзя «задекларировать» — его приходится выстраивать итеративно. На каждом шаге фиксируются критерии качества, разбираются ошибки, уточняются ограничители и процедуры контроля. Такой подход дает практический эффект без потери управляемости: качество решений опирается на технологические механизмы и процесс, а не на «удачные ответы модели».

Финальное решение по операциям остается за человеком. И это не компромисс, а требование к надежности и ответственности. ИИ усиливает эксперта в тех задачах, где теряется время и внимание: поиск, выделение важного, структурирование информации, сопоставление документов с выпиской, формирование гипотез и интерпретация данных. При этом система должна оставаться объяснимой и пригодной для контроля. Выводы привязываются к источникам, действия логируются, а доступ к данным строго регламентируется. Именно так ИИ становится надежным партнером комплаенс-функции — не заменяя профессиональное суждение, а делая процесс его формирования более быстрым и технологически поддержанным.

Дальнейшее развитие мы видим в расширении покрытия данных и в повышении управляемости. С одной стороны, это более полный контекст расследования за счет новых источников, например достоверной информации из интернета. С другой — развитие механизмов оценки уверенности и качества: система должна понимать, когда она может уверенно подсветить факт, а когда обязана явно указать на пробелы в данных. Критично, чтобы технологическое усиление оставалось безопасным и не приводило к раскрытию деталей, которые могли бы облегчить обход процедур ПОД/ФТ.

Таким образом, ИИ в ПОД/ФТ превращается из набора разрозненных инструментов в зрелую, контролируемую архитектуру, которая повышает точность выявления, ускоряет расследование и поддерживает воспроизводимое принятие решений.

ЧАТ-БОТЫ И ВИРТУАЛЬНЫЕ ПОМОЩНИКИ ДЛЯ ЗАЩИТЫ КЛИЕНТОВ ОТ МОШЕННИЧЕСТВА:
опыт банков и финансовых организаций

Рост дистанционных операций усиливает уязвимость клиентов к мошенничеству, основанному на социальной инженерии, когда человек сам инициирует перевод под давлением или в результате обмана. В подобных сценариях классический мониторинг транзакций часто реагирует поздно: риск проявляется не столько в «аномальном» платежном паттерне, сколько в ошибке принятия решения клиентом. В статье, опираясь на зарубежные кейсы и международную нормативную рамку ПОД/ФТ, рассматриваются чат-боты и виртуальные помощники как элемент комплаенс-инфраструктуры. Обосновывается, что их внедрение повышает превентивное информирование клиентов, формирует стандартизированный цифровой канал сообщения о подозрениях и способствует повышению управляемости операционного риска.

По оценке Consumer Financial Protection Bureau, в 2022 году более 98 млн пользователей взаимодействовали с чат-ботом, а прогноз на 2026 год — 110,9 млн пользователей. Таким образом, виртуальные помощники становятся массовым каналом клиентского взаимодействия, где ошибки дизайна, маршрутизации или контроля приобретают характер комплаенс-риска.

ХУРРАМ РИЗОЕВ
Ведущий комплаенс-офицер
ЗАО «Международный банк Таджикистана»

Рекомендация 1 ФАТФ закрепляет фундамент риск-ориентированного подхода, в соответствии с которым государства обязаны идентифицировать, оценивать и понимать риски ПОД/ФТ, а финансовые учреждения — самостоятельно выявлять и оценивать собственные риски и принимать соразмерные меры по их снижению. В этом контексте мошеннические сценарии, при которых клиент действует под влиянием третьих лиц, должны рассматриваться как управляемый риск, требующий формализованного процесса, назначения владельца, установления метрик и применения пропорциональных мер контроля, а не исключительно как последствие понесенных потерь.

В обзоре ФАТФ, посвященном возможностям и вызовам новых технологий в сфере ПОД/ФТ, подчеркивается, что цифровые решения способны усиливать эффективность внедрения стандартов, улучшать понимание рисков, поддерживать надлежащую проверку клиентов и совершенствовать мониторинг операций. В этой логике виртуальный помощник выступает как встроенный комплаенс-канал в клиентском интерфейсе, позволяющий трансформировать регламенты и процедуры в повторяемые процессы предупреждения, фиксации фактов и маршрутизации инцидентов.

Зарубежная практика демонстрирует прикладную ценность подобной архитектуры. В Соединенных Штатах виртуальный ассистент

Erica банка Bank of America предоставляет клиентам инструменты управления картами, включая временную блокировку и замену утерянных карт, а также функции повышения защищенности аккаунта. По данным CFPB, к октябрю 2022 года число пользователей Erica достигло почти 32 млн, а количество взаимодействий превысило один миллиард. В Великобритании банк NatWest развивает цифровой канал репортинга подозрительного мошенничества через виртуального помощника Cora, что позволяет оперативнее защищать счета клиентов и снижать нагрузку на операторов контакт-центра. В Сингапуре DBS Bank использует DBS digibot для приема структурированных сообщений о мошеннических попытках, включая фишинговые атаки, параллельно регулярно обновляя предупреждения о текущих схемах обмана. Ценность данных моделей для комплаенса заключается в стандартизации входящего репортинга, возможности оперативного обновления сценариев предупреждений и формировании проверяемой цифровой следовой базы.

С комплаенс-позиции принципиальное значение имеет не сам факт наличия чат-бота, а доказуемая контрольная среда вокруг него. Персонализированные действия должны сопровождаться надлежащей аутентификацией и соблюдением принципа минимально необходимого доступа. Диалоги подлежат протоколированию и хранению в рамках управляемой политики логирования с обеспечением защиты персональных данных. При признаках спора, жалобы или повышенного риска должна обеспечиваться обязательная эскалация к сотруднику банка. Формализация процесса предполагает закрепление владельца, определение контрольных точек комплаенса и аудита, а также установление требований к качеству ответов и корректности маршрутизации инцидентов.

Дополнительные риски связаны с качеством потребительского сервиса и возможными злоупотреблениями. CFPB отмечает, что жалобы потребителей нередко обусловлены неспособностью чат-ботов корректно распознавать и сопровождать споры, что может повлечь правовые последствия для финансовых организаций. Отдельное внимание должно уделяться риску имитации, когда злоумышленники создают поддельные чат-боты для фишинговых целей, а также вопросам конфиденциальности и защиты журналов чатов, содержащих чувствительные данные.

Актуальность внедрения цифровых превентивных механизмов подтверждается отраслевой статистикой. По информации Reuters со ссылкой на UK Finance, в первом полугодии 2024 года в Великобритании было похищено более 570 млн фунтов стерлингов в рамках платежного мошенничества. Подобные показатели служат аргументом в пользу инвестиций в цифровые инструменты раннего предупреждения и управляемого репортинга.

Для ЗАО «Международный банк Таджикистана» внедрение виртуального помощника в связке с формализованными комплаенс-процессами рассматривается как элемент развития внутренней системы контроля и повышения устойчивости к мошенническим и санкционным рискам. Эффективность данной модели достигается при управлении полным циклом: от проактивного информирования клиента о типовых схемах злоупотреблений и рисков до предоставления ему простого цифрового канала для оперативного сообщения о подозрительных ситуациях; от фиксации минимально достаточного объема данных до их структурирования, автоматизированной маршрутизации, эскалации и аналитической обработки с целью актуализации контрольных сценариев.

В экосистеме банка такие виртуальные решения интегрируются прежде всего с механизмами скрининга, верификации данных и автоматической генерации алертов в службу комплаенса. Взаимодействие бота с внутренними базами позволяет осуществлять первичную проверку клиента и операций по санкционным перечням, внутренним стоп-листам и индикаторам повышенного риска, проводить цифровую верификацию сведений и при выявлении несоответствий формировать структурированный сигнал для дальнейшего анализа специалистами комплаенса.

Таким образом, виртуальный помощник становится частью единой цифровой инфраструктуры контроля, обеспечивая непрерывность процесса «обнаружение — проверка — уведомление — анализ». Это повышает скорость реагирования, снижает вероятность человеческого фактора на первичном этапе и усиливает превентивный характер комплаенс-функции банка в условиях усложняющейся регуляторной среды.

«Виртуальный помощник становится частью единой цифровой инфраструктуры контроля, обеспечивая непрерывность процесса «обнаружение — проверка — уведомление — анализ». Это повышает скорость реагирования, снижает вероятность человеческого фактора на первичном этапе и усиливает превентивный характер комплаенс-функции банка в условиях усложняющейся регуляторной среды.

«ОТВЕТСТВЕННАЯ ИГРА» И ЗАКОНОДАТЕЛЬНЫЕ МЕРЫ САМООГРАНИЧЕНИЯ:

цифровые технологии как инструмент повышения финансовой безопасности в регулируемой индустрии развлечений

Регулируемая индустрия развлечений в Российской Федерации, включающая сегмент онлайн-ставок, активно развивается, в том числе за счет цифровизации и развития мобильных платформ. На фоне этого, предупреждая возможные риски, связанные с вовлечением уязвимых категорий граждан в азартную деятельность, ЕДИНЫЙ ЦУПИС[1] внедрил цифровой сервис «Ответственная игра», а на законодательном уровне приняты меры по самоограничению игроков. Это важный шаг к формированию цифровой культуры финансовой безопасности, снижению социальной напряженности и укреплению устойчивости регулируемой индустрии развлечений.

ТАТЬЯНА САНЖИЕВА
Руководитель Службы финансового мониторинга ЕДИНОГО ЦУПИС, к. э. н.

К числу основных рисков сферы онлайн-ставок относятся формирование игровой зависимости, потеря контроля над личными финансами, рост закредитованности населения, а также вовлечение уязвимых категорий граждан — несовершеннолетних, лиц пожилого возраста и лиц с психическими расстройствами — в неконтролируемую азартную деятельность. Эти процессы приводят не только к личным финансовым потерям, но и увеличивают нагрузку на социальные институты, банковский сектор и систему финансового мониторинга, создавая почву для мошеннических схем, легализации преступных доходов и финансирования противоправной деятельности.

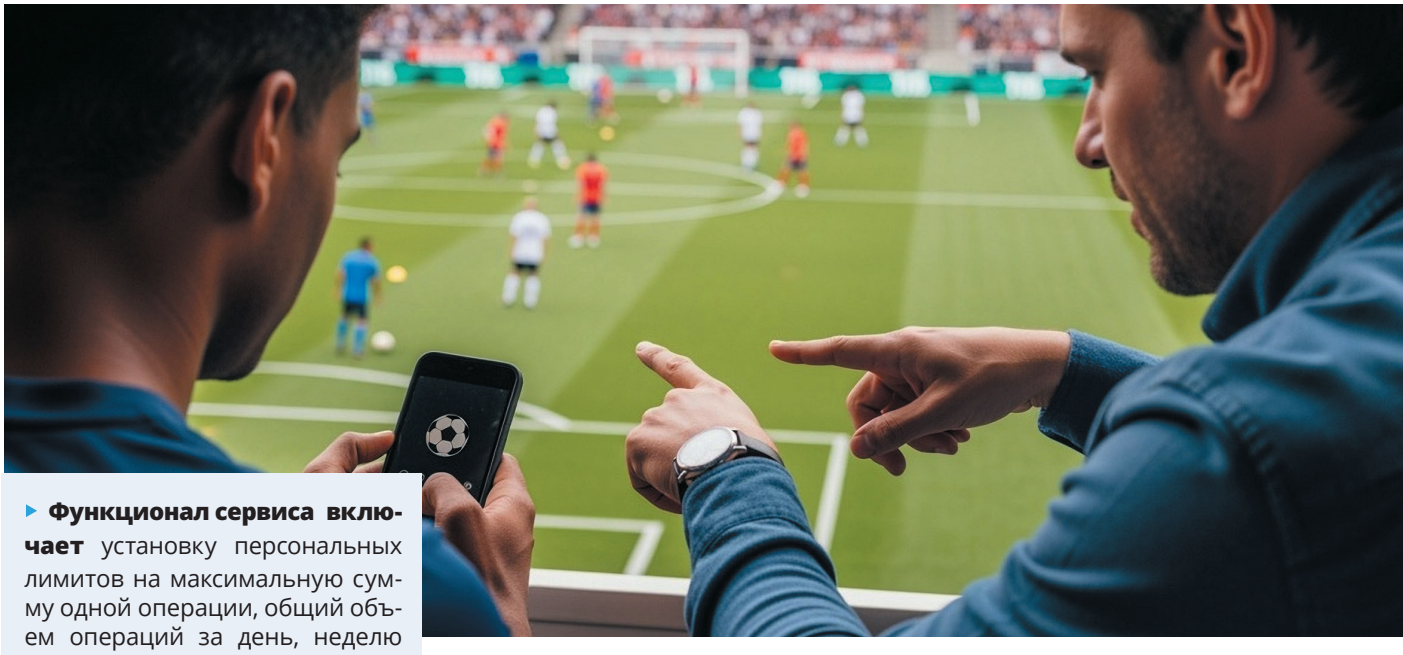
В таких условиях цифровые технологии играют двойную роль: будучи драйвером роста рынка, они одновременно становятся мощным инструментом защиты при условии их целенаправленного и ответственного применения в рамках регуляторных требований.

Именно в контексте этих двух ролей осенью 2023 года ЕДИНЫЙ ЦУПИС запустил сервис, направленный на укрепление политики ответственной игры[2]. Одноименный сервис направлен на формирование культуры самоконтроля у пользователей, предлагая инструменты для ограничения нежелательного или неконтролируемого поведения. Сервис доступен всем пользователям компании в Кошельке ЦУПИС[3] в мобильном приложении или на сайте в личном кабинете.

[1] ЕДИНЫЙ ЦУПИС — общество с ограниченной ответственностью небанковская кредитная организация «Мобильная карта», лицензия Банка России № 3522-К, выполняющая функции единого центра учета переводов ставок букмекерских контор и тотализаторов в соответствии с распоряжением Президента Российской Федерации от 25.08.2021 № 236-П.

[2] Ответственная игра (или Responsible Gambling) — это комплекс принципов в игровой индустрии, которых придерживаются все ее участники. Суть ответственной игры заключается в том, чтобы игроки воспринимали беттинг в первую очередь как один из видов развлечений, а не способ получить дополнительный доход.

[3] Кошелек ЦУПИС — это Личный кабинет и мобильное приложение с балансом и привязанными букмекерами.



Функционал сервиса включает установку персональных лимитов на максимальную сумму одной операции, общий объем операций за день, неделю или месяц. Лимиты определяются самостоятельно: например, не более 3 тысяч рублей на операцию, без необходимости дублировать настройки у конкретного букмекера. Кроме этого, пользователи могут активировать самоисключение — временный или постоянный запрет на переводы средств букмекерам, что полностью блокирует пополнение балансовых счетов у букмекерских контор и возможность делать интерактивные ставки.

