АССОЦИАЦИЯ КОРПФИНТЕХ

Перспективы развития процедур KYC в России на основе глобального опыта

Аналитический отчет

2026

Алексей Сизов
Вице-президент по развитию Ассоциации КорпФинТех

Уважаемые коллеги!

Представляю вашему вниманию комплексное исследование, посвященное перспективам и стратегии развития процедуры KYC (Know Your Customer) в Российской Федерации.

Российский финансовый сектор совершил масштабный переход к модели тотальной цифровой идентификации, опирающейся на сквозные государственные платформы — ЕСИА, Единую биометрическую систему (ЕБС), платформу «Знай своего клиента» (ЗСК) и ГИС «Антифрод». Эти изменения позволили существенно повысить прозрачность и безопасность рынка, однако они же поставили перед нами новые, не менее сложные вызовы.

В Ассоциации КорпФинТех мы ежедневно видим, как трансформируются бизнес-процессы наших участников. Мы понимаем, что для устойчивого развития цифровой экономики процедура KYC не должна превращаться исключительно в репрессивный механизм или тяжелое административное бремя.

Эффективный комплаенс будущего — это интероперабельная экосистема, которая обеспечивает абсолютную безопасность расчетов, минимизирует операционные издержки финансовых институтов и гарантирует бесшовный клиентский опыт.

Чтобы сформировать объективный образ будущего для российской инфраструктуры, в рамках данного исследования мы вышли за рамки локального рынка. Нами был проведен анализ передовых международных практик.

Мы детально проанализировали архитектуру Центрального реестра CKYCRR в Индии, национальную блокчейн-платформу в Объединенных Арабских Эмиратах, высокоинтегрированные системы Myinfo и COSMIC в Сингапуре, а также гибридный опыт скандинавских стран.

Особое внимание в отчете уделено самым острым и дискуссионным вопросам отрасли: правовым последствиям использования централизованных систем, распределению ответственности за риски идентификации (концепция Safe Harbor) между банками и операторами данных, влиянию комплаенс-скоринга на корпоративную ликвидность, а также технологическим перспективам перехода к непрерывному мониторингу (Perpetual KYC).

Это исследование — экспертный компас, цель которого — примерить лучшие мировые решения к российскому правовому и ИТ ландшафту.

Мы хотим предложить рынку вектор развития процедур идентификации. Надеемся, что материалы и выводы данного исследования станут хорошей отправной точкой для принятия стратегических и архитектурных решений при развитии KYC-инфраструктуры в России.

Об Ассоциации

Созданная по инициативе корпоративного сообщества и ключевых участников финансового рынка, Ассоциация КорпФинТех является межотраслевой площадкой для взаимодействия представителей крупнейших корпораций России с ИТ-организациями, платежными платформами, банками, телеком-операторами, вендорами, инновационными компаниями, венчурными проектами и другими ключевыми участниками отрасли с целью создания условий для развития перспективных финансовых технологий для корпоративного сектора.

Ассоциация объединяет ведущих экспертов рынка, обеспечивает постоянный мониторинг, анализ и трансляцию ключевых тематических материалов для своего сообщества. Для участников Ассоциации КорпФинТех доступны отечественные и иностранные обзоры, исследования, аналитика, мнения и комментарии. Регулярно проходят мероприятия различных масштабов и форматов, обеспечиваются условия для эффективной коммуникации как внутри сообщества, так и с внешними участниками в России и за рубежом.

Оглавление

АССОЦИАЦИЯ КОРПФИНТЕХ

Суть процедуры KYC 6

Ключевые проблемы и вызовы процедуры KYC 8

Влияние комплаенс-процедур на бизнес 9

Процедура KYC в России 10

Международный опыт KYC 14

Распределение ответственности 26

Шаги развития KYC в России 27

Эталон процедуры KYC 28

Использованные источники 30

Суть процедуры KYC

Процедура KYC (Know Your Customer / «Знай своего клиента») представляет собой строго регламентированный и технологический процесс, посредством которого финансовые институты выполняют идентификацию и верификацию клиентов, оценивают их риск-профиль на предмет вовлеченности в легализацию преступных доходов (AML), финансирование терроризма (CFT) и мошеннические схемы. В современной архитектуре финансового мониторинга KYC представляет собой комплексную систему, состоящую из взаимосвязанных участников и функциональных блоков.

