RWA FIN · RWAFIN.RU

SDK клиентской защиты

Защита клиентских приложений по ст. 45: проверка устройства до операции

SDK и серверная политика для мобильного приложения и сайта обменника цифровой валюты или депозитария. До каждой операции SDK проверяет целостность устройства и сигналы средства защиты. Вредоносное ПО выявляет средство защиты партнёра, прошедшее оценку соответствия, — его выбираем с вами на пилоте; собственной оценки соответствия у SDK нет — он связывает сигналы этого средства с операциями. Требования — ст. 45 ч. 15–17 закона № 282-ФЗ, они вступают с 01.09.2027.

Задача
С 01.09.2027 ст. 45 ч. 15–17 закона о цифровых валютах обязывает цифровой депозитарий, а также обменника, предоставляющего клиентам программные средства для сделок (ст. 18 ч. 8 п. 3), защищать мобильное приложение и официальный сайт средствами, прошедшими оценку соответствия. Нужно выявлять вредоносное ПО до операции, предлагать клиенту подключить средство защиты по согласию и отказывать в операции с заражённого устройства. Это отдельный компонент информационной безопасности с оценкой ФСТЭК / ФСБ — серверный комплаенс его не заменяет.

Решение
SDK клиентской защиты — клиентский SDK (Android, iOS, веб-агент) и серверная политика. Вместе со средством защиты партнёра, прошедшим оценку соответствия (выбор средства — на пилоте), SDK выявляет вредоносное ПО, рутинг и джейлбрейк, перехват и инструментирование, наложение, эмулятор и отладчик. Перед операцией он проверяет целостность устройства и при угрозе отказывает (ст. 45 ч. 17). Клиенту предлагается установить средство защиты, согласия и отказы пишутся в журнал (ч. 15–16). Сведения для Банка России (ч. 18) готовятся из журнала, сигналы уходят в антифрод по ст. 45, телеметрия инцидентов хранится в России (ст. 40). Каждая проверка оставляет подписанное доказательство: вердикт привязан к устройству, сумме и получателю операции, реакция на угрозу задаётся подписанной политикой, а по спорной операции выгружается выписка без персональных данных. Задачи учётного и антифрод-контура — проверка получателя и 48-часовая задержка с порогами 100 и 300 тыс. ₽ (ч. 7), приём и хранение обращений клиентов пять лет (ч. 20) — остаются у вашей организации: SDK их не подменяет, а передаёт этому контуру вердикт устройства и журнал.

Для кого

Обменник цифровой валюты
С 01.09.2027, если предоставляет клиентам программные или технические средства для сделок купли-продажи с ним (ст. 18 ч. 8 п. 3), обязан защищать приложение и сайт средством, прошедшим оценку соответствия (ст. 45 ч. 15), и отказывать в операции с заражённого устройства (ч. 17).

Цифровой депозитарий
Клиентские приложения депозитария подпадают под ст. 45 ч. 15–17. Нужны встраиваемый SDK и отчётность в Банк России (ч. 18).

Финтех-приложение для цифровой валюты
Клиентскому приложению нужна проверка целостности устройства до операции. В CryptoBox SDK помогает выполнить обязанность обменника или депозитария по ст. 45; в Cifra и Управлении Крипто-портфелем это дополнительная защита, а не требование закона.

Служба информационной безопасности обменника или депозитария
Нужны картина атак на клиентскую базу и возможность менять реакцию на угрозу без релиза приложения. SDK даёт отчёт по классам угроз, платформам и повторным инцидентам и подписанную матрицу реагирования: наблюдать, предупредить, запросить подтверждение, отказать, завершить сеанс.

Комплаенс и внутренний контроль
Нужно показать регулятору и клиенту, что контроль работает: журнал согласий и отказов с версией текста, пооперационная выписка с цепочкой хешей, дата включения нормы и подтверждение принятого регуляторного профиля. Персональных данных в журналах нет.

Антифрод-подразделение
Решение об операции принимается в вашей системе. SDK передаёт ей вердикт по стабильному контракту: целостность устройства, признаки сессии мошенника (демонстрация экрана, удалённое управление, звонок во время операции) и повторные инциденты с одного устройства.

Мобильная команда или подрядчик
Встраивает библиотеку в существующее приложение. Один формат вердикта на Android, iOS и в веб-агенте, подписанные политики подтягиваются без обновления приложения, серверная часть описана в OpenAPI.