Снятие ограничений возможно через Службу поддержки ЕДИНОГО ЦУПИС, что исключает импульсивные решения и усиливает защитный эффект. С момента запуска сервиса зарегистрировано порядка 165 тысяч обращений по самоограничениям с устойчивым ростом числа полного самоисключения. Эти меры не затрагивают имеющиеся средства на балансе Кошелька ЦУПИС, но эффективно снижают риски финансовых потерь и вовлечения в сомнительные схемы. За все вышеперечисленные удобства и возможности «Ответственная игра» официально признана социально значимым сервисом национальной премией инноваций и достижений в финансовой отрасли FINAWARD[4].

Эффективность подобных инициатив, таких как сервис «Ответственная игра», напрямую зависит от возможностей современных информационно-коммуникационных технологий (далее — ИКТ). Именно ИКТ выступают ключевым инструментом реализации принципов самоограничения в регулируемой индустрии развлечений, обеспечивая не только высокую доступность сервисов, но и их практическую действенность в условиях интенсивного пользовательского трафика.

Цифровые платформы автоматизируют контроль на всех этапах взаимодействия: от оперативной идентификации клиента до точной настройки индивидуальных лимитов и их строгого соблюдения посредством API-интеграций с организаторами азартных игр. При превышении установленных параметров система мгновенно приостанавливает операции, информируя пользователя через мобильное приложение, смс- или push-уведомления, что гарантирует превентивный эффект даже в пиковые периоды активности.

> **При превышении установленных параметров система мгновенно приостанавливает операции, информируя пользователя через мобильное приложение, смс- или push-уведомления, что гарантирует превентивный эффект даже в пиковые периоды активности.**

Такие решения минимизируют влияние человеческого фактора, исключают субъективные ошибки и обеспечивают бесперебойное функционирование правил

[4] https://www.mcplat.ru/news/otvetstvennaya-igra-edinogo-tsupis-priznana-finaward-sotsialno-znachimym-servisom/.

даже под высокой нагрузкой. Естественным и логичным дополнением к технологическим инновациям становится совершенствование нормативно-правовой базы, переводящее меры самоконтроля из добровольной практики в механизм государственной защиты.

В 2024–2025 годах были доработаны законодательные инициативы по созданию перечня физических лиц, отказавшихся от участия в азартных играх (далее — Перечень). Теперь, согласно Федеральному закону № 575-ФЗ[5], вступающему в силу 1 сентября 2026 года, гражданин вправе подать заявление в ЕРАИ[6] через портал Госуслуг или многофункциональный центр (МФЦ), определив срок самоограничения не менее 12 месяцев без досрочного отзыва (с возможностью продления). Информация будет передана в ЕДИНЫЙ ЦУПИС и организаторам азартных игр (далее — ОАИ), которые будут обязаны заблокировать доступ к ставкам, игорным заведениям, личным кабинетам на сайтах ОАИ, используемым для принятия интерактивных ставок, а также в пятидневный срок отменить все незавершенные пари с полным возвратом средств физическому лицу на указанный в заявлении банковский счет.

Указанные механизмы цифрового самоконтроля и законодательные меры самоограничения оказывают системное и прямое воздействие на укрепление финансовой безопасности граждан, финансовой системы и государства в целом.

Цифровой сервис ЕДИНОГО ЦУПИС «Ответственная игра» и положения Федерального закона № 575-ФЗ существенно снижают риски закредитованности населения, предотвращая неконтролируемые траты и накопление долговой нагрузки на домохозяйства. Они эффективно блокируют вовлечение граждан в финансовые махинации, нелегальные схемы по обналичиванию денежных средств или легализации преступных доходов через операции с ОАИ. Стратегическое значение эти меры приобретают в контексте защиты наиболее уязвимых категорий — несовершеннолетних, лиц пожилого возраста, индивидов с психическими расстройствами и граждан с диагностированной игровой зависимостью, минимизируя социальные и экономические последствия их участия в индустрии.

> **«Механизм самоограничения не только минимизирует риски вовлечения добросовестных граждан в мошеннические схемы, но и кардинально повышает общий уровень цифровой и финансовой безопасности, усиливая защиту финансовой системы от вторичных угроз.**

Включение физических лиц в Перечень трансформирует меру индивидуальной самозащиты в системный превентивный инструмент противодействия мошенничеству с персональными данными. В условиях экспоненциального роста киберпреступлений — от кражи учетных данных до несанкционированной регистрации электронных кошельков, игровых аккаунтов и дропперских схем — статусная запись в Перечне создает непреодолимый барьер для проведения операций через ЕДИНЫЙ ЦУПИС. Злоумышленники лишаются возможности использовать похищенные чужие персональные данные для нелегальных транзакций, включая интерактивные ставки.

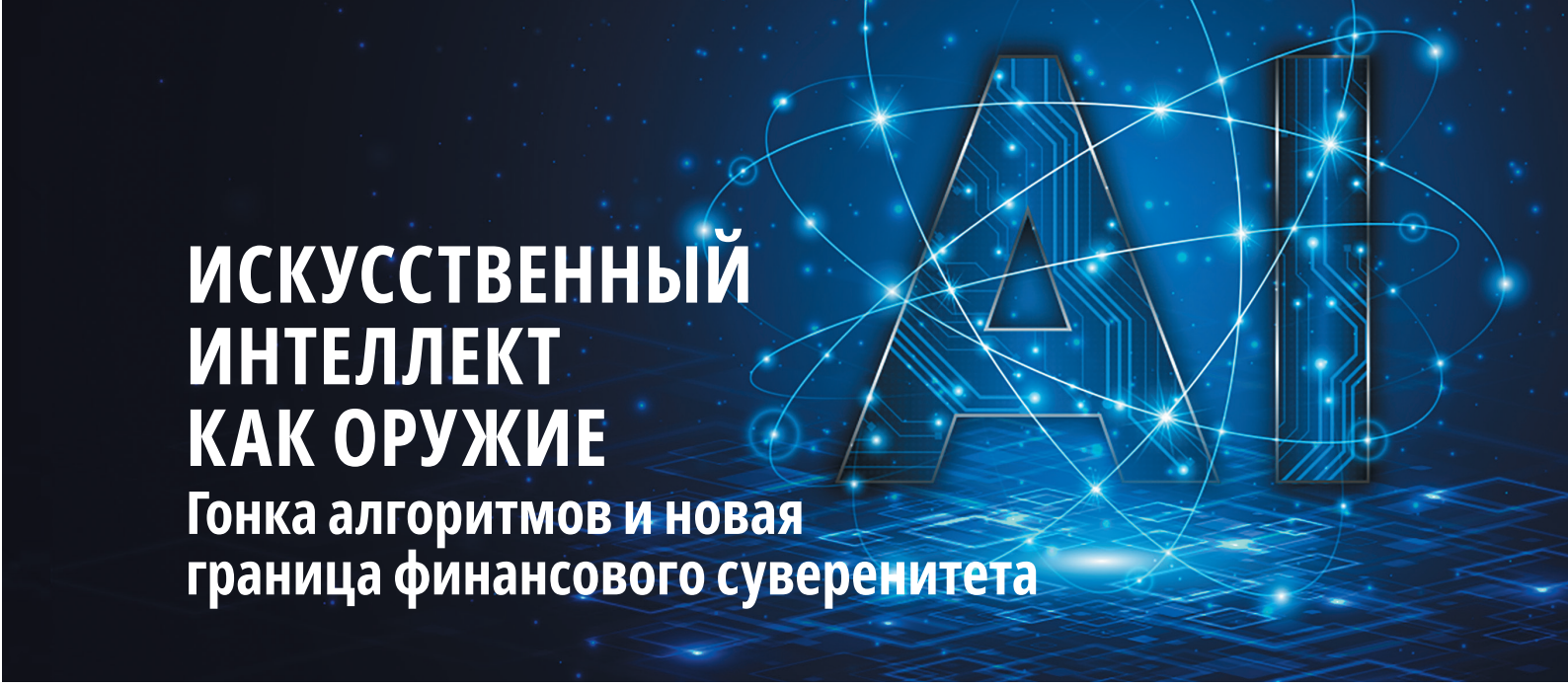
Таким образом, механизм самоограничения не только минимизирует риски вовлечения добросовестных граждан в мошеннические схемы, но и кардинально повышает общий уровень цифровой и финансовой безопасности, усиливая защиту финансовой системы от вторичных угроз.

Цифровая политика ответственной игры дополнительно повышает доверие к легальным организаторам азартных игр и государственным регуляторам, формирует культуру осознанного финансового поведения в цифровой среде и существенно снижает социальную напряженность, связанную с азартными играми.

Развитие сервиса «Ответственная игра» ЕДИНОГО ЦУПИС и принятие Федерального закона № 575-ФЗ знаменует переход регулируемой индустрии развлечений к модели цифровой зрелости, где технологии и право совместно обеспечивают защиту граждан, устойчивость финансовой системы и национальную финансовую безопасность.

[5] Федеральный закон от 29.12.2025 № 575-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

[6] ЕРАИ — публично-правовая компания «Единый регулятор азартных игр», созданная Российской Федерацией в соответствии с Федеральным законом от 30.12.2020 № 493-ФЗ «О публично-правовой компании “Единый регулятор азартных игр” и о внесении изменений в отдельные законодательные акты Российской Федерации» в целях повышения эффективности контроля (надзора) за организацией и проведением азартных игр и обеспечения внебюджетного финансирования спорта в Российской Федерации.



ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ОРУЖИЕ

Гонка алгоритмов и новая граница финансового суверенитета

Современные мошеннические схемы больше не строятся на случайности. Они опираются на обработку массивов данных, в том числе утекших, сопоставление цифровых событий, прогнозирование поведенческих паттернов и выбор оптимального момента контакта.

АЛЕКСАНДР ГАТИН
Исполнительный директор по исследованию данных ПАО «Сбербанк», консультант по искусственному интеллекту

КОГДА ТЕХНОЛОГИЯ ПЕРЕСТАЕТ БЫТЬ НЕЙТРАЛЬНОЙ

История показывает, что любая технология, способная изменить баланс сил, со временем перестает быть нейтральной. Порох изменил архитектуру войны. Интернет радикально перестроил экономику и коммуникации. Искусственный интеллект меняет более фундаментальную конструкцию — природу доверия, которая является базовым элементом финансовой системы.

Сегодня в публичной повестке ИИ чаще обсуждается как инструмент эффективности, который позволяет автоматизировать процессы, оптимизировать затраты, повысить точность решений. Однако в финансовой сфере он все отчетливее проявляется как инструмент асимметричного давления.

Речь идет не о гипотетическом будущем, а о текущей реальности. Современные мошеннические схемы больше не строятся на случайности. Они опираются на обработку массивов данных, в том числе утекших, сопоставление цифровых событий, прогнозирование поведенческих паттернов и выбор оптимального момента контакта. Это уже не хаотичный спам, а управляемая вероятностная система.

ОТ МАССОВОСТИ К АДАПТИВНОСТИ

Архитектура атаки изменилась принципиально. Ранее работала логика, в которой упор делался на объем: массовая рассылка, низкая персонализация, ставка на вероятность случайного отклика.

> **Искусственный интеллект в финансовой сфере все отчетливее проявляется как инструмент асимметричного давления.**

Сегодня модель выглядит иначе. Аудитория все лучше сегментируется на основе данных и цифровых следов пользователей. В пределе

сегментирование дойдет до каждого человека. Сценарии становятся персональными, на них тестируются реакции людей. Дальше вносятся корректировки, в том числе автоматически, а самые успешные сценарии масштабируются.

Фактически это переход от линейной схемы к адаптивной системе с обратной связью. Алгоритм учится быстрее, чем обновляется регламент.

ПЕРСОНАЛЬНЫЙ КЕЙС КАК СИМПТОМ СИСТЕМЫ

Недавно мошенники дважды пытались атаковать мою семью. Оба эпизода произошли с пугающей точностью по времени. В первом случае после подачи заявления в поликлинике утром поступил звонок с просьбой «подтвердить прикрепление кодом из СМС». Контекст совпадал полностью. Во втором случае «курьер» позвонил сыну сразу после экзамена с просьбой назвать код для получения доставки. Сценарий был правдоподобен, момент выбран точно, детали звучали естественно. Ни медицинские учреждения, ни крупные ритейлеры не запрашивают коды подтверждения заранее. Но в обоих случаях атака была встроена в реальные жизненные ситуации.

Подобная точность невозможна без анализа цифровых следов, сопоставления событий и выбора оптимального времени для атаки. Это уже не социальная инженерия в ее классическом понимании. Это алгоритмически усиленная модель воздействия.

АЛГОРИТМИЧЕСКАЯ ГОНКА

Мы живем в условиях тотальной цифровизации. Платежи, государственные сервисы, логистика, коммуникации и хранение документов — все интегрировано в мобильные и облачные контуры. Производственные процессы предприятий соединены с цифровыми системами управления. Каждый новый сервис повышает удобство, но одновременно расширяет поверхность атаки.

По данным регуляторов, за 2025 год число преступлений в сфере дистанционного финансового мошенничества продолжило рост, а ущерб измеряется уже сотнями миллиардов рублей. Однако ключевой показатель — это не абсолютный объем, а ускорение динамики.

Преступные команды работают вне регуляторных циклов. Они не ограничены процедурами согласования, бюджетными периодами или квартальными планами. Их главное преимущество — скорость, с которой они проводят свои «эксперименты».

Мы вступили в фазу алгоритмической гонки. С одной стороны — модели мошенников, обновляющиеся ежедневно. С другой — институциональные механизмы защиты, обновляющиеся значительно реже.

Если защита работает по старому регламенту, а атака — с помощью постоянно обновляемых моделей машинного обучения, возникает конфликт скоростей. И в этой конфигурации скорость становится определяющим фактором.

ЦИФРОВАЯ САМОУВЕРЕННОСТЬ КАК НОВАЯ УЯЗВИМОСТЬ

Отдельного внимания заслуживает изменение целевой аудитории. Если ранее акцент мошенников делался преимущественно на пожилых гражданах, то сегодня все чаще объектом атак становится молодое поколение, т. е. студенты и только что начавшие трудовую деятельность молодые специалисты.

Эти люди выросли в цифровой среде. Телефон для них — это кошелек, пропуск, средство обучения, коммуникации и работы. Реакция на уведомление мгновенная. Сообщение в мессенджерах воспринимается как прямой разговор.

«Мы живем в условиях тотальной цифровизации. Платежи, государственные сервисы, логистика, коммуникации и хранение документов — все интегрировано в мобильные и облачные контуры. Производственные процессы предприятий соединены с цифровыми системами управления. Каждый новый сервис повышает удобство, но одновременно расширяет поверхность атаки.

Парадокс в том, что высокая технологическая вовлеченность формирует ощущение компетентности. Такие люди искренне уверены, что во всем разбираются. Они быстро принимают решения, редко проверяют источники информации, привыкли к постоянному онлайн-контакту с другими людьми, с большинством из которых вживую никогда не виделись.

Проблема на самом деле серьезная и состоит в дефиците понимания процедурных границ. В одном из опросов среди студентов технического вуза значительная доля респондентов считала допустимым так называемый видеообыск через камеру телефона по требованию «представителя органов». Незнание процессуальных рамок и полномочий государственных органов становится точкой входа

для социальной инженерии. Искусственный интеллект усиливает не давление, а правдоподобие. А правдоподобие снижает внутренний барьер критического восприятия. Люди не ожидают подвоха, поскольку схемы встроены в реальные жизненные ситуации.