Участники процедуры KYC

В рамках процедуры KYC взаимодействуют четыре ключевые группы сторон:

- **Финансовые институты (субъекты контроля):** Банки, микрофинансовые организации (МФО), операторы цифровых финансовых активов (ЦФА), криптовалютные биржи и страховые компании. Они несут прямую ответственность за выполнение проверок и выявление сомнительной активности.
- **Клиенты:** Физические лица (сегмент B2C) и юридические лица или индивидуальные предприниматели (сегмент B2B), обязанные предоставлять верифицированные сведения при онбординге и обновлении данных.
- **Поставщики данных и операторы инфраструктуры:** Государственные информационные системы, ведомственные реестры, операторы биометрических данных, а также специализированные провайдеры списков санкций, политически значимых лиц (PEP) и негативных новостей (Adverse Media).
- **Регуляторы и надзорные органы:** Государственные органы, устанавливающие нормативно-правовые стандарты и осуществляющие предиктивный контроль (в РФ — Банк России, Росфинмониторинг).

Базовые функциональные блоки

- **Программа идентификации клиентов:** Начальный этап сбора первичных идентификаторов. Для физических лиц — ФИО, дата рождения, адрес регистрации и реквизиты документов. Для юридических лиц — наименование, регистрационный номер, учредительные документы и сведения об органах управления и др.
- **Верификация данных:** Проверка достоверности собранных сведений по независимым, официальным и авторитетным источникам (базам данных госорганов, биометрическим слепкам и другим доступным реестрам).
- **Надлежащая проверка клиента:** Анализ характера деятельности клиента, структуры его собственности (выявление бенефициаров) и составление риск-профиля контрагента для предотвращения скрытых угроз.
- **Усиленная проверка:** Углубленный аудит клиентов с повышенным уровнем комплаенс-риска (включая PEP, компании из офшорных зон или юрисдикций под санкциями) с раскрытием источников происхождения капитала.
- **Мониторинг:** Отслеживание транзакционной активности и изменений регистрационных данных клиента на протяжении всего его жизненного цикла.

Ключевые проблемы и вызовы процедуры KYC

- **Дублирование запросов и «клиентская усталость»:** Из-за изолированности внутренних систем коммерческих банков клиенты вынуждены многократно предоставлять идентичные пакеты документов при открытии счетов в разных банках, сталкиваясь с административным давлением.
- **Отсутствие гармонизации и разрозненность форматов данных:** Различия во внутренних регламентах финансовых организаций приводят к тому, что схожая информация запрашивается в разных форматах (сканы, оригиналы, выписки, нотариальные копии), что блокирует сквозную автоматизацию.
- **Чрезмерная нагрузка на комплаенс-подразделения:** Огромный массив рутинных операций по сопоставлению данных выполняется вручную комплаенс-офицерами, что приводит к операционным ошибкам и отвлекает ресурсы от сложной интеллектуальной оценки рисков.
- **Технологические барьеры удаленных каналов:** Процесс цифрового онбординга часто усложняется дефицитом качественного интернет-покрытия в удаленных регионах и психологическим барьером пользователей перед передачей биометрических данных.

Влияние комплаенс-процедур на бизнес

В современных реалиях скорость и бесшовность комплаенс-контроля имеют для корпоративного сектора прямое экономическое выражение. Любая задержка при верификации контрагентов, ложное алгоритмическое срабатывание систем финансового мониторинга или внезапное ограничение дистанционного банковского обслуживания (ДБО) мгновенно парализуют транзакционные потоки компании. Это оборачивается блокированием значительных объемов оборотного капитала, срывом контрактных обязательств, штрафными санкциями и, в критических случаях, возникновением кассовых разрывов.

Для минимизации этих рисков корпоративные казначейства вынуждены отвлекать ресурсы из операционного оборота и формировать избыточный буфер ликвидности — держать «замороженные» остатки на резервных счетах для подстраховки на случай непредвиденных блокировок.

Переход финансовой инфраструктуры к предиктивным моделям и концепции непрерывного KYC (Perpetual KYC) кардинально меняет эту ситуацию.

Быстрая автоматическая верификация данных из доверенных государственных реестров позволяет казначеям проводить платежи без искусственных задержек, повышает оборачиваемость капитала, высвобождает скрытую ликвидность и кардинально укрепляет общую платежную дисциплину внутри холдинговых структур.

Процедура KYC в России

Обзор регуляторной модели

Российская национальная модель построена на принципах риск-ориентированного подхода с глубокой централизацией верификационных сервисов на стороне государственных операторов при сохранении децентрализованной оценки рисков в банках.