Что входит

Выявление угроз на устройстве (RASP)

RASP — защита приложения во время работы: выявление вредоносного ПО, рутинга и джейлбрейка, перехвата, наложения, эмулятора, отладчика для приложения (Android / iOS) и сайта (веб-агент) — ст. 45 ч. 15.

Компрометация устройства видна до совершения операции.

Отказ в операции до её совершения

Отказ в операции с заражённого оборудования, уведомление о причинах и предложение другого устройства или личного присутствия (ст. 45 ч. 17).

Сделка с заражённого устройства не проходит.

Согласие клиента

Сценарий предложения установить средство защиты по согласию и журнал согласий и отказов с закреплением права в договоре (ст. 45 ч. 15–16).

Право клиента на согласие или отказ соблюдено и задокументировано.

Отчётность в Банк России

Подготовка сведений для ЦБ о выявленных случаях и попытках воздействия по форме ЦБ (ст. 45 ч. 18); направляет их ваша организация.

Сведения для Банка России не собираются вручную: они готовятся из журнала инцидентов.

Особые случаи ст. 45 ч. 23–25

В настройках задаются исключения: сделки с юрлицами и ИП (ч. 23 п. 1–2), с квалифицированными инвесторами-физлицами и нерезидентами в пределах порогов (1 млн ₽ — при переводе на адрес вне цифрового депозитария, 3 млн ₽ — в остальных случаях, п. 3), операции по торговым цифровым счетам и цифровым субсчетам к клиринговым счетам (ч. 24). Часть 25 снимает только 48-часовую задержку по ч. 7 — проверку устройства на вредоносное ПО она не отменяет.

Особые правила применяются точно, а обязательная проверка не отключается по ошибке.

Средство защиты партнёра и хранение в России

Угрозы выявляет средство защиты партнёра, прошедшее оценку соответствия ФСТЭК / ФСБ; выбор средства — на пилоте. Телеметрия хранится в России 5 лет (ст. 40), ключи доступа к адресам SDK не получает.

Защита построена на средстве, которое уже прошло оценку соответствия.

Криптографическое доказательство вердикта

Сервер не верит вердикту на слово. Устройство подписывает его собственным ключом (Ed25519 или ES256); подпись связывает вердикт с одноразовым запросом сервера, версией политики, суммой и получателем операции. На Android ключ создаётся в защищённой среде телефона и не покидает её, сервер проверяет аттестацию ключа. Повторный, просроченный, отозванный или не подходящий к операции ответ считается неподтверждённым и ведёт к отказу или повторной проверке. Ключей доступа к адресам и персональных данных в подписанных данных нет.

«Чистый» ответ нельзя подделать с заражённого устройства или использовать повторно для другой операции.

Матрица реагирования и подписанные политики

Реакция на каждый класс угрозы задаётся таблицей «сигнал × серьёзность → действие»: наблюдать, предупредить, запросить подтверждение, отказать, завершить сеанс. Таблица, пороги и веса входят в подписанный пакет политики с версией и возможностью отката; SDK принимает политику только с верной подписью, для своей организации и с действующим сроком. Неизвестный сигнал и истёкшая политика ведут к отказу. Если причин несколько, итоговый код выбирается по фиксированному приоритету: один и тот же случай всегда даёт один и тот же вердикт.

Служба ИБ меняет реакцию на новую угрозу политикой, без релиза приложения, а отказ воспроизводим при разборе.

Социнженерия и удалённый доступ в момент операции

Главный сценарий хищений у розничных клиентов — звонок «сотрудника банка» при включённой демонстрации экрана или удалённом управлении. SDK принимает от приложения признаки такой сессии (демонстрация экрана, удалённое управление, злоупотребление службами доступности, активный звонок во время операции) и по настраиваемым весам считает оценку сценария мошенника. При превышении порога действует реакция из матрицы: подтверждение или отказ с уведомлением клиента. В телеметрии — только факты-флаги, без содержимого экрана и разговора.

Операцию, которую клиент совершает под диктовку мошенника, можно остановить до отправки.

Подмена приложения, фишинг и контроль самого SDK

Проверка собственного пакета: дайджест подписи и контрольные суммы критичных файлов сравниваются с эталоном выпуска, переподписанная копия из стороннего магазина получает признак подмены. Офлайн-проверка адресов сайтов: список подозрительных доменов в политике и