РЕГЛАМЕНТ ПРОТИВ АДАПТАЦИИ

Финансовая система традиционно защищается регламентом: лимиты операций, периоды охлаждения, типологии подозрительных транзакций, формальные критерии риска. Эта модель была эффективна в среде, где процессы меняются медленно.

Но ИИ способен анализировать сами правила. Он тестирует систему малыми операциями, выявляет чувствительные параметры и перестраивает поведение, оставаясь в пределах формального соответствия и старых регламентов. Защита обновляется по планам, которые пишутся на год вперед. Атака обновляется по результатам эксперимента. Возникает институциональный разрыв.

Обмен информацией между банками, профильными ведомствами и регуляторами остается фрагментированным. Каждая организация строит собственную архитектуру данных. Юридические и процедурные фильтры замедляют обмен информацией.

Если схема перестраивается за часы, а сигнал распространяется днями, система проигрывает не из-за недостатка интеллекта, а из-за недостатка скорости. В условиях алгоритмической гонки данные становятся стратегическим ресурсом. Кто быстрее агрегирует, очищает и анализирует информацию, тот получает преимущество.

СИСТЕМНЫЙ РИСК: ПОДРЫВ ДОВЕРИЯ

Финансовая безопасность — это не только борьба с отдельными инцидентами. Это поддержание доверия к системе. Массовая автоматизация мошеннических схем способна запускать синхронные волны давления. Рост числа инцидентов снижает доверие клиентов, усиливает осторожность в цифровых каналах, увеличивает долю ложных срабатываний. Система начинает защищаться настолько активно, что становится неудобной. Кризис доверия — это уже не частная проблема, а системный риск.

«Незнание процессуальных рамок и полномочий государственных органов становится точкой входа для социальной инженерии. Искусственный интеллект усиливает не давление, а правдоподобие. А правдоподобие снижает внутренний барьер критического восприятия. Люди не ожидают подвоха, поскольку схемы правдоподобно встроены в реальные жизненные ситуации.

АЛГОРИТМИЧЕСКИЙ СУВЕРЕНИТЕТ

Зачастую финансовые преступления трансграничные. Инфраструктура атак распределена по разным юрисдикциям. ИИ ускоряет адаптацию и усложняет атрибуцию. Национальная защита без международной координации неизбежно ограничена. Но простого взаимодействия с другими странами недостаточно. Необходима собственная технологическая платформа как элемент суверенитета в области финансовой безопасности.

Перспективной представляется модель обмена сигналами риска, когда данные остаются внутри национальных контуров, но аналитические индикаторы и сигналы циркулируют через защищенный протокол. И Россия способна создать такую международную платформу.

Такой подход снижает угрозу утраты суверенитета данных и одновременно формирует коллективный контур раннего предупреждения. Тот, кто задает стандарты и методики обмена, фактически формирует правила игры.

КОНТРОЛИРУЕМЫЙ ВЗЛОМ КАК НОРМА

Если ИИ используется как инструмент атаки, защита должна учиться быстрее. Это требует постоянных лабораторных экспериментов наступательного анализа, моделирующих поведение злоумышленников.

Контролируемый взлом должен стать частью культуры финансовой безопасности. Обнаружение уязвимостей необходимо поощрять. Белый взлом должен быть выгоднее черного, а белые хакеры должны становиться героями. Регулярные хакатоны по тестированию финансовых систем могут стать механизмом выявления уязвимостей и одновременно инструментом повышения грамотности среди молодого поколения.

При этом усиление роли ИИ в защите порождает новые вопросы: прозрачность алгоритмов, ответственность за ошибки модели, баланс между безопасностью и правами клиента. Решение этих задач требует новой компетентности экспертов по безопасности, а именно сочетания технологической глубины и понимания правовой рамки.

СКОРОСТЬ КАК НОВАЯ КАТЕГОРИЯ БЕЗОПАСНОСТИ

Искусственный интеллект сам по себе нейтрален. Но в условиях конфликта интересов он становится инструментом усиления и атаки, и защиты. Алгоритмическая гонка уже началась. Финансовый суверенитет сегодня определяется не количеством нормативных актов и не числом отчетов. Он определяется скоростью обработки данных, скоростью обучения моделей и скоростью институциональной реакции.

Если защита обновляется раз в квартал, а атаки — ежедневно, выигрывает не тот, кто сильнее, а тот, кто быстрее. Скорость становится базовым элементом безопасности. И именно в этом измерении сегодня проходит новая граница финансового суверенитета. Давайте разгоняться, пока еще есть время!

ЛАБОРАТОРИЯ БЕЗОПАСНОСТИ. НАУЧНЫЙ ОТВЕТ НА НОВЫЕ РИСКИ

58 **СЕРГЕЙ ЛУЦЕНКО**
Информационная безопасность в банковском секторе

62 **ОЛЕГ ИВАНОВ, АНДРЕЙ ЛЕОНИДОВ**
Методы искусственного интеллекта в контексте задач в сфере ПОД/ФТ

66 **ВЛАДИСЛАВ ГЕНЕРАЛОВ, ЛЮДМИЛА МАКАРОВА**
Фактчекинг в сфере финансовой безопасности: научно-образовательные траектории противодействия недостоверной информации

71 **МАРИНА ШЕМЯКИНА**
Урок по финансовой безопасности: от внеурочной инициативы к международному образовательному проекту

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКОВСКОМ СЕКТОРЕ

Утечка информации является одной из актуальных угроз нарушения информационной безопасности в банковском секторе, которую могут реализовать возможные внутренние нарушители самой информационной безопасности.

СЕРГЕЙ ЛУЦЕНКО
Директор Центра экономического анализа права и проблем правоприменения Института экономических стратегий РАН, член Экспертного совета Комитета Государственной Думы Федерального Собрания РФ по обороне

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646 и представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере, устанавливает, что информационной безопасностью Российской Федерации является состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. В свою очередь, угрозой информационной безопасности Российской Федерации является совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

В Доктрине определены национальные интересы в информационной сфере, к числу которых в том числе отнесены обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий.

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации (пункт 9 Доктрины).

Таким образом, информационная безопасность Российской Федерации является частью системы национальной безопасности государства.

Защита персональных данных субъектов персональных данных от неправомерного их использования обеспечивается в установленном действующим законодательством Российской Федерации в сфере персональных данных (в частности, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных») порядке путем выполнения комплекса организационных и технических мер, обеспечивающих их безопасность и определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Необеспечение принятия своевременных и достаточных мер для целей защиты персональных данных физических лиц от неправомерного доступа к ним, что повлекло за собой распространение персональных данных граждан неограниченному кругу лиц посредством размещения данных в сети «Интернет», не позволяет исключить как создание угрозы безопасности физических лиц ввиду размещения их персональных данных в открытом доступе (к тому же в данном случае был допущен факт несанкционированного доступа в личные кабинеты физических лиц с распространением паролей, при этом личные кабинеты содержат в том числе сведения об адресе электронной почты, номере телефона, адресе проживания лица и иных данных о гражданах, а также платежную информацию), равно как и создает угрозу причинения ущерба информационной безопасности государства, поскольку в таком случае не обеспечивается состояние защищенности личности от

информационных угроз и неприкосновенность частной жизни при использовании информационных технологий, что является национальным интересом государства в информационной сфере.

Кибербезопасность — сфера деятельности, занимающаяся защитой компьютерных систем, сетей, программ и данных от киберугроз, включая хакерские атаки, вирусы, вредоносное программное обеспечение и другие цифровые угрозы.

Необходимо отметить, что на национальном уровне к числу нормативных актов, связанных со сферой кибербезопасности, необходимо отнести, в частности, Федеральные законы от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Указы Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», распоряжение Правительства РФ от 30.12.2024 № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий».

Отдельно хотелось бы обратить внимание на банковский сектор в информационном пространстве, который представляет уязвимость для киберугроз.

Банк России планирует участвовать в разработке федеральными органами исполнительной власти требований информационной безопасности, предъявляемых к субъектам критической информационной инфраструктуры, которые являются организациями кредитно-финансовой сферы («Основные направления развития финансовых технологий на период 2025–2027 годов» (одобрены Советом директоров Банка России)).

При осуществлении дистанционного банковского обслуживания должны применяться защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы. Все попытки таких подмен должны регистрироваться регламентированным образом.

Обязанность идентификации клиентов при открытии и ведении банковских счетов возложена на банк, сотрудник которого при открытии расчетного счета юридическому лицу осуществляет прием документов, необходимых для открытия счета соответствующего вида, проверку надлежащего оформления документов, полноты представленных сведений и их достоверности.

«При осуществлении дистанционного банковского обслуживания должны применяться защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы.

На основании полученных документов проверяют у клиента правоспособности (дееспособности), а также выполняют другие функции, предусмотренные нормами закона, банковскими правилами и должностной инструкцией. В указанных целях должностные лица кредитного учреждения взаимодействуют с клиентами и их представителями, запрашивают и получают необходимую информацию.

Противоправное поведение банка, выразившееся в непринятии банком достаточных мер для проверки информации и надлежащей идентификации клиента, на которую в соответствии с законом распространяется соответствующий режим охраны, привело к нарушению прав клиента и возникновению у него убытков[1].

Комплекс мер по обеспечению информационной безопасности от киберугроз банковского платежного технологического процесса должен предусматривать в том числе защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений; доступ работника организации банковской системы РФ (далее — БС РФ) только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации; контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации; аутентификацию входящих электронных платежных сообщений; двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями; возможность ввода платежной информации в АБС (автоматизированная банковская система) только для авторизованных пользователей; контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т. д.); восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или

[1] Постановление Девятого арбитражного апелляционного суда от 02.07.2024 по делу № А40-16376/2024.

выхода из строя средств вычислительной техники; сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов; доставку электронных платежных сообщений участникам обмена.

В соответствии с приказом Банка России от 11.04.2016 № ОД-1205 приняты и введены рекомендации в области стандартизации Банка России (РСБР ИББС-2.9-2016) «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации», установлено, что наибольшими возможностями для нанесения ущерба, в том числе неумышленного, организации БС РФ и (или) ее клиентам в части возможного нарушения конфиденциальности обрабатываемой информации обладают работники организации БС РФ и (или) иные лица, обладающие легальным доступом к информации, — возможные внутренние нарушители информационной безопасности. При этом одной из актуальных таких угроз является утечка информации.

Кредитное учреждение в своей деятельности должно руководствоваться Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и Правилами внутреннего контроля по проверке спорной платежной операции с учетом критериев операций, подлежащих обязательному контролю, и подозрительных операций. Необходимо принимать разумные меры к соответствующей проверке при приостановке операции по перечислению денежных средств с выяснением ее законности и реальности выполнения клиентом.

Обращаем внимание, что, поскольку работники банка являются непосредственными лицами, имеющими доступ к сведениям, составляющим банковскую тайну, банк как профессиональный участник рынка банковских услуг с учетом указанных рекомендаций ЦБ РФ обязан с должной осмотрительностью относиться к выбору сотрудников, а также обеспечивать такой режим работы со сведениями, составляющими банковскую тайну, который предполагает минимизацию рисков распространения таких сведений его сотрудниками.

Банк как профессиональный участник рыночных отношений должен определить достаточность надежности работы при приеме, передаче, обработке и хранении информации, а также защите информации, обеспечивающей разграничение доступа, шифрование, контроль целостности и других параметров.

Именно кредитное учреждение как субъект профессиональной предпринимательской деятельности в области проведения операций по счетам клиентов и осуществляющий их с определенной степенью риска должен нести ответственность в виде возмещения убытков, причиненных неправомерным списанием принадлежащих его клиенту денежных средств[2].

В Определении Конституционного Суда Российской Федерации от 13.10.2022 № 2669-О указано, что в большинстве случаев мошенничества сделки оспариваются как совершенные под влиянием обмана потерпевшего третьим лицом. При рассмотрении подобных споров необходимо учитывать особенности добросовестности и осмотрительности банков. В частности, к числу обстоятельств, при которых кредитной организации в случае дистанционного оформления кредитного договора надлежит принимать повышенные меры предосторожности, следует отнести факт подачи заявки на получение клиентом кредита и незамедлительной выдачи банку распоряжения о перечислении кредитных денежных средств в пользу третьего лица (лиц).

В соответствии с пунктом 3 Признаков осуществления перевода денежных средств без добровольного согласия клиента, утвержденных приказом Банка России от 27.06.2024 № ОД-1027, к таким признакам относится несоответствие характера, и (или) параметров, и (или) объема проводимой операции (время (дни) осуществления операции, место осуществления операции, устройство, с использованием которого осуществляется операция, и параметры его использования, сумма осуществления операции, периодичность (частота) осуществления операций, получатель средств по операциям, обычно совершаемым клиентом оператора по переводу денежных средств (осуществляемой клиентом деятельности).

[2] Постановление Девятого арбитражного апелляционного суда от 21.03.2024 по делу № А40-237179/2023.

Иногда работники кредитного учреждения могут быть участниками преступления, связанного с хищением денежных средств через преступную группу, связанную с обналичиванием денежных средств и финансовым мошенничеством, нарушая при этом правила внутреннего контроля проверки финансовой операции, которая может подпадать под критерии, подлежащие обязательному контролю. Кроме того, в данной ситуации сотрудники банка нарушают рекомендации в области стандартизации Банка России (РС БР ИББС-2.9-2016) «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации». А именно речь идет о разглашении сведений о клиенте третьим лицам и непринятие банком достаточных мер для защиты информации, на которую в соответствии с законом распространяется соответствующий режим охраны[3].

В заключение хотелось бы обратить внимание на следующее обстоятельство.

Банком России выявлено использование кредиторами практик заключения кредитных договоров, при которых согласие заемщика выражается посредством совершения действий, свидетельствующих о его согласии с предлагаемыми кредитором индивидуальными условиями (конклюдентные действия), либо телефонного звонка в адрес кредитора с информированием последнего о согласии на получение потребительского кредита (займа) на предложенных индивидуальных условиях. По мнению Банка России, устанавливающего правила проведения банковских операций, заемщиком индивидуальные условия договора потребительского кредита (займа) не подписываются ни собственноручной подписью, ни ее аналогом.

«Иногда работники кредитного учреждения могут быть участниками преступления, связанного с хищением денежных средств через преступную группу, связанную с обналичиванием денежных средств и финансовым мошенничеством, нарушая при этом правила внутреннего контроля проверки финансовой операции, которая может подпадать под критерии, подлежащие обязательному контролю.

Составление договора в письменной форме с приведением индивидуальных условий в виде таблицы по установленной Банком России форме, с указанием полной стоимости кредита, с напечатанными отметками (V) напротив строк об ознакомлении и согласии с различными условиями договора и т. п. лишено всякого смысла, если фактически все действия по предоставлению кредита сводятся к направлению банком потенциальному заемщику смс-сообщения для однократного введения цифрового смс-кода[4].