Регуляторный ландшафт определяется:

- Федеральным законом № 115-ФЗ (в его актуальной 128-й редакции),
- Федеральным законом № 572-ФЗ (регулирующим оборот биометрических данных) и
- Федеральным законом № 41-ФЗ (в рамках которого развернута ГИС «Антифрод»).

С 1 марта 2026 года регулятор ввел жесткие требования: микрофинансовые компании (МФК) полностью лишены права применять упрощенную идентификацию при выдаче онлайн-займов. Теперь они обязаны проводить строгую проверку через связку ЕСИА и Единой биометрической системы (ЕБС) для борьбы с цифровым мошенничеством.

Надзорную и методологическую координацию осуществляют Банк России, Росфинмониторинг и Минцифры.

Архитектура хранения и обмена данными

Инфраструктура опирается на сквозные государственные платформы:

- **ЕСИА (Единая система идентификации и аутентификации):** Главная государственная точка входа для подтверждения цифрового профиля гражданина.
- **Цифровой профиль СМЭВ 4:** Высокоскоростная система межведомственного электронного взаимодействия, обеспечивающая банкам прямой легитимный доступ к данным ФНС (доходы, налоги) и Социального фонда РФ.
- **Единая биометрическая система (ЕБС):** Централизованная платформа хранения и верификации биометрических векторов (лица и голоса).
- **Платформа «Знай своего клиента» (ЗСК) Банка России:** Централизованный комплаенс-ядро, распределяющий всех юридических лиц и ИП страны по трем зонам риска («зеленая», «желтая», «красная»).
- **ГИС «Антифрод»:** Предиктивная система реального времени под эгидой Роскомнадзора, анализирующая цифровой след устройств и сотовых номеров для пресечения фрод-активности.

Процедура идентификации и верификации

Взаимодействие систем строго разграничено по функциональным этапам:

Этап процесса	Задействованный механизм
Сбор первичных данных	Запрос в Цифровой профиль ЕСИА через СМЭВ 4
Биометрическая верификация	Сопоставление слепков лица и голоса с ЕБС
Первичный комплаенс-скоринг	Запрос риск-статуса контрагента в Платформе ЗСК
Принятие решения об онбординге	Внутренний Due Diligence и сопоставление данных

Эффективность и системные ограничения

Функционирование платформы ЗСК позволило отнести 97,1% российского бизнеса к категории низкого риска, что радикально сократило объем избыточных запросов документов.

Главным ограничением модели остается дублирование проверок: банк законодательно лишен права использовать данные ЗСК или СМЭВ как единственный стопроцентный источник истины. Кредитная организация обязана проводить независимую внутреннюю проверку.

При возникновении технических расхождений между государственными реестрами и реальными транзакциями банк руководствуется собственным консервативным анализом, что заставляет корпорации заново доказывать свою легитимность комплаенс-службам каждого банка отдельно.

Перспективы развития (2026–2028): Дальнейший вектор эволюции российской системы направлен на полную интеграцию процедур KYC в быстрорастущий рынок цифровых финансовых активов (ЦФА) и оборот криптовалют (с обязательным комплаенс-контролем участников с 1 июля 2026 года). Планируется полный переход всех участников взаимодействия с госсистемами на стандартизированные протоколы OpenID Connect.

Важнейшим направлением выступает тесная интеграция комплаенс-профилей с развивающейся платформой Цифрового рубля Банка России. Связывание риск-профилей ЗСК со смарт-контрактами Цифрового рубля позволит автоматически одобрять и проводить транзакции в пользу добросовестных контрагентов (из «зеленой» зоны), оптимизируя оборотный капитал корпораций и исключая риски нецелевого расходования средств.

Международный опыт KYC

KYC в Индии: Архитектура «Единого окна»

Обзор регуляторной модели: Национальная система Индии демонстрирует высокий уровень нормативной гармонизации. Ключевыми законодательными актами выступают Закон о предотвращении отмывания денег (PMLA) 2002 года и Правила ведения записей (PML Rules) 2005 года. Регуляторные директивы синхронизированы между Резервным банком Индии (RBI), Регулятором рынка ценных бумаг (SEBI), Страховым надзором (IRDAI) и Пенсионным фондом (PFRDA).

К 2026 году в стране достигнута тотальная унификация комплаенс-шаблонов: правила едины для всех регулируемых организаций (RE), включая операторов виртуальных цифровых активов (VDA).