В случае совершения лицом сделки с помощью электронных либо иных технических средств его письменная форма считается соблюденной, если эти средства позволяют воспроизвести на материальном носителе содержание договора в неизменном виде (в частности, при распечатывании).

Информация в электронной форме, подписанная простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами или соглашением между участниками электронного взаимодействия, которые должны предусматривать в том числе правила определения лица, подписывающего электронный документ, по его простой электронной подписи.

Соответственно, для обеспечения документа, подписанного простой электронной подписью, юридической силой необходимо идентифицировать лицо, которое использует простую электронную подпись, понятие которой в законе определено не только через наличие присущих ей технических признаков — использование кодов, паролей или иных средств, но и через ее функциональные характеристики — необходимость подтверждения факта формирования электронной подписи определенным лицом.

Учитывая изложенное, легитимность электронного документа с простой электронной подписью, содержащего условия, которые названы в законе или иных правовых актах как существенные или необходимые для договоров данного вида, а также все те условия, относительно которых по заявлению одной из сторон должно быть достигнуто соглашение, подтверждается наличием указания в нем лица, от имени которого составлен и отправлен электронный документ.

Таким образом, по мнению Банка России, подобные практики не могут быть признаны надлежащими и соответствующими требованиям действующего законодательства о потребительском кредите[5].

[3] Постановление Арбитражного суда Московского округа от 27.06.2022 по делу № А40-92593/2021.

[4] Определение Первого кассационного суда общей юрисдикции от 10.07.2025 № 88-18497/2025.

[5] Определение Третьего кассационного суда общей юрисдикции от 27.10.2025 № 88-17204/2025.

МЕТОДЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ ЗАДАЧ В СФЕРЕ ПОД/ФТ

Проблема отмывания денег и финансирования терроризма является одной из наиболее важных в современном обществе. Ее масштаб (оценка ФАТФ) — от 2 до 5 процентов мирового ВВП, т. е. триллионы долларов. В этих условиях развитие эффективных методов противодействия таким преступным схемам является приоритетной задачей. По мнению экспертов, огромную перспективу имеет здесь применение современных алгоритмов искусственного интеллекта.

ОЛЕГ ИВАНОВ
Заместитель директора по развитию Физического института им. П.Н. Лебедева РАН, к. ф.-м. н.

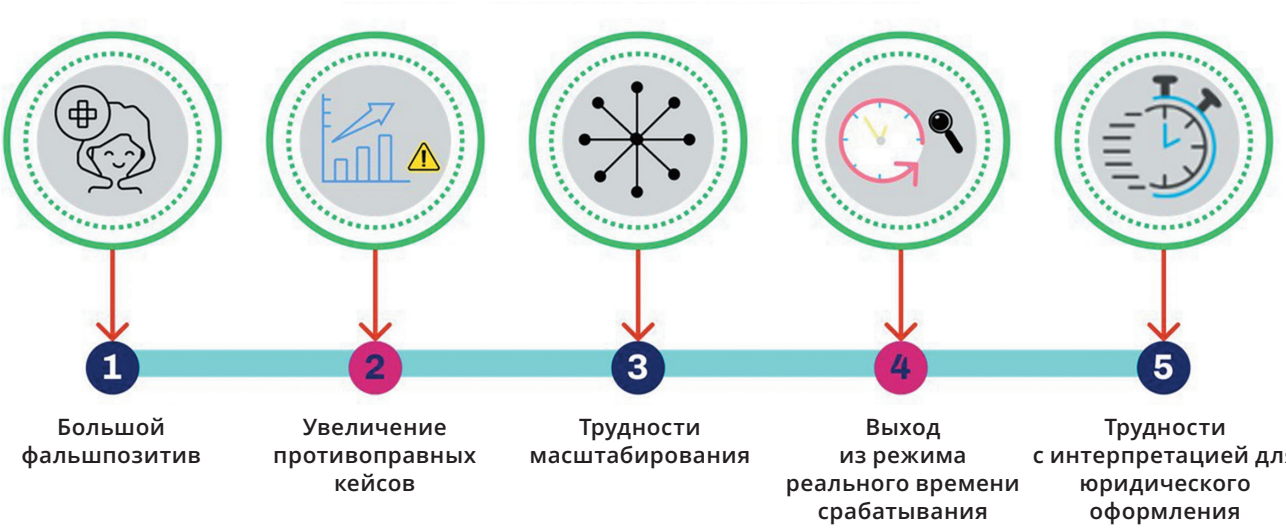
АНДРЕЙ ЛЕОНИДОВ
Руководитель Лаборатории математического моделирования сложных систем Отделения теоретической физики им. И.Е. Тамма Физического института им П.Н. Лебедева РАН, д. ф.-м. н.

Финансовые организации реализуют антиотмывочные меры по двум главным направлениям. Во-первых, это создание и адаптивная поддержка баз данных по клиентам, включающих верифицированную персональную информацию, сведения об их источниках финансирования, характере финансовых операций (в особенности трансграничных) с ранжированием по специфическим рискам в сфере ПОД/ФТ. Во-вторых, это генерация отчетов о подозрительных операциях, являющихся основанием для проведения расследований и принятия соответствующих мер. Для реализации этого функционала требуется обеспечить систематический адаптивный анализ огромного объема разнородной сложно структурированной информации. Качественный анализ такой информации без привлечения современных методов искусственного интеллекта (ИИ) кажется невозможным, что и объясняет значительные человеческие и финансовые ресурсы, направляемые на совершенствование алгоритмов ИИ, используемых для решения задач в сфере ПОД/ФТ.

Первоначально в сфере ПОД/ФТ использовались простейшие конструкции распознавания подозрительных паттернов в данных, основанных на наборе заранее сформулированных признаков/правил. Применение подобных алгоритмов приводит, однако, к огромному проценту ложных срабатываний — по имеющимся оценкам до 90%, что влечет за собой большие временные и финансовые затраты на «ручную» очистку полученного сигнала. Кроме того, возникают новые типы рисков, таких как использование криптовалют, для которых формулировка фиксированного набора правил, определяющих сигнал, весьма затруднительна. При огромном объеме анализируемых данных эти факты представляют собой трудноразрешимую проблему и служат доминирующим мотивом для разработки и внедрения более совершенных алгоритмов. Существующие вызовы в связи с использованием традиционных алгоритмов рас-

Рис. 1.

ВЫЗОВЫ К ТРАДИЦИОННЫМ AML ТЕХНОЛОГИЯМ



познавания подозрительных схем в сфере ПОД/ФТ проиллюстрированы на рис. 1.

Возможность существенного продвижения в разработке таких алгоритмов связана прежде всего с использованием современных методов искусственного интеллекта, в частности машинного, в том числе глубокого обучения, использования больших языковых моделей и графовой аналитики.

Главное достоинство методов машинного обучения — их способность выявлять в интенсивном потоке данных необычные паттерны, в том числе сложно структурированные и выраженно динамические. Что касается методов глубокого обучения, то они могут быть особенно полезны при выявлении в реальном времени паттернов, характеризующихся аномальными свойствами.

Традиционные алгоритмы в сфере ПОД/ФТ были основаны на использовании структурированных данных. Применение алгоритмов, связанных с большими языковыми моделями, позволяет включить в информационную орбиту поиска неструктурированные тексты — отчеты, публикации и т. д., в которых можно выделить описание явлений, релевантных для сферы ПОД/ФТ.

Особое значение имеет применение для решения задач в сфере ПОД/ФТ графовых алгоритмов ИИ. По существу, речь идет о создании, поддержании и развитии машиночитаемой онтологии для схем отмывания денег и финансирования терроризма, которая используется для их выявления в потоке данных. Использование таких шаблонов позволяет выявлять преступные сообщества и роли их участников. Особенно важно, что графовые алгоритмы обеспечивают полную интерпретируемость полученных результатов.

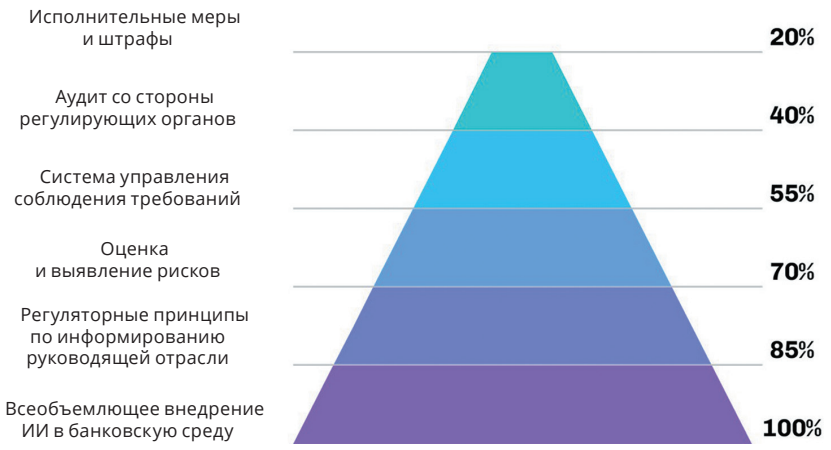
По оценке специалистов, основанные на использовании современных методов ИИ, алгоритмы поиска подозрительных схем в сфере ПОД/ФТ позволяют существенно увеличить эффективность антиотмывочной деятельности. Так, использование наиболее современных алгоритмов позволяет уменьшить число ложных срабатываний в три раза — примерно до 30%, что несомненно свидетельствует об их большом потенциале.

Использование и совершенствование алгоритмов искусственного интеллекта для решения задач в сфере ПОД/ФТ сопряжено с рядом трудностей как юридического, так и технического характера.

> **«Использование наиболее современных алгоритмов позволяет уменьшить число ложных срабатываний в три раза — примерно до 30%, что несомненно свидетельствует об их большом потенциале.**

С точки зрения законодательства наибольшие трудности возникают в связи с необходимостью соблюдения законов о персональных данных, в особенности при анализе информации об иностранных участниках предполагаемых схем. Важным аспектом применения законодательства о персональных данных является также необходимость их анонимизации, которая резко снижает эффективность алгоритмов машинного обучения. Нормативные аспекты при-

Рис. 2.



менения ИИ в банковской среде проиллюстрированы на рис. 2.

С технической точки зрения ключевой особенностью используемых для обучения первичных данных является их выраженный дисбаланс с абсолютным преобладанием законных операций. Кроме того, необходимый для реализации алгоритмов обучения с учителем набор размеченных данных имеет, как правило, крайне ограниченный объем. Важной проблемой, требующей, как правило, весьма дорогостоящих решений, является также необходимость бесшовной интеграции новых алгоритмов с уже существующими системами — как с точки зрения гармонизации баз данных, так и с точки зрения гармонизации алгоритмического функционала.

Отдельного упоминания заслуживают риски, связанные с появлением новых технологий, таких как криптовалюты. Быстрое развитие такого рода инструментов и существенно более высокий уровень защищенности информации о сделках по сравнению с традиционными рынками представляет фундаментальный вызов для деятельности в сфере ПОД/ФТ, справиться с которым без привлечения самых современных алгоритмов ИИ не представляется возможным.

Фундаментальной проблемой при использовании методов ИИ является также необходимость обеспечения приемлемого уровня интерпретируемости при принятии окончательного решения о характере изучаемой финансовой операции/схемы. Это особенно важно при валидации модели и проверке соответствия результатов работы алгоритма с точки зрения соответствия требованиям регулятора.

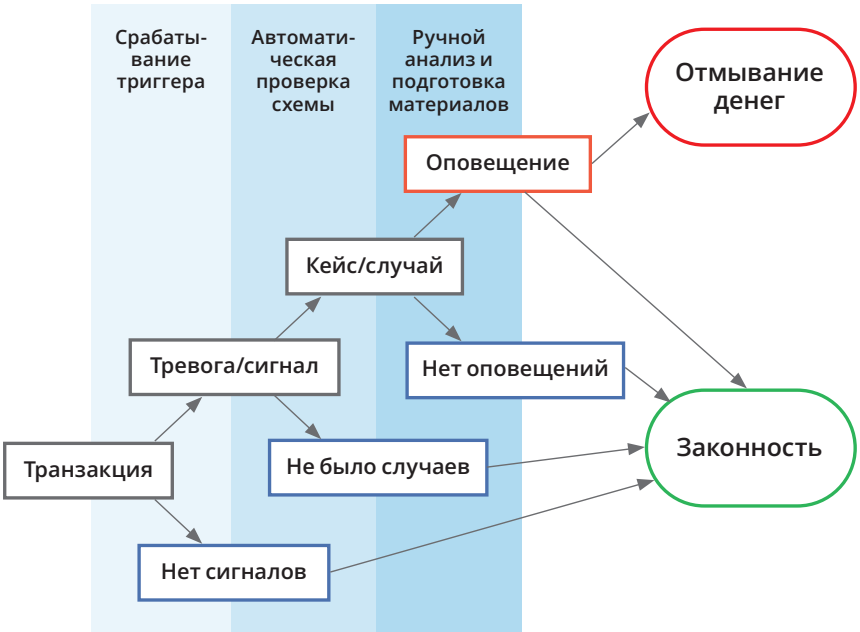
Общая функциональная схема использования алгоритмов ИИ в сфере ПОД/ФТ проиллюстрирована на рис. 3.

В настоящее время алгоритмы ИИ для решения задач в сфере ПОД/ФТ широко используются как крупными финансовыми учреждениями, так и правительственными агентствами. В банке HSBC реализованы использующие методы машинного обучения алгоритмы мониторинга транзакций и риск-скоринга в реальном времени. В банке JPMorgan Chase также реализованы алгоритмы мониторинга, работающие в реальном времени и использующие поведенческий анализ, большие языковые модели и методы глубокого обучения. Отметим также, что в США поддерживается сотрудничество регулятора FinCEN и финансовых фирм в рамках т. н. инновационной инициативы.

Перечислим некоторые платформенные решения, использующие технологии искусственного

Рис. 3.

ОБЩАЯ СХЕМА ПРИМЕНЕНИЯ АЛГОРИТМОВ ИИ В СФЕРЕ ПОД/ФТ



интеллекта, в том числе алгоритмы машинного обучения, для выявления схем, относящихся к сфере ПОД/ФТ.

Наиболее эффективной является, по-видимому, платформа Palantir Gotham компании Palantir technologies, в которой обеспечивается анализ огромного объема информации о финансовых транзакциях, включая межстрановые, и выявление подозрительных паттернов.

Платформа Института SAS, являющегося одним из глобальных лидеров в анализе больших данных, при выявлении схем, подозрительных в контексте ПОД/ФТ, существенно использует современные методы машинного обучения, что позволяет, в частности, обеспечить адаптивность работы системы в реальном времени. Кроме того, система обеспечивает автоматическую генерацию отчетов, в которых полученная в результате работы системы информация помещается в контекст релевантного антиотмывочного/антитеррористического законодательства.

Платформа IBM Watson Financial Services также предлагает основанные на использовании методов ИИ решения, позволяющие идентифицировать подозрительные в контексте ПОД/ФТ паттерны. В свою очередь, платформа IBM Financial Services обеспечивает детальный менеджмент рисков, в том числе в привязке к релевантному антиотмывочному/антитеррористическому законодательству.

При анализе перспективы использования методов ИИ для решения задач в сфере ПОД/ФТ отметим следующие пункты:

- ключевым перспективным направлением является расширение спектра использования больших языковых моделей, в особенности применительно к дальнейшей автоматизации подготовки отчетов о подозрительных явлениях и расширению спектра понятий, используемых при анализе рисков в сфере ПОД/ФТ;
- перспективным направлением является также дальнейшее развитие методов федеративного обучения, основанных на одновременном использовании в процессе машинного обучения баз данных, контролируемых различными ведомствами и (или) юридическими лицами, в том числе и для трансграничных юрисдикций с обеспечением гарантий нераспространения чувствительных данных.

В целом можно отметить, что использование методов ИИ для решения задач в сфере ПОД/ФТ имеет значительную перспективу, в частности, с точки зрения возможности детектировать релевантные явления в реальном времени, реализации масштабируемых решений и улучшения качества работы поисковых алгоритмов. Такие перспективы сопровождаются вместе с тем существенным усложнением профиля ошибочных решений, требующего развития эффективных алгоритмов для постоянного контроля работы алгоритмов ИИ человеком.

ЛИТЕРАТУРА

1. K. Cyrkin et al. Using artificial intelligence to counter money laundering and terrorist financing ASEJ 28, № 1 (2024), 101–106.
2. G. Pavlidis. Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. Journal of Money Laundering Control 26, № 7 (2023), 155–166.
3. S. Aidoo et al. Developing AI-Powered AML Compliance Systems: Challenges and opportunities (2025).
4. A. Ghimire. AI-Powered Anomaly Detection for AML compliance in US Banking: Enhancing Accuracy and Reducing False Positives. Global Trends in Science and Technology 1, № 1, (2025), 95–120.
5. V. Boateng et al. Harnessing Artificial Intelligence for combatting money laundering and fraud in the U.S. financial industry: A comprehensive analysis. Finance and Accounting Research Journal 7 (1) (2025), 37–49.
6. E. K. Amoako et al. Exploring the role of Machine Learning and Deep Learning in Anti-Money Laundering (AML) strategies within U.S. Financial Industry: A systematic review of implementation, effectiveness and challenges. Finance and Accounting Research Journal 7 (1) (2025), 22–36.
7. J. Han et al. Artificial intelligence for anti-money laundering: a review and extention. Digital Finance (2019).
8. J. A. Tsapa. Artificial Intelligence Use Cases for Banking Anti-Money Laundering. Journal of Artificial Intelligence, Machine Learning and Data Science (2019), 1–6.

«Ключевым перспективным направлением является расширение спектра использования больших языковых моделей, в особенности применительно к дальнейшей автоматизации подготовки отчетов о подозрительных явлениях и расширению спектра понятий, используемых при анализе рисков в сфере ПОД/ФТ.

ФАКТЧЕКИНГ В СФЕРЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ:

научно-образовательные траектории противодействия недостоверной информации

ВЛАДИСЛАВ ГЕНЕРАЛОВ
Руководитель Научно-образовательного центра финансового мониторинга Нижегородского государственного университета им. Н.И. Лобачевского, заместитель начальника отдела Межрегионального управления Росфинмониторинга по Приволжскому федеральному округу

ЛЮДМИЛА МАКАРОВА
Руководитель Научно-образовательного центра применения искусственного интеллекта в журналистике и массовой коммуникации Нижегородского государственного университета им. Н.И. Лобачевского

Проблема циркуляции недостоверной (фейковой) информации, в том числе в сфере финансовой безопасности, сегодня приобретает критическое значение. Развитие и доступность технологий имеет и негативные последствия, включая возможность использования искусственного интеллекта для создания фейкового контента, дезинформации и манипулирования общественным мнением. Это формулирует запрос на создание гибридных технологий верификации информации, которые позволили бы соединить традиционные методики проверки информации и возможности прикладного искусственного интеллекта. Решение данной проблемы необходимо прежде всего в контексте защиты от фальсифицированной и недостоверной информации, формирования медиаграмотности аудитории, предотвращения информационных угроз, в том числе в области финансовой безопасности. Ответом на этот вызов становится проект AUTOFACTCHECK — не просто инструмент автоматической проверки фактов, а полноценный технологический фреймворк, разрабатываемый в ННГУ им. Н. И. Лобачевского.

Нижегородский государственный университет им. Н. И. Лобачевского (ННГУ) как активный участник Международного сетевого института в сфере противодействия отмыванию доходов и финансированию терроризма (далее — МСИ в сфере ПОД/ФТ) реализует различные цифровые проекты с применением искусственного интеллекта, особое внимание уделяя финансовой безопасности.

В 2025 году на базе ННГУ им. Н. И. Лобачевского в рамках международного круглого стола «Актуальные практики и проблемы научно-образовательного развития финансовой безопасности» с участием 15 государств были

поддержаны предложения Университета Лобачевского в реализации проекта «цифрового хаба» научных и образовательных проектов по финансовой безопасности. Мероприятие закончилось торжественным открытием лаборатории «ФинБез Lab» с демонстрацией собственных цифровых наработок, в том числе интерактивной игры по проведению финансовых расследований. В тестировании виар-комплекса приняли участие эксперты и студенты, в том числе совместного бакалавриата ННГУ и Ташкентского государственного юридического университета (вуз — участник МСИ в сфере ПОД/ФТ). Открытие лаборатории дает возможность развивать собственные проектные траектории по финансовой безопасности, а также партнерскую площадку научно-образовательной среды с IT-компаниями и банковским сектором.

Команда Научно-образовательного центра применения ИИ в журналистике и массовой комуникации Университета Лобачевского. 2025 год, Общественная палата Нижегородской области

#СТУДФАКТЧЕК КАК БАЗОВАЯ МОДЕЛЬ ФАКТЧЕКИНГА

В настоящее время одним из совместных проектов Университета Лобачевского является мониторинг и тестирование искусственного интеллекта на достоверность выдаваемой информации, который вызывает особый интерес у специалистов в сфере финансовой безопасности.

Основой такой работы станет фактчекинг — проверка сообщений в открытых источниках информации с использованием технологий, при помощи которых выявляются несоответствия между публикуемыми фактами и теми, что существуют в реальности, в том числе в рамках цифровой финансовой среды.

С 2020 года по настоящее время в Университете Лобачевского реализуется сетевой образовательный студенческий проект по верификации информации СМИ и социальных медиа #СТУДФАКТЧЕК. В рамках деятельности Научно-образовательного центра применения искусственного интеллекта в журналистике и массовой коммуникации студенты проводят исследования в соответствии с оригинальной методикой, связанные с проверкой достоверности представленной информации, выявляют фейковые сообщения и размещают свои работы на сайте проекта. Особое внимание в рамках проекта уделяется проблеме обеспечения информационной безопасности и противодействия информационным угрозам, необходимости использования технологий фактчекинга в процессе анализа публикаций СМИ и социальных медиа.

Именно технология проверки информации СМИ и социальных медиа проекта #СТУДФАКТЧЕК может быть описана как базовая модель фактчекинга и использоваться для создания прототипа информационной системы, позволяющей в автоматическом режиме находить и атрибутировать фейковую информацию.

На первом этапе высказывание, представленное в материале СМИ или социальных медиа, анализируется участниками исследования с точки зрения понимания содержания: является ли оно «фактом», «мнением», «предсказанием/предположением». «Мнение» и «предсказание» сразу отсекаются: они относятся к категории «непроверяемое», следовательно, не могут быть «истинными» или «ложными» с точки зрения процедуры фактчекинга. Если высказывание в рамках сюжета определяется в качестве «факта» (для этого он должен прежде всего быть привязан к таким параметрам, как дата, событие, конкретный человек, место, количественные данные), то начинается непосредственный процесс проверки. Главной задачей данного этапа является выделение предмета высказывания и его четкая атрибуция с точки зрения смысла: верификация проводится только в системе того, что можно обозначить как «количественно/качественно атрибутируемое», то есть то, что можно объективно проверить при помощи статистики, географических данных, фото- и видеофиксации, данных геолокации, квалифицированного экспертного комментария. Если сделать этого нельзя, то проверка завершается, высказы-

вание определяется как «непроверяемое».

После подтверждения возможности объективной проверки высказывания наступает этап, связанный с анализом источника и его авторства. Самое важное здесь — определить первичный источник, пройти по всей цепочке ссылок, чтобы убедиться в «существовании» автора и в том, что его информация может быть подтверждена при помощи объективных доказательств (факты, свидетели, обстоятельства, даты, упоминаемые географические локации, социальные сети).

На третьем этапе анализируется именно первичный источник, который и подвергается процедуре фактчекинга. В рамках данного этапа студенты пытаются связаться с автором первоначального высказывания для того, чтобы получить комментарий или задать уточняющие вопросы, получить дополнительную информацию. Для этого используются возможности социальных сетей, личные контакты, материалы СМИ.

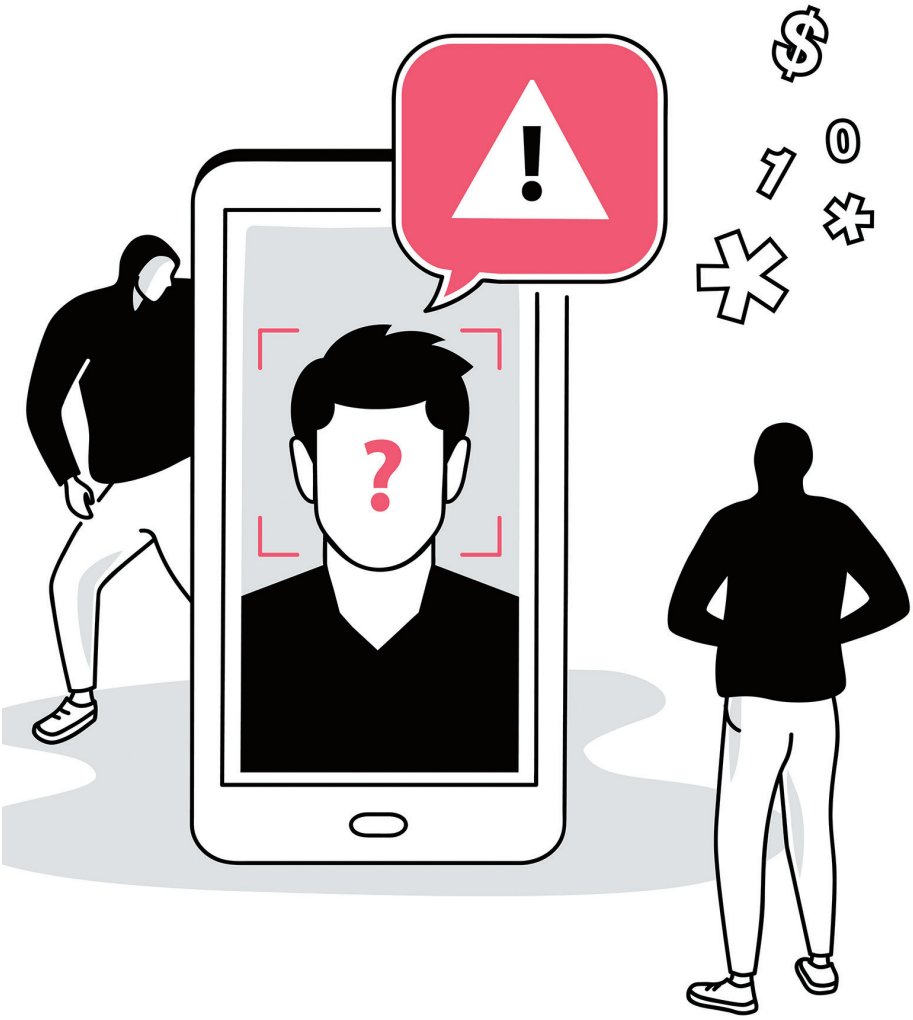
Одновременно с этим начинается активная работа по поиску экспертов, готовых дать комментарий и оценить правдивость/ложность высказывания. Иногда их мнения могут не совпадать: в отдельных случаях это дает возможность использовать материалы интервью в жанре «блогпост», позволяющем расширить контекст сюжета, высказать мнения и оценки, имеющие отношение к фактчеку, но выходящие за его непосредственные рамки. Любое свидетельство в рамках системы доказательства «истинности» или «ложности» высказывания обязательно подкрепляется ссылкой на источник информации. В конце третьего этапа проставляется рейтинг высказывания: подтвержденный «клейм» определяется как «правда»/«в большей степени правда», высказывание, не имеющие объективного подтверждения, — как «ложь»/«в большей степени ложь».

НЕЙРОННАЯ СЕТЬ AUTOFACTCHECK

Современное информационное пространство переживает беспрецедентную трансформацию под влиянием технологий генеративного искусственного интеллекта. Объемы цифрового контента растут экспоненциально, а вместе с ними — распространение дезинформации, синтезированной с высокой степенью правдоподобия. В таких условиях верификация утверждений становится не просто вспомогательной функцией журналистики, а стратегической задачей обеспечения информационной устойчивости общества.

Традиционные методы фактчекинга, основанные на ручной экспертизе, не справляются с масштабом вызова: качественная проверка одного утверждения может занимать от нескольких недель до месяцев. Эта задержка делает подобные методы неэффективными в условиях скорости распространения фейков в социальных сетях и мессенджерах.

С 2025 года командой Центра применения искусственного интеллекта в журналистике и массовой коммуникации разрабатывается и тестируется гибридная



платформа проверки информации на основе собственной нейронной сети AUTOFACTCHECK. Именно проект #СТУДФАКТЧЕК стал методологической основой для разработки автоматизированного конвейера проверки достоверности утверждений. Цель работы — создание гибридного фреймворка, сочетающего образовательные практики ручного фактчекинга с возможностями современных больших языковых моделей (LLM) и принципами доверенного искусственного интеллекта.

На текущем этапе команда проекта завершает формирование ядра фреймворка — масштабируемой архитектуры, способной интегрироваться в различные цифровые среды. В 2025 году была создана архитектура конвейера проверки достоверности утверждения на базе технологии генеративного ИИ. Она построена модульно и включает следующие этапы: извлечение утверждения из текста или пользовательского ввода; сбор контекстуальных данных (дата, источник, тематика); агрегация релевантных источников с использованием технологии Retrieval-Augmented Generation (RAG); анализ достоверности с помощью LLM; генерация структурированного вердикта в формате JSON с аргументацией и ссылками; фильтрация контента на предмет потенциально опасной риторики. Подобная структура обеспечивает не только высокую точность, но и полную объяснимость решения — ключевое требование для использования в образовательной и регуляторной среде. В качестве эталона для оценки эффективности использовался открытый датасет от Facticity.AI, на котором были протестированы как коммерческие, так и локально разворачиваемые модели. Результаты показали, что модель SaigaGemma2:9b, обученная на русскоязычных данных и донастроенная под задачи фактчекинга, достигает точности 87% — показатель, сопоставимый с ведущими зарубежными решениями на тех же данных. Конвейер ориентирован на общую задачу проверки утверждений в открытом информационном пространстве, где контекст и источник критически важны. Все модули взаимодействуют через стандартизированные API, что позволяет легко адаптировать систему под разные сценарии использования — от встраивания в редакционные CMS до создания ботов в мессенджерах или расширений для браузеров.