Архитектура хранения и обмена данными: Система развернута вокруг уникального государственного ядра:

- **CKYCRR (Central KYC Records Registry):** Центральный реестр записей KYC под операционным управлением государственной корпорации CERSAI.
- **Платформа CKYC 2.0:** Обновленная в начале 2026 года интеллектуальная система, полностью отказавшаяся от хранения неструктурированных PDF-документов в пользу высокоскоростного обмена машиночитаемыми данными в форматах XML и JSON через защищенные интерфейсы Open API.
- **Интеграция с India Stack:** Прямое сопряжение по API с биометрической системой Aadhaar и национальным защищенным хранилищем электронных документов DigiLocker.

Процедура идентификации и верификации: Каждому верифицированному клиенту присваивается постоянный 14-значный цифровой идентификатор — номер KIN (KYC Identifier Number). При онбординге в любом банке система проверяет наличие KIN контрагента в реестре CKYCRR.

Доступ к профилю открывается мгновенно, но строго после ввода клиентом одноразового пароля (SMS/Email OTP). Если профиль отсутствует, банк самостоятельно проводит полную надлежащую проверку (CDD), включая удаленную видеоверификацию по стандарту V-CIP (Video-Based Customer Identification Process), и обязан загрузить сформированное досье в центральный реестр в течение 7–10 дней.

Лучшие практики

- Сквозная привязка к номеру KIN и ИИ-алгоритмы нечеткой логики сопоставления имен минимизировали проблему дублирования профилей.
- Сроки онбординга сократились до 2–3 минут.
- В Индии действует уникальный принцип «ответственности последнего обновителя» (Last Uploader Liability): финансовая организация, которая последней внесла изменения или актуализировала профиль клиента, несет жесткую нормативную ответственность перед регулятором за точность и подлинность этих данных, при этом CKYCRR автоматически рассылает обновления по API всем связанным с клиентом учреждениям.

Выученные уроки

- Главным уроком миграции в 2026 году стало критическое качество «наследуемых данных» (Legacy Data), загруженных в реестр до 2017 года в устаревших графических форматах, что потребовало колоссальных ресурсов на их очистку.

KYC в Сингапуре: Межбанковский обмен

Обзор регуляторной модели и архитектуры: В рамках общенациональной стратегии Smart Nation Денежно-кредитное управление Сингапура (MAS) выстроило высокотехнологичную систему, базирующуюся на четком разграничении каналов поставки официальных ведомственных данных и межбанковского обмена комплаенс-рисками. Нормативные рамки задаются Уведомлением MAS Notice 626 (AML/CFT). Инфраструктура опирается на два технологических столпа:

- **Государственные API-шлюзы Myinfo и Myinfo Business:** Платформы под управлением правительственного агентства GovTech, агрегирующие верифицированные данные из всех министерств и ведомств в реальном времени. Сквозными ключами выступают Singpass (для физических лиц) и номер UEN (Unique Entity Number) для корпоративного сектора.
- **Межбанковская платформа COSMIC:** Развернутая регулятором MAS специализированная защищенная цифровая среда, предназначенная для обязательного шеринга комплаенс-информации между крупнейшими коммерческими банками (включая DBS, OCBC, UOB) при выявлении подозрительной активности или «красных флагов».

Лучшие практики:

При онбординге банк осуществляет автоматический запрос к Myinfo Business с цифрового согласия клиента, получая верифицированные государством сведения (структура директоров, бенефициары, финансовая отчетность).

Регулятор MAS официально закрепил за Myinfo статус «надежного и независимого источника». Это дает банкам частичный Safe Harbor — юридический иммунитет за достоверность базовых атрибутов личности: банк освобожден от сбора бумажных копий паспортов, подтверждений адресов или фотоснимков.

Myinfo Business сокращает сроки корпоративного онбординга на 80%. Однако этот иммунитет не распространяется на оценку легитимности происхождения капитала (Source of Wealth) — этот сложный блок due diligence банк обязан проводить вручную и индивидуально.

Банки также обязаны проверять клиентов через COSMIC, обходя ограничения классической банковской тайны для пресечения сетевых схем отмывания денег.

Выученные уроки

Риском сингапурской модели остается жесткая централизация ИТ-контура GovTech, превращающая его в потенциальную единую точку отказа.