«На текущем этапе команда проекта завершает формирование ядра фреймворка — масштабируемой архитектуры, способной интегрироваться в различные цифровые среды.

Действующий прототип AUTOFACTCHECK 28 мая 2025 года прошел публичную валидацию в Общественной палате Нижегородской области и получил самые высокие оценки от представителей СМИ, общественности и органов государственного и муниципального управления.

Одним из ключевых направлений развития проекта является запуск специализированного портала для фактчекеров, который станет центральным элементом научно-практической экосистемы.

Проект по созданию гибридной платформы AUTOFACTCHECK включен в Программу стратегического академического лидерства «Приоритет 2030», в которой участвует ННГУ им. Н. И. Лобачевского (трек «Программное обеспечение для критической инфраструктуры»), что подтверждает его научную и социально-практическую значимость. В ближайших планах — разработка полноценной платформы с веб-интерфейсом, API для интеграции в СМИ, образовательные и государственные системы, а также механизмами SLA-гарантий для институциональных пользователей. Особое внимание уделяется аудиту моделей на предмет предвзятости и соответствия требованиям российского законодательства в сфере ИИ.

На данный момент Центр применения искусственного интеллекта в журналистике и массовой коммуникации получил два свидетельства о государственной регистрации результатов интеллектуальной деятельности (РИД) — программ для ЭВМ (правообладателем выступает ННГУ им. Н. И. Лобачевского). Разработки направлены на автоматизацию анализа новостного контента и проверку достоверности информации с использованием технологий искусственного интеллекта.

Первое свидетельство зарегистрировано на программу «Система поиска и извлечения контекста из найденных новостных ресурсов» — парсер, позволяющий автоматически собирать и обрабатывать данные из медиасреды и формировать контекст по заданным темам. Второе свидетельство получено на программу «Конвейер проверки достоверности утверждений на базе технологии генеративного искусственного интеллекта». Речь идет о нейросети, которая сопоставляет утверждения с проверенными источниками и помогает выявлять недостоверные сообщения.

ПРОТИВОДЕЙСТВИЕ ДИПФЕЙКАМ, ПОИСК ИНФОРМАЦИИ И НЕ ТОЛЬКО

AUTOFACTCHECK будет служить не только интерфейсом для проверки утверждений, но и платформой для совместной работы: профессиональные верификаторы, журналисты, исследователи и студенты смогут вносить экспертные оценки, дополнять контекст, предлагать источники и участвовать в кураторстве данных. Это позволит формировать уникальный датасет проверенной информации, структурированный по тематикам, источникам, типам утверждений и уровням достоверности. Такой датасет станет ценным ресурсом как для дообучения и калибровки языковых моделей, так и для академических исследований в различных областях, включая сферу финансового контроля и безопасности.

Важнейшим преимуществом фреймворка AUTOFACTCHECK является его универсальность. Технологию можно применять в самых разных контекстах:

- как бот в мессенджерах, позволяющий пользователям мгновенно проверять сомнительные утверждения;
- как модуль маркировки контента на новостных сайтах, в социальных сетях или образовательных платформах, автоматически помечающий спорные или недостоверные высказывания;
- в виде браузерного расширения с интеграцией с различными LLM (YandexGPT, GigaChat) и модулем контентной безопасности;
- в сфере образования предполагается внедрение в качестве инструмента освоения компетенций в сфере ИТ и финансовой безопасности, кибербезопасности, работы с большими данными и верификации информации СМИ и социальных медиа.

Особый интерес использования фактчекинга возникает в рамках противодействия дипфейкам. Так, в процессе анализа система транскрибирует текст ролика, определяет общий эмоциональный посыл, выделяет смысловой нарратив и прогнозирует потенциальную общественную опасность. В настоящее время ведется работа по тестированию возможностей AUTOFACTCHECK при анализе информации «высокого социального риска», формировании отчетов о содержании текстов и выявлении признаков преступлений в сфере ПОД/ФТ/ФРОМУ.

Отдельное внимание уделяется возможности поиска информации в сети Интернет по текстам, которые включают фрагменты из приговоров уголовных дел за призывы к противоправной деятельности, что способствует автоматическому выявлению ресурсов и владельцев, требующих дальнейшей проверки. Возможности данных программных продуктов имеют колоссальный потенциал, так как в дальнейшем способны обеспечить широкое создание технологий ИИ, ориентированных на поиск достоверной информации, выявление подозрительных операций, противодействие манипулятивным действиям, повышение качества данных и защиту репутации.

Таким образом, научно-образовательные траектории фактчекинга в сфере финансовой безопасности способны содействовать цифровой трансформации, обелению экономики, выявлению риск-контингента ОД/ФТ/ФРОМУ, а также улучшению сервисов, основанных на использовании искусственного интеллекта.

Университет Лобачевского продолжает развивать научно-образовательные проекты, направленные на повышение уровня финансовой безопасности и открыт к совместной плодотворной деятельности!

Урок по финансовой безопасности:

ОТ ВНЕУРОЧНОЙ ИНИЦИАТИВЫ К МЕЖДУНАРОДНОМУ ОБРАЗОВАТЕЛЬНОМУ ПРОЕКТУ

МАРИНА ШЕМЯКИНА
Руководитель Центра межолимпиадной подготовки школьников и студентов (ФИАН)

В 2021 году в поддержку первой Международной олимпиады по финансовой безопасности при участии Департамента образования г. Москвы был подготовлен видеоролик для молодежи, где впервые поднимались вопросы финансовой грамотности и личной финансовой безопасности. То, что начиналось как внеурочное школьное мероприятие, стремительно переросло в масштабную международную образовательную инициативу. За 5 лет проведения в Уроке приняли участие более 12,5 млн человек.

Тема Урока 2026 — темная сторона искусственного интеллекта, в рамках которой освещаются вопросы применения ИИ в преступных схемах, создания поддельных сообщений, сайтов, подмены личности при помощи технологии дипфейков, формирования цифрового следа пользователя в сети «Интернет» и защиты персональных данных.

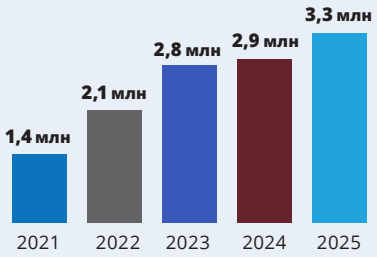
ОРГАНИЗАЦИОННАЯ МОДЕЛЬ УРОКОВ ПО ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Основная миссия проекта — воспитание нового поколения ответственных граждан, понимающих и осознающих, что финансовая безопасность — это фундамент суверенитета страны.

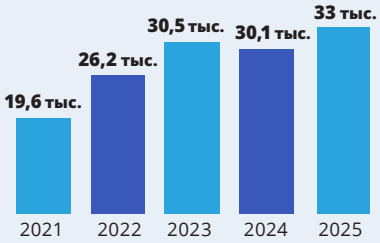
Традиционно Международная олимпиада по финансовой безопасности начинается с Урока. Именно тема Урока задает вектор всей содержательной части Олимпиады, определяя структуру заданий, тематику мастер-классов и фокус внимания экспертного сообщества. Кроме того, тема Урока способствует международному диалогу молодежи из более чем 40 стран мира. Единая повестка позволяет участникам из разных культур и правовых систем говорить на одном профессиональном языке. Общая тема — будь то формы мошенничества или этика ИИ — становится связующим звеном, которое превращает разрозненные знания в коллективный разум, направленный на защиту глобальной финансовой стабильности.

Проведение Урока поддерживают государственные и другие профильные институты: Минпросвещения России, Минобрнауки России, Росфинмониторинг, МВД России, подразделения финансовой разведки стран-партнеров, при участии которых ежегодно разрабатывается тема Урока. Она актуальна и соответствует проблематике и рискам в сфере противодействия легализации доходов и финансированию терроризма (ПОД/ФТ).

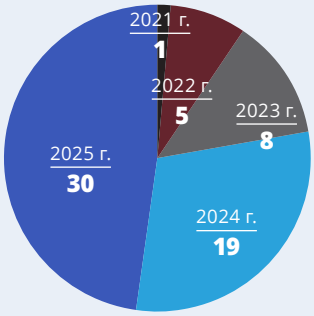
Численный охват молодежи, принявшей участие в Уроке в 2021–2025 гг.



Количество образовательных организаций, участвовавших в проведении урока в 2021–2025 гг.



Количество стран — участниц Урока



География Урока в 2025 г.

- о финансовой безопасности говорили в посольских школах в Алжире, Индонезии, Камбодже, Кувейте, Корее, Мозамбике, Сербии, Таиланде, Чили и Эфиопии.
- уроки прошли в Азербайджане, Армении, Аргентине, Беларуси, Бразилии, Индии, Иране, Египте, Казахстане, Китае, Кыргызстане, Узбекистане, Таджикистане, Туркменистане и в других странах.

С 2021 года разработкой материалов Урока в соответствии с утвержденной темой занимается вуз Международного сетевого института в сфере ПОД/ФТ: Российский университет дружбы народов имени Патриса Лумумбы. В эти материалы входят: содержательная презентация, конспект лекций для учителя и методические рекомендации по работе с презентацией.

Материалы Урока проходят экспертизу в Минпросвещения России, адаптируются и переводятся на иностранные языки. После этого материалы Урока направляются в органы образования, вузы Международного сетевого института в сфере ПОД/ФТ, школы, колледжи, образовательные детские центры и т. д.

В 2026 году Урок переведен на 6 языков ООН: английский, арабский, испанский, китайский, русский и французский.

Материалы урока доступны для самостоятельного изучения:

Официальный сайт Международной олимпиады по финансовой безопасности

Платформа «Содружество»

УЧАСТНИКИ И ФОРМАТЫ УРОКА

Изначально тематический урок по финансовой безопасности проводился на базе общеобразовательных школ в формате внеурочной деятельности. С 2023 года к его реализации подключились вузы — участники Международного сетевого института в сфере ПОД/ФТ. Уроки организовывали в подшефных школах, предуниверсариях, а затем — на площадках вузов для абитуриентов в рамках профориентационной деятельности при организации дня открытых дверей, выставки «Образование и карьера» и т. д.

Благодаря работе вузов МСИ Урок был адаптирован в формат лекционных занятий для студентов, включая обучающихся по профильным направлениям, связанным с тематикой Международной олимпиады по финансовой безопасности, а также для студентов других специальностей.

К проведению Урока приглашаются эксперты-практики, представители профильных министерств, ведомств, банковского и частного сектора. Партнерская сеть Урока по финансовой безопасности ежегодно расширяется. В качестве постоянных лекторов выступают эксперты Росфинмониторинга, включая межрегиональные управления, подразделений финансовой разведки и учебных центров стран-партнеров, Лаборатории Касперского, Сбера, Альфа-банка, Банка ПСБ, Т-банка и др.

Третий год подряд опорными площадками для проведения Урока по финансовой безопасности выступают главные детские центры страны: «Артек», «Смена», «Орленок» и «Океан». В текущем сезоне формат взаимодействия был существенно расширен: если ранее мероприятия носили эпизодический характер, то теперь уроки интегрированы в годовую программу обучения на протяжении нескольких смен. Благодаря такому подходу удалось охватить более 1000 наиболее инициативных школьников из разных стран, обеспечив глубокое погружение в повестку финансовой безопасности.

Большой интерес к уроку финансовой безопасности проявили полуфиналисты Всероссийского инженерного конкурса, интеллектуального соревнования, проводимого с 2021 года с целью формирования кадрового резерва

для инновационного развития России. Высокая вовлеченность полуфиналистов ВИК в изучение финансовой безопасности подчеркивает, что защита цифровой среды сегодня является фундаментом любого инженерного решения. Овладение навыками борьбы с кибермошенничеством и понимание рисков ИИ становятся обязательными компетенциями для инженеров нового поколения, создающих будущее нашей страны.

«Основная миссия проекта — воспитание нового поколения ответственных граждан, понимающих и осознающих, что финансовая безопасность — это фундамент суверенитета страны.

Особое внимание при проведении Урока в прошлом году было уделено ребятам, которые нуждаются в защите и поддержке больше всего — воспитанникам детских домов. Финансовая безопасность для них — не просто теория, а жизненно важные знания. Чтобы разговор получился честным и открытым, уроки проводили члены региональных Молодежных советов межрегиональных управлений Росфинмониторинга. Благодаря близости по возрасту и общему языку общения барьеры были сняты: встреча превратилась в искренний диалог, где каждый ребенок чувствовал себя услышанным и не боялся задавать самые смелые вопросы. Это первый и очень успешный опыт работы с такой важной аудиторией.

Кроме того, в уроках приняли участие более 250 российских учреждений социальной защиты.

Одной из самых ярких и масштабных площадок проведения урока в прошлом году стала Международная выставка-форум «Россия» на ВДНХ. Этот формат позволил выйти на новый уровень охвата и привлечь внимание самой разной аудитории. Благодаря партнерству с Минпросвещения России, региональными министерствами и Департаментом образования Москвы была создана единая точка доступа к знаниям о финансовой безопасности прямо в центре событий российской столицы. Мастер-классы и лекции, проводимые экспертами Международного учебно-методического центра финансового мониторинга на выставочных стендах, вызвали живой интерес у молодежи и стали отличным примером эффективного межведомственного сотрудничества в сфере финансового просвещения.

Тематики Урока в 2021–2026 гг.:

2021 «Финансовое мошенничество с банковскими картами»

Современные мошеннические схемы в сфере банковских платежей, технологии социальной инженерии и методы дистанционной компрометации данных. Меры профилактики и противодействия финансовым угрозам

2022 «Финансовые пирамиды»

Признаки и механизмы функционирования финансовых пирамид. Практика распознавания и снижения рисков вовлечения в мошеннические схемы

2023 «Финансовая безопасность личности в интернет-среде»

Угрозы, с которыми сталкиваются пользователи в интернет-среде. Важность защиты персональных данных, противодействия фишингу и предотвращения несанкционированных транзакций. Формирование устойчивого иммунитета к мошенническим схемам

2024 «НЕдетские игры: как не стать участником финансовых преступлений»

Риски вовлечения молодежи в преступные финансовые схемы. Правовые последствия содействия теневым финансовым операциям. Формирование этической установки на соблюдение финансовой дисциплины и законодательных норм

2025 «НЕдетские игры 2.0: Дроп поневоле»

Проблема вовлечения молодежи в цепочки легализации преступных доходов через механизм дропперства. Алгоритмы действий по предотвращению использования своих счетов в противоправных финансовых операциях

2026 «Темная сторона ИИ»

Неправомерное использование искусственного интеллекта в финансовой сфере, включая методы автоматизированного мошенничества, создания дипфейков, фишинга, вишинга, вербовки дропперов. Противодействие киберугрозам, формирование навыков критического восприятия цифрового контента и защиты персональных данных от продвинутых алгоритмов

Участники:
- школьники из разных стран
- студенты вузов МСИ
- студенты иных вузов
- детские центры и лагеря отдыха
- воспитанники детских домов
- учащиеся школ при посольствах
- учителя, преподаватели вузов, эксперты-практики
- пенсионеры

> 12,5 млн человек

С целью повышения вовлеченности участников и масштабирования проекта с 2024 года внедряются обновленные форматы проведения тематических уроков. Традиционные материалы перерабатываются в современный видеоконтент, адаптированный под информационные запросы молодежной аудитории. В поддержку тематических материалов уже снято более 20 видеолекций и видеороликов, понятных и интересных школьникам и студентам. Например, в Ставропольском государственном аграрном университете студентами — финалистами V Международной олимпиады по финансовой безопасности подготовлен мини-сериал, сюжет которого сфокусирован на противодействии современным киберугрозам и «темной стороне» технологий. Авторы наглядно демонстрируют механизмы работы нейросетей в руках мошенников и обучают зрителей методам цифровой защиты. Этот проект стал важным шагом в цифровой трансформации Урока, превратив его из обычной лекции в увлекательный медиапродукт, отвечающий интересам современных школьников и студентов.

«В поддержку тематических материалов уже снято более 20 видеолекций и видеороликов, понятных и интересных школьникам и студентам.

УРОК КАК ИНСТРУМЕНТ НАСТАВНИЧЕСТВА И СОЦИАЛЬНОГО ЛИФТА

Одним из наиболее эффективных форматов проведения Урока, на наш взгляд, является формат, при котором в роли лекторов и спикеров Урока по финансовой безопасности выступают финалисты и победители Олимпиады прошлых лет. Этот подход базируется на методе «равный — равному» и обладает рядом уникальных преимуществ.

Во-первых, информация воспринимается легче, когда она исходит от сверстника. Отсутствие возрастного и иерархического барьера (учитель — ученик) снимает психологическое напряжение и повышает вовлеченность слушателей.

Во-вторых, финалисты делятся не только теорией, но и практическими советами: как лучше готовиться к Олимпиаде, на что обратить внимание, как справляться со стрессом в финале. История успеха или живой пример сверстника, который уже прошел путь от обычного школьника/студента до финалиста Олимпиады, мотивирует и вдохновляет.

Очевидные плюсы данный проект несет и для самих спикеров: обучая других, финалисты Олимпиады сами глубже погружаются в материал, повышают свой уровень знаний. Участие в роли лектора развивает навыки публичных выступлений, лидерские качества, умение работать с аудиторией и аргументировать свою позицию. Это важнейший этап профессионального роста будущего специалиста финансовой разведки. Выступая послами Олимпиады и Международного движения по финансовой безопасности, ребята осознают свою значимость как части мирового профессионального сообщества, что укрепляет их лояльность к выбранной профессии.

В своих университетах уроки проводили финалисты Олимпиады из Алжира, Бразилии, Индии, Ирана, Кубы, Казахстана, Кыргызстана, Китая, России, Узбекистана, Таджикистана.

Форматы:
- в очном формате в школах
- в очном формате на площадках вузов в рамках дня открытых дверей и выставки «Образование и карьера»
- онлайн-трансляции и уроки в дистанционном формате
- трансляция на платформе «Содружество»
- на выставке-форуме «Россия» на ВДНХ на стендах Минпросвещения России
- с привлечением финалистов Международной олимпиады по финансовой безопасности из Алжира, Бразилии, Индии, Ирана, Кубы, Казахстана, России, Таджикистана, Узбекистана

МЕРОПРИЯТИЯ-«СПУТНИКИ»

Отдельного внимания заслуживают образовательные мероприятия, проводимые в поддержку тематического Урока по финансо-

вой безопасности и старта Международной олимпиады по финансовой безопасности.

Например, масштабное мероприятие «Финбез Weekend» проходит второй год подряд в ННГУ им. Н. И. Лобачевского совместно с Межрегиональным управлением Федеральной службы по финансовому мониторингу по Приволжскому федеральному округу и собирает международную аудиторию более 4 тысяч человек, включая участников из российских регионов (от Поволжья до Северного Кавказа), учащихся образовательных организаций Минска (Беларусь), Ашхабада (Туркменистан), Ташкента (Узбекистан) и Нови-Сада (Сербия).

▸ Урок по финансовой безопасности для участников фиджитал-турнира «Игры будущего», Казань, 2024 год

В Республике Казахстан уроки по финансовой безопасности проходят в формате образовательного фестиваля по всей стране — тематические лекции, флешмобы, конкурсы рисунков и викторины.

В Республике Таджикистан уже третий год подряд проводится классическая олимпиада в очном формате, где принимают участие школьники из всех районов республики. Организаторы Олимпиады добираются до самых удаленных точек, горных районов республики, чтобы провести Урок по финансовой безопасности и найти талантливых и мотивированных участников.

По инициативе Учебного центра Государственной службы финансовой разведки Кыргызской Республики урок по финансовой безопасности стал частью обязательного школьного предмета «Человек и общество». Этому предшествовала системная подготовка методической базы: разработка методических рекомендаций к уроку для педагогического состава. Эту идею поддержало государство, и сегодня педагоги по всей стране используют эти материалы, обучая школьников правилам безопасности в современном финансовом мире.

РЕЗЮМЕ И ПЛАНЫ НА БУДУЩЕЕ

За 5 лет Урок по финансовой безопасности стал самостоятельным образовательным проектом Международного движения по финансовой безопасности. Его проведение формирует устойчивые сообщества: участники Олимпиады не «исчезают» после финала, а остаются в проектах и Движении, выступая его движущей силой. Планируется продолжить развитие системы наставничества («финалисты — новым участникам») для подготовки кадров профессионального сообщества.

Одной из ключевых перспектив является создание международной базы методических материалов, адаптированной под правовые и культурные особенности стран-партнеров. Это позволит сформировать единый культурный код финансовой безопасности на международном уровне.

В планах на 2026 год и далее — создание полноценной цифровой образовательной среды с веб-элементами, геймификацией и технологиями искусственного интеллекта. Урок эволюционирует в обучающий сериал-тренажер, где каждый участник сможет в реальном времени отрабатывать навыки противодействия финансовым угрозам в интерактивном формате.

Ну и наконец, укрепление финансового суверенитета через массовое просвещение. Урок закладывает основы коллективного иммунитета к финансовым преступлениям. Это стратегическая задача Движения — воспитать поколение, способное обеспечить экономическую стабильность и безопасность своих стран в условиях глобальной неопределенности.

«В планах на 2026 год и далее — создание полноценной цифровой образовательной среды с веб-элементами, геймификацией и технологиями искусственного интеллекта.

Медиапрививка от обмана:

ВЛАДИМИР ТОДОРОВ

О РОЛИ ДОКУМЕНТАЛЬНОГО КИНО В ПРОФИЛАКТИКЕ МОШЕННИЧЕСТВА

Сегодня телефонное мошенничество стало масштабной индустрией, использующей психологию, технологии и глобальную инфраструктуру. В ответ на это киноиндустрия все чаще берет на себя не только информационно-развлекательную, но и профилактическую функцию, объясняя зрителям, как устроены схемы обмана и почему на них попадаются даже образованные и осторожные люди. О том, может ли документальное кино играть роль «медиавакцины» от мошенничества и как создаются подобные проекты, редакция «Финансовой безопасности» поговорила с продюсером документального контента Okko Владимиром Тодоровым — автором журналистского расследования о внутренней кухне кол-центров как криминальной индустрии.

— Владимир, что вас подтолкнуло к созданию проекта на тему мошенничества?

— У меня есть опыт и интерес к исследованию тем, которые сильно и негативно влияют на нашу жизнь, но про которые много не говорят. Когда мы взялись за тему телефонных мошенников, все-таки она не была так популярна, как случилось в процессе производства и уж тем более во время релиза. При этом мне всегда интересно как журналисту-расследователю смотреть вглубь и не просто рассказывать истории жертв. Сегодня они не вызывают у людей ни сочувствия, ни интереса. Пока ты не покажешь механизм, схему работы, люди не поверят. Весь контент про телефонных мошенников в 2023–2024 гг. строился на историях жертв. Мы решили пойти от противного: задались целью рассказать о том, как устроена масштабная индустрия мошенничества, про ее законы и персонал. И у нас получилось. Единственный вызов, с котором мы столкнулись, — размещение большинства мошеннических кол-центров за рубежом, а значит, отсутствие возможности снять реальных участников. Поэтому нам пришлось выдумать некую художественную линию, в основу которой легли реальные диалоги с теми, кто ранее работал в кол-центрах.

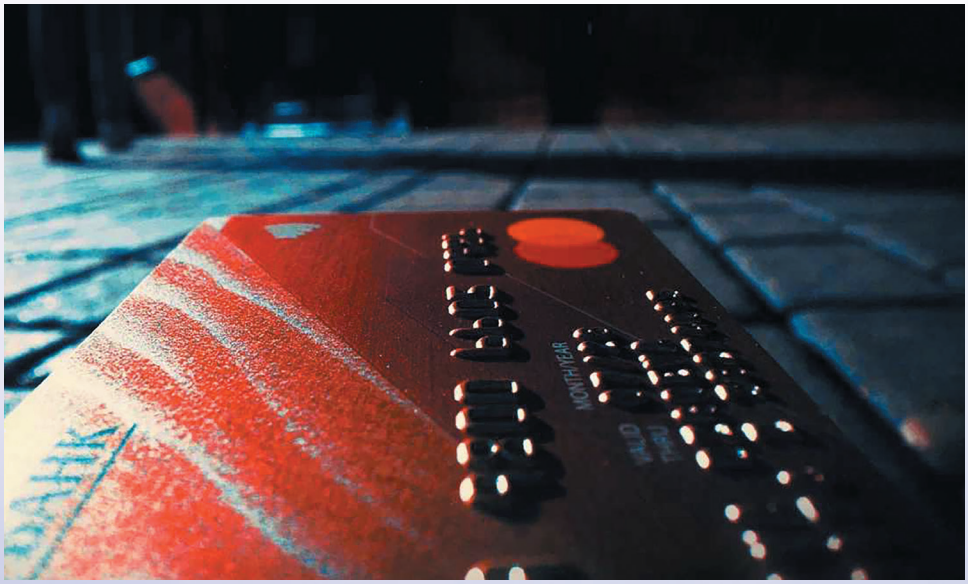
«На мой взгляд, на зрителей больше всего действуют объяснения, как работает машина мошенничества и кому это выгодно. Таким образом зритель из некой неощутимой угрозы понимает, что в реальности ему противостоит, становится более осторожным.

— Получается, на зрителя больше действуют факты, а не эмоции?

— На мой взгляд, на зрителей больше всего действуют объяснения, как работает машина мошенничества и кому это выгодно. Таким образом зритель из некой неощутимой угрозы понимает, что в реальности ему противостоит, становится более осторожным.

— Была ли обратная связь от зрителей, может, сериал помог избежать схемы обмана?

— Мы получили очень много обратной связи от разных возрастных групп, но запомнилось больше всего вот что. Мы показывали сразу все серии в главном центре московского долголетия. «На крючке: когда звонит мошенник» выходил в спайке с художественным сериалом «Мамонты»: мы уделяли много внимания старшему поколению, потому что оно самое доверчивое и особенно подвержено мошенническим угрозам. Я опасался, что слишком динамичный монтаж, обилие графики может показаться им излишне сложным, перегруженным просто потому, что старшее поколение зачастую смотрит другой контент. Но как я был не прав — они получили огромное удовольствие, после показа мы проговорили 2,5 часа, я лично настраивал бабушкам двухфакторную идентификацию в мессенджере. Они благодарили за то, что мы объяснили, как работают подобные схемы, ведь на момент 2024 года до сознания людей еще не доносили такое количество информации о мошенниках. Наверное, мы первые вышли с таким контентом на широкую аудиторию.

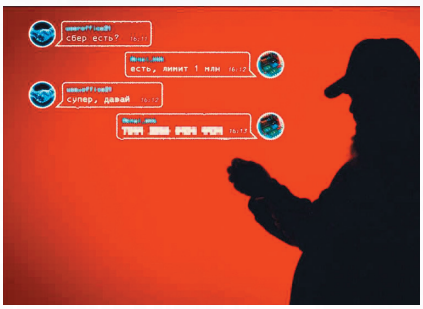


Источник фото: Okko

— Что было самым сложным в работе над этой темой?

— Самым сложным было добраться до работников кол-центров, на каждой стадии были свои вызовы. Уже на начальном этапе написания сценарных планов стало очевидно, что нам нужны инсайды. Найти их оказалось довольно непросто, но благодаря журнали-

стам нам это удалось. Следующая проблема — обеспечить безопасность инсайдеров, потому что по косвенным признакам можно было определить, где они работают, а люди, которые держат и крышуют кол-центры, в целом со своим персоналом не церемонятся. Поэтому нам пришлось очень тщательно сглаживать истории, чтобы нельзя было догадаться, где работают конкретно наши источники. И были сложности с тем, чтобы визуализировать сюжет: кол-центр в сериале практически скопирован с одного из реальных центров в Днепре.



Источник фото: Okko

— Считаете ли тему мошенничества этически сложной?

— Нет: очевидно, что виноват тот, кто обманывает. Ключевые действия — просвещать население: нельзя брать трубки с незнакомых номеров, нужно всегда проверять, с кем ты общаешься. Самое опасное, что можно сделать и что довольно часто делают в сети, это перекладывать ответственность и вину на жертву. Люди не виноваты в том, что они проявляют больше доверия и эмпатии, чем того требует наше суровое время. Не виноваты в том, что они боятся авторитетов в лице сотрудников ведомств. Не виноваты и в том, что они пугаются звонка в 8 утра от «начальника» с просьбой связаться с сотрудником ФСБ.

Мошенникам удалось развести жертву из-за недостатка технического контроля (почему этот звонок вообще прошел) и из-за недостатка информированности (человек просто не знал, что обман возможен). Отлично, что обе проблемы сейчас активно ликвидируются. Сегодня трудно вообразить себе человека, который не знает про большинство популярных мошеннических схем, и очень трудно вообразить, что мошенники смогли вот так легко позвонить, ведь процент звонков сильно снижается. При этом нельзя заканчивать с просветительскими кампаниями, поскольку изобретается большое количество мошеннических схем. Это огромная индустрия, она не может просто взять и раствориться.

«Нельзя заканчивать с просветительскими кампаниями, поскольку изобретается большое количество мошеннических схем. Это огромная индустрия, она не может просто взять и раствориться.

— В чем опасность новых технологий в руках мошенников?