KYC в ОАЭ: Национальная блокчейн-система

Обзор регуляторной модели и DLT-архитектуры: Финансовый мониторинг ОАЭ функционирует в режиме строгого соответствия стандартам FATF. Правовой фундамент и обязательный статус национальной e-KYC платформы закреплены обновленным Федеральным декрет-законом № 30 от 2024 года «О цифровой платформе Know Your Client» под эгидой Центрального банка ОАЭ (CBUAE). Внедрение платформы является ключевым элементом масштабной Программы трансформации финансовой инфраструктуры (FIT Programme).

ОАЭ стали первой в мире юрисдикцией, выстроившей национальный комплаенс-контур на базе технологии распределенного реестра (DLT / Блокчейн) в партнерстве с технологическим вендором Norbloc AB.

Процедура и новые требования 2026 года: В ОАЭ завершена тотальная ликвидация одноразовых SMS-паролей (SMS OTP) для верификации финансовых транзакций и авторизации — с 31 марта 2026 года регулятор законодательно перевел весь финансовый рынок на биометрическую аутентификацию через национальное приложение UAE Pass.

Корпоративным ключом служит налоговый номер TRN. Доступ к зашифрованным блокам данных контрагента открывается только после предоставления клиентом цифрового согласия через UAE Pass.

Обновление информации в любом регистрирующем органе (например, продление лицензии Департаментом экономического развития или администрацией Свободной экономической зоны RAKEZ) мгновенно меняет криптографический хэш в распределенном реестре. Все банки, связанные с данным клиентом, автоматически получают уведомление и актуальные сведения, что реализует на практике бесшовную модель Perpetual KYC.

Лучшие практики

Использование блокчейна гарантирует неизменность аудиторского следа, но не предоставляет банкам «безопасной гавани» — CBUAE возлагает на лицензированные финансовые учреждения (LFIs) всю полноту рисков за итоговый CDD/EDD.

Выученные уроки

Ключевыми вызовами для рынка в 2026 году стали высокая частота ложных алгоритмических блокировок (False Positives) при минимальных текстовых опечатках в реестрах СЭЗ,

Высокий финансовый барьер интеграции: стоимость развертывания и поддержки собственной ноды блокчейна для малых финтех-компаний и стартапов.

KYC в странах Скандинавии

Обзор модели и отказ от Invidem: Нормативно-правовая среда Северной Европы (Швеция, Дания, Норвегия, Финляндия) определяется Шестой директивой ЕС по борьбе с отмыванием денег (6AMLD) и регламентами Европейской службы финансового мониторинга (AMLA).

Скандинавский регион продемонстрировал важнейший исторический урок: масштабный проект создания единой централизованной межбанковской KYC-утилиты (проект Invidem, инициированный крупнейшими банками Nordea, SEB, Swedbank) к 2026 году официально признан полностью неэффективным и закрыт.

Попытка частного консорциума монополизировать сбор KYC-данных привела к чрезмерному росту издержек, регуляторным спорам и жесткому сопротивлению корпоративных клиентов.

В результате Скандинавия сделала выбор в пользу гибридной децентрализованной API-оркестрации, где базовым фундаментом выступают развитые национальные системы e-ID (BankID в Швеции и Норвегии, MitID в Дании).

Технологические особенности и EUDI Wallet: К концу 2026 года регион осуществляет полномасштабное внедрение Европейского кошелька цифровой идентификации (EUDI Wallet).

Лучшие практики

Скандинавские финансовые институты стали лидерами в практическом применении криптографических протоколов доказательства с нулевым разглашением (Zero-Knowledge Proofs, ZK-proofs). Данная технология позволяет банкам математически подтверждать комплаенс-статус контрагента или бенефициара (например, факт совершеннолетия, налоговое резидентство, непревышение лимитов транзакций) без фактической передачи и трансграничного сохранения исходных конфиденциальных персональных данных, радикально снижая риски утечек.

Выученные уроки

Однако децентрализация сохраняет проблему дублирования проверок: концепция Safe Harbor отсутствует, шлюзы e-ID не несут ответственности за ошибки, а процедуры углубленного анализа (EDD) выстраиваются каждым банком обособленно. При смене финансовой организации корпоративный клиент вынужден проходить EDD-комплаенс заново.

Сравнение архитектур KYC

Россия	Индия	Сингапур
Центральный узел системы		
Государственные платформы: Платформа ЗСК, ЕСИА, ЕБС, ГИС «Антифрод»	Центральный реестр CKYCRR (под операционным управлением CERSAI)	Раздельные платформы: Myinfo (GovTech) и среда COSMIC (MAS)
Технологический базис		
Реляционные базы данных, шина СМЭВ 4, биометрические векторы	Централизованный ИТ-хаб, Open API, обмен данными в XML/JSON	Ведомственные правительственные API-шлюзы, межбанковский шеринг
Сквозной идентификатор		
ИНН / ОГРН для бизнеса, СНИЛС / Паспорт для физических лиц	Уникальный 14-значный номер KIN, привязка к Aadhaar и PAN	Номер UEN для юридических лиц, профиль Singpass для граждан
Юридический статус		
Частичный (законодательная защита банков от гражданских исков по ЗСК)	Полностью отсутствует (вся полнота фидуциарного риска лежит на банке)	Ограниченный (иммунитет исключительно на верифицированные атрибуты Myinfo)
Ключевой операционный эффект		
Минимизация сомнительных операций (-19%), разгрузка «зеленой» зоны риска	Онбординг за 2-3 минуты, автоматический межбанковский шеринг через KIN	Сокращение сроков онбординга на 80%, преодоление банковской тайны в COSMIC

ОАЭ	Скандинавия
Центральный узел системы	
Единая блокчейн-платформа UAE KYC Blockchain Platform (CBUAE)	Отсутствует. Распределенные e-ID и общеевропейский EUDI Wallet
Технологический базис	
Технология распределенного реестра (DLT / Блокчейн), смарт-контракты	Децентрализованная API-оркестрация, криптография ZK-proofs
Сквозной идентификатор	
UAE Pass (биометрический ID), налоговый номер TRN бизнеса	Национальные цифровые ID (BankID, MitID), номера CVR / VAT
Юридический статус	
Полностью отсутствует (платформа гарантирует только доставку данных)	Полностью отсутствует (ИТ-провайдеры шлюзов не несут ответственности)
Ключевой операционный эффект	
Автоматический Perpetual KYC, отказ от SMS OTP в пользу биометрии	Максимальный уровень конфиденциальности данных без их избыточного накопления

Суммируем положительный опыт

Изучение глобальных KYC-практик позволяет выделить наиболее эффективные технологические и организационные решения, заслуживающие имплементации при развитии процедур KYC в Российской Федерации:

- **Применение технологий распределенного реестра (DLT):** Блокчейн-архитектура (опыт ОАЭ) доказывает свою незаменимость для реализации концепции Perpetual KYC. Мгновенное обновление хэш-функций при изменении данных в любом ведомстве исключает задержки актуализации и защищает информацию от несанкционированных манипуляций.
- **Криптография доказательств с нулевым разглашением (Zero-Knowledge Proofs):** Использование ZK-proofs (скандинавский опыт) позволяет подтверждать необходимые комплаенс-параметры контрагентов и бенефициаров без передачи и накопления избыточных персональных или коммерческих данных.
- **Законодательное закрепление статуса «Надежного источника»:** Признание государственных реестров (сингапурский кейс Myinfo) официальной точкой истины освобождает финансовые организации от рутинного бумажного документооборота при верификации базовых атрибутов.
- **Организационная модель «Последнего обновителя»:** Механизм делегирования комплаенс-подотчетности (индийский опыт CKYC 2.0) стимулирует участников рынка поддерживать актуальность баз данных: банк, обновивший досье клиента, гарантирует его точность для остальных институтов.
- **Управление через Специализированную компанию:** Создание независимого, жестко контролируемого государством оператора инфраструктуры (как CERSAI в Индии) гарантирует высокое качество очистки, дедупликации данных и бесперебойность сервисов.

Суммарные риски и выученные уроки

Анализ ошибок и ограничений международных моделей подсвечивает критические риски, которые необходимо превентивно нивелировать в отечественной практике:

- **Проблема «Наследуемых данных» (Legacy Data):** Отсутствие жестких стандартов очистки старых архивных баз при миграции на новые платформы приводит к лавинообразному накоплению технических ошибок и сбоев скоринга (кейс Индии).
- **Рост алгоритмических ложных срабатываний (False Positives):** Повышение чувствительности автоматизированных ИИ-систем комплаенс-контроля неизбежно оборачивается необоснованными блокировками транзакций из-за минимальных опечаток (кейс ОАЭ). Требуются быстрые "человекоцентричные" механизмы реабилитации.
- **Высокие финансовые барьеры для малого бизнеса (SME):** Чрезмерно высокая стоимость прямой технологической интеграции (покупка нод блокчейна, развертывание сложных шифровальных шлюзов) способна заблокировать развитие инновационных финтех-стартапов и МСП.
- **Единая точка отказа (Single Point of Failure):** Тотальная централизация верификационных сервисов в одном ИТ-контуре создает угрозу парализации онбординга и расчетов во всем финансовом секторе при любом масштабном техническом сбое или кибератаке на госоператора.
- **Крах сугубо частных межбанковских инициатив:** Скандинавский опыт закрытия проекта Invidem доказывает, что комплаенс-платформы, инициированные исключительно консорциумом коммерческих банков без прямой ресурсной и нормативной поддержки государства, обречены на неудачу из-за конфликта интересов и дефицита правоспособности.

Распределение ответственности

Ключевым правовым выводом исследования является неизменная регуляторная константа: **в мировой практике не зафиксировано ни одного прецедента, когда национальный регулятор согласился бы полностью освободить коммерческий банк от ответственности за онбординг или обслуживание нелегитимного контрагента**.

Централизованные ИТ-системы, государственные платформы и реестры расцениваются надзорными органами исключительно как качественные инструменты автоматизации, но они никогда не предоставляют финансовым институтам абсолютную правовую «безопасную гавань» (Safe Harbor) от AML-санкций.

При обнаружении любых критических расхождений между транзакционной активностью и данными реестров, банк обязан полагаться на результаты собственного углубленного Due Diligence.

Вместе с тем, опыт ОАЭ и Индии демонстрирует эффективный правовой подход к разделению зон ответственности: оператор централизованной платформы несет юридическую и материальную ответственность за технологическую точность, неизменность и безопасность доставки данных из первоисточников, в то время как фидуциарная ответственность за итоговую оценку риск-профиля клиента и принятие его на обслуживание безоговорочно остается на финансовой организации.

Такой баланс защищает банки от штрафов за технические сбои госсистем, сохраняя за ними функцию финального комплаенс-фильтра.

Шаги развития KYC в России

На основе синтеза верифицированного международного опыта и специфики отечественного регулирования, Ассоциация КорпФинТех предлагает пять стратегических шагов по развитию национальной комплаенс-инфраструктуры:

1. Учреждение отдельного института (организации), оператора единого решения для сбора, хранения и обработки данных.
2. Проработка всесторонней концепции решения с учетом передовых международных практик и потребностей участников российского финансового рынка.
3. Закрепление юридической ответственности за качество и своевременность предоставляемых данных для всех сторон процесса. Приведение законодательной базы в соответствие с потребностями цифрового развития комплаенс-процедур.
4. Подготовка детального задания на разработку решения.
5. Подготовка (повышение качества) исторических данных к использованию в решении.
6. Разработка решения и развертывание его на суверенной инфраструктуре.
7. Развертывание инфраструктуры для запуска решения.
8. Проведение масштабирования решения на все организации и финансовые институты на территории Российской Федерации и дружественных стран.

Эталон процедуры KYC

Ассоциация КорпФинТех

Чтобы получить отправную точку для сравнения мы объединили опыт разных стран в эталонную картину, объединяющую передовые практики

Функциональность ИТ платформы

- Консолидация полной информации о компаниях, необходимой для проведения финансовыми организациями процедуры KYC.
- Обработка информации с целью повышения ее качества (проверка технических ошибок и опечаток, дедупликация, выявление факторов, повышающих риски и т.д.).
- Ограничение передаваемой информации необходимым минимумом, за счет настройки на стороне владельца профайла.
- Немедленное уведомление заинтересованных лиц, имеющих права доступа, к информации о произошедших в профайле изменениях.
- Обеспечение аудиторского следа всех изменений в профайле
- Обеспечение доступа к информации в профайле только с явного разрешения собственника профайла (за исключением случаев предусмотренных законодательством)
- Возможность и обязанность для финансовых организаций запрашивать обновление профайла контрагента, в случае выявления расхождений, выявленных в результате проверки.
- Хранение всех данных в машиночитаемом формате.
- Возможность мгновенного проведения онбординга добросовестных клиентов.

Регулирование

- Юридическая ответственность источника, вносящего или предоставляющего информацию за ее достоверность и актуальность на момент внесения.
- Юридическая ответственность владельца ИТ-платформы за ошибки при обработке полученных данных.
- Юридическая ответственность финансовой организации за принятие решения о работе с контрагентом на основании полученной информации. Некорректная информация, полученная из любых источников, не может быть основанием для снятия ответственности с финансовой организации за ошибки, допущенные при проведении процедуры KYC.

Стоимость

- Доступная стоимость использования платформы для всех участников финансового рынка.

Безопасность

- Шифрование данных с высоким уровнем криптографической защиты.

Высокая степень защиты хранимых данных от утечек, потерь и неправомерного изменения

Использованные источники

1. Данные Центрального банка РФ по работе платформы «Знай своего клиента» (ЗСК): https://www.cbr.ru/press/event/?id=28444
2. Сведения о внедрении ЕБС и Федеральный закон № 572-ФЗ: https://ebs.ru/news/
3. Внедрение ГИС «Антифрод» (Закон № 41-ФЗ): https://pay.yandex.ru/blog/articles/kak-rabotaet-antifraud-v-platezhah
4. Операционные директивы CKYCRR, Индия (версия 1.5): https://www.ckycindia.in/ckyc/assets/doc/Operating_Guidelines_version1.5.pdf
5. Интеграция CKYC и государственных сервисов DigiLocker, Индия: https://hyperverge.co/blog/power-of-video-kyc-through-c-kyc-and-digilocker/
6. Директивы об управлении наследуемыми данными (Legacy Data), Индия: https://www.ckycindia.in/ckyc/assets/doc/CommuniqueManagementOfLegacyData.pdf
7. Официальный релиз MAS о запуске платформы COSMIC, Сингапур: https://www.mas.gov.sg/news/media-releases/2024/mas-launches-cosmic-platform
8. Руководящие принципы к MAS Notice 626 (Сингапур): https://www.mas.gov.sg/-/media/amld-amendments---30-june-2025/guidelines-to-mas-notice-626.pdf
9. Архитектура и спецификации Myinfo / Singpass (GovTech, Сингапур): https://www.developer.tech.gov.sg/products/categories/digital-identity/myinfo/overview
10. 10623/digital-identity-wallet-to-be-launched-in-2026

11. Релиз Центрального банка ОАЭ (CBUAE) о блокчейн-платформе KYC: https://www.centralbank.ae/en/news-and-publications/news-and-insights/press-release/cbuae-develops-e-kyc-platform-and-appoints-norbloc-ab-as-a-technology-partner-to-support-an-innovative-technology-infrastructure/
12. Федеральный декрет-закон ОАЭ № 30 от 2024 года: https://uaelegislation.gov.ae/en/legislations/2711/download
13. Переход на UAE Pass и отмена SMS OTP с 31 марта 2026 года в ОАЭ: https://facephi.com/en/cbuae-otp-deadline-uae-banks-compliance/
14. Данные о закрытии проекта межбанковской утилиты Invidem в Скандинавии: https://norbloc.com/the-sad-conclusion-of-an-effort-to-make-bank-customers-happier-and-banks-and-regulators-too/
15. Официальный релиз ЕС о внедрении Digital Identity Wallet (EUDI) к 2026 году: https://valtioneuvosto.fi/en/-/10623/digital-identity-wallet-to-be-launched-in-2026

Ассоциация КорпФинТех © 2014-2026

info@corpfintech.ru
8 495 199 88 95
www.akft.ru

Ограничение ответственности

Настоящий аналитический отчет подготовлен Ассоциацией КорпФинТех исключительно в информационных, исследовательских и дискуссионных целях. Содержащиеся в документе материалы, выводы и архитектурные концепции не являются юридической, финансовой, инвестиционной или профессиональной комплаенс-консультацией.

•**Актуальность данных:** Информация, представленная в исследовании, опирается на нормативно-правовую базу, международные стандарты (включая рекомендации FATF) и рыночную практику, актуальные на момент публикации. В связи с высокой динамикой изменения законодательства в сфере AML/CFT, Ассоциация не гарантирует абсолютную полноту или применимость данных в будущем.

•**Прогнозные заявления:** Любые форсайт-оценки, касающиеся развития технологической инфраструктуры (включая Платформу ЗСК, Цифровой рубль, трансграничные DLT-решения и биометрическую идентификацию), представляют собой экспертное мнение авторов. Реальное развитие процедур KYC может отличаться от описанных сценариев.

•**Отказ от ответственности:** Ассоциация КорпФинТех, ее участники, руководство и авторы отчета не несут ответственности за любые прямые, косвенные или репутационные убытки, понесенные физическими или юридическими лицами в результате использования данных материалов или принятия управленческих решений на их основе.

Любые действия по трансформации внутренних комплаенс-процедур или внедрению ИТ-решений финансовыми институтами должны осуществляться только после проведения независимого профильного аудита (Due Diligence) и консультаций с собственными юридическими подразделениями.