— К сожалению, история с генеративным искусственным интеллектом, дипфейками и поддельными голосовыми идет на пользу кол-центрам. Это бизнес, а бизнесу нужно наращивать прибыль, сокращая расходы. Голосовые модели, сгенерированные на основе скачанного архива видео и аудио из взломанного аккаунта, могут сократить траты на персонал. Недалек тот день, когда сотрудников кол-центров первого звена, так называемых холодильников (прим. ред. «холодильники» являются первичным звеном в мошеннической схеме, совершают «холодные» звонки по номерам из баз данных), заменят на ИИ или на продвинутых голосовых роботов. Вторая история — это точечная работа по более богатым потенциальным жертвам из-за утечек банковских баз данных. Мошенники уже сегодня этим занимаются, весь вопрос в том, насколько эти схемы будут совершенствоваться. Аферисты ищут точечный подход к жертвам с помощью методов социальной инженерии: анализируют окружение, социальные сети, определяют, куда можно надавить, кем можно притвориться. После — стадия взлома и внедрения, отправка сгенерированных видео и аудио. Эти угрозы будут только расти. Задача людей, которые занимаются контентом, определять угрозы и предупреждать людей раньше, чем мошенники начнут масштабировать схемы.

Источник фото: Okko

Беседовала Екатерина Истомина, главный специалист-эксперт пресс-службы Росфинмониторинга

Деньги как элемент культуры:

ПАМЯТНЫЕ МОНЕТЫ И БАНКНОТЫ СТРАН ЕВРАЗИЙСКОЙ ГРУППЫ

Страны Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма объединяет богатая культурная традиция. Каждое государство выпускает памятные монеты и банкноты, посвященные важным событиям национальной истории.

Памятные деньги — особая часть денежной системы. Формально они остаются законным платежным средством, однако чаще служат культурным и историческим символом. Центральные банки разных стран выпускают такие банкноты и монеты к юбилеям, историческим событиям, достижениям науки или важным национальным датам. Они часто отличаются сложным художественным оформлением.

История памятных денег уходит глубоко в прошлое. Еще в античные времена правители чеканили монеты в честь военных побед или важных государственных событий. В современном виде традиция сформировалась в XX веке, когда многие государства начали выпускать специальные денежные серии.

РОССИЯ: МОНЕТА К 80-ЛЕТИЮ ПОБЕДЫ

В 2025 году Банк России выпустил памятную монету номиналом 50 рублей, посвященную 80-летию Победы в Великой Отечественной войне. На реверсе монеты изображен знаменитый мемориал «Родина-мать зовет!» в Волгограде — один из самых узнаваемых символов памяти о войне. Монета была выпущена крупным тиражом, поэтому часть экземпляров попала в обычное денежное обращение. Однако многие из них сразу стали предметом коллекционирования.

Источник фото: https://www.cbr.ru/

БЕЛАРУСЬ: МОНЕТА «ВСЕМИРНОЕ НАСЛЕДИЕ ЮНЕСКО. МИРСКИЙ ЗАМОК»

Беларусь активно использует памятные деньги для популяризации архитектурного наследия. Монета 1 рубль «Мирский замок» была выпущена в 2014 году. На реверсе изображен знаменитый Мирский замок — один из главных исторических символов страны и объект Всемирного наследия ЮНЕСКО. Его стилизованное изображение отражается в воде, символизируя глубину веков, загадочность и множество нераскрытых тайн.

Источник фото: https://monloisir.ru/

КЫРГЫЗСТАН: МОНЕТА «АЙТМАТОВ — 90 ЛЕТ»

Национальный банк Кыргызстана в 2018 году выпустил серебряную монету «90 лет со дня рождения Чингиза Айтматова». Она посвящена знаменитому писателю, произведения которого переведены на десятки языков. На реверсе монеты изображен портрет Айтматова и элементы, связанные с его литературным наследием, — белый пароход и Мать-олениха. Выпуск монеты стал данью уважения одному из самых известных культурных деятелей страны.

Источник фото: https://vmiremonet.ru/

ТАДЖИКИСТАН: БАНКНОТА 500 СОМОНИ

В Таджикистане памятный характер нередко имеют и банкноты. Например, банкнота номиналом 500 сомони, выпущенная в 2010 году, посвящена выдающемуся поэту и мыслителю X века Абу Абдуллаху Джафару Рудаки, которого считают основателем классической персидско-таджикской литературы. На лицевой стороне банкноты изображен портрет поэта, выполненный по историческим реконструкциям, а на обороте — архитектурные мотивы и национальные орнаменты.

Источник фото: https://coins-mos.ru/

УЗБЕКИСТАН: МОНЕТА К 2200-ЛЕТИЮ ТАШКЕНТА

Центральный банк Узбекистана в 2009 году выпустил памятную монету 100 сум, посвященную 2200-летию Ташкента. На реверсе изображен Монумент независимости Узбекистана и скульптура Счастливой матери, которая символизирует Родину, мудрость, надежду на светлое будущее. Этот выпуск стал частью масштабных мероприятий, посвященных юбилею одной из старейших столиц Центральной Азии.

Источник фото: https://albonumismatico.com/

ТУРКМЕНИСТАН: МОНЕТА «АХАЛТЕКИНСКАЯ ЛОШАДЬ»

Туркменистан выпускает памятные монеты, посвященные национальным символам. Одной из таких стала серебряная монета «Ахалтекинская лошадь» номиналом 50 манатов. Ахалтекинская порода считается национальной гордостью страны и одной из древнейших пород лошадей в мире. На реверсе монеты изображен изящный профиль скакунов, выполненный с высокой детализацией, на фоне гор. Композиция подчеркивает грациозность животного и значение коневодства для культуры Туркменистана.

Источник фото: https://ru.ucoin.net/

КИТАЙ: МОНЕТА К ОЛИМПИАДЕ В ПЕКИНЕ

Китай активно использует памятные монеты для отражения крупных международных событий. В серию монет, выпущенных к летним Олимпийским играм 2008 года в Пекине, вошли как обычные памятные монеты, так и коллекционные экземпляры из серебра и золота. На них изображены олимпийские виды спорта, традиционные китайские символы и элементы культуры. Некоторые монеты показывают спортсменов в движении, что придает композиции динамику. Другие используют традиционные китайские мотивы, соединяя современный спорт с многовековой культурной традицией страны.

Источник фото: https://www.monetnik.ru/

ИНДИЯ: МОНЕТА К 150-ЛЕТИЮ МАХАТМЫ ГАНДИ

Индия выпустила памятную монету номиналом 150 рупий, посвященную 150-летию со дня рождения Махатмы Ганди — лидера движения за независимость и одного из самых известных политических деятелей XX века. На реверсе монеты изображен портрет Ганди, выполненный на основе исторических фотографий. Рядом размещена памятная надпись с указанием события.

Источник фото: https://en.numista.com/

КАЗАХСТАН: МОНЕТА «ДЖЕЙРАН»

В 2005 году Национальный банк Казахстана выпустил серебряную монету номиналом 500 тенге из серии «Красная книга Казахстана», посвященную редкому виду газели — джейран. Это изящное степное животное обитает в пустынных и полупустынных районах страны и считается одним из символов экосистемы Центральной Азии. На реверсе монеты изображена пара джейранов в характерной для животного позе: они стоят настороженно, словно прислушиваясь к звукам степи. На заднем плане – стилизованный пустынный ландшафт с плавными линиями холмов. Аверс украшен государственным гербом Казахстана, номиналом и традиционными казахскими орнаментами.

Источник фото: https://www.monetnik.ru/

Подготовила Екатерина Истомина, главный специалист-эксперт пресс-службы Росфинмониторинга

НОВОСТИ АНТИОТМЫВОЧНОЙ СИСТЕМЫ

МЕХИКО: в Мексике прошла Пленарная сессия Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ)

Делегации обсудили актуальные вопросы противодействия отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Утверждены отчеты о взаимной оценке Австрии, Италии и Сингапура, в которых рассмотрена эффективность антиотмывочных мер с точки зрения соответствия их Рекомендациям ФАТФ. В «серый» список ФАТФ включены Кувейт и Папуа — Новая Гвинея, «черный» остался без изменений.

АСТАНА: обучение для экспертов-оценщиков Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ)

Участники мероприятия изучили основные подходы к проведению взаимных оценок национальных антиотмывочных систем. Прошедшие обучение сотрудники будут включены в пул экспертов, имеющих право участвовать в оценочных миссиях.

ВЕНА: Глобальный саммит по проблеме мошенничества

Сотрудники Федеральной службы по финансовому мониторингу в составе российской межведомственной делегации приняли участие в Глобальном саммите по проблеме мошенничества. Мероприятие прошло в Австрии и объединило представителей профильных ведомств, правоохранительного блока, международных организаций, частного сектора и экспертного сообщества. Организатором выступило Управление ООН по наркотикам и преступности (УНП ООН) совместно с Интерполом. Эксперты обсудили проблему глобальной распространенности мошенничества, работы скам-центров и принимаемые странами меры по выявлению и пресечению деятельности транснациональных преступных групп.

ТАШКЕНТ: в Узбекистане обсудили меры по борьбе с финансированием терроризма

Дискуссия состоялась на полях Совместного семинара Совета руководителей подразделений финансовой разведки государств — участников СНГ (СРПФР), Антитеррористического центра СНГ, Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ) и Международного учебно-методического центра финансового мониторинга (МУМЦФМ).

Семинар направлен на укрепление взаимодействия между подразделениями финразведки и правоохранительными органами в сфере противодействия финансированию терроризма. За два дня программы участники обменялись опытом и лучшими практиками по линии межведомственного взаимодействия и международного сотрудничества.

МОСКВА: состоялось заседание организационного комитета VI Международной олимпиады по финансовой безопасности

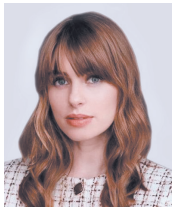
Заседание прошло под председательством заместителя Председателя Правительства РФ Дмитрия Чернышенко. В обсуждении финального этапа участвовали директор Росфинмониторинга Юрий Чиханчин, губернатор Красноярского края Михаил Котюков, представители ведомств и соорганизаторы. Отмечен возрастающий интерес к Олимпиаде со стороны молодых людей из России и зарубежных стран: в 2026 году в финальной неделе примут участие до 700 школьников и студентов из более чем 40 стран. В рамках профессионального трека на полях финала пройдут форум Международного движения по финансовой безопасности, заседание совета Международного сетевого института, мероприятия по линии БРИКС.

РЕДАКЦИОННЫЙ СОВЕТ

Председатель редакционного совета
Чиханчин Ю.А.

Заместитель председателя редакционного совета
Овчинников В.В.

Заместитель председателя редакционного совета
Негляд Г.Ю.



Главный редактор
Рязанова И.С.

ЧЛЕНЫ РЕДАКЦИОННОГО СОВЕТА

Бобрышева Г.В.

Гилета Е.С.

Корнев И.А.

Крылов О.В.

Лисицын А.С.

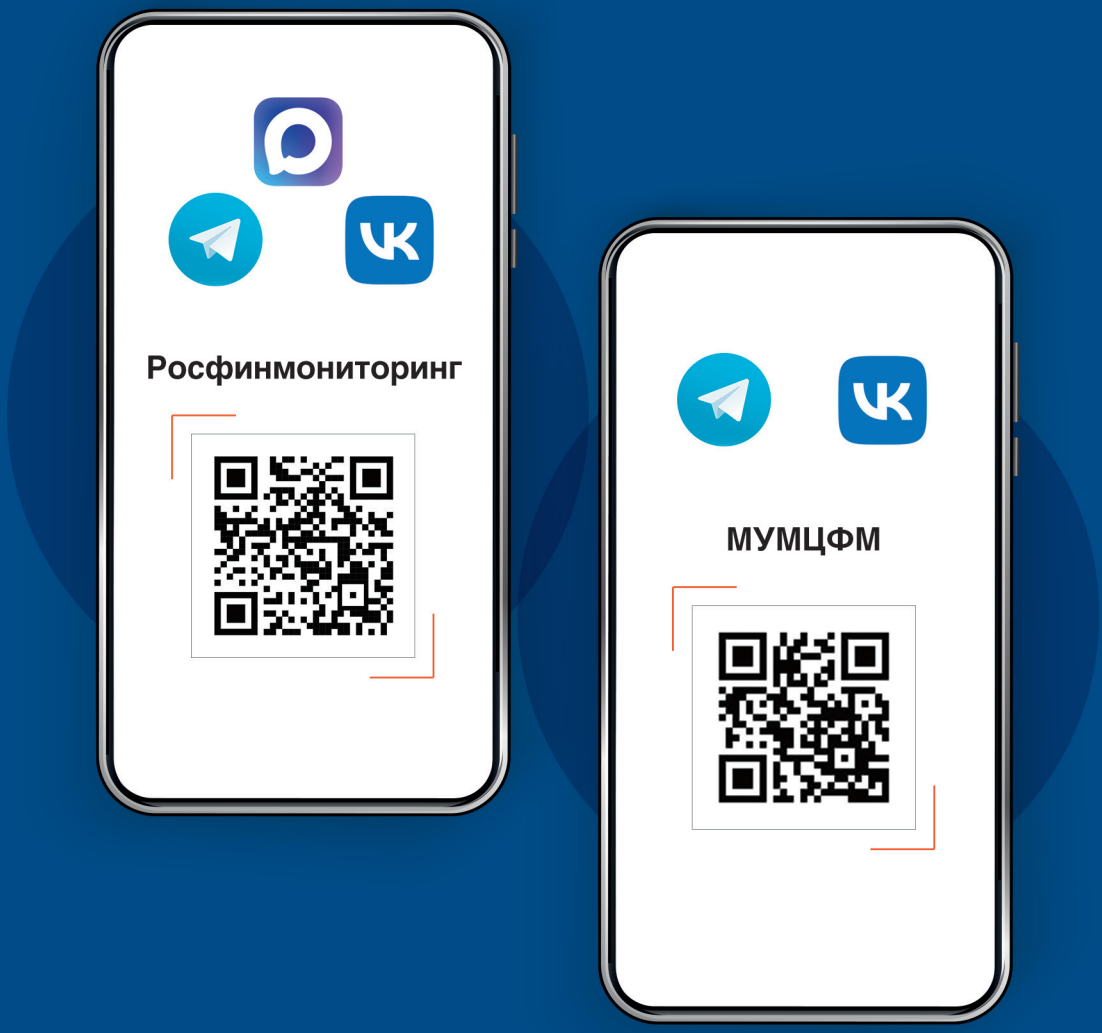
Петренко А.Г.

Тетеруков С.А.

Уваров И.А.

Шемякина М.С.

Росфинмониторинг и МУМЦФМ в MAX, Telegram и VKontakte



Издательство
Автономная некоммерческая организация
Международный учебно-методический центр финансового мониторинга
105064, г. Москва, Хомутовский тупик, 5А, стр. 1.
E-mail: info@mumcfm.ru
Тираж 600 экземпляров.

Мнение редакции может не совпадать с позицией авторов.

МУМЦФМ
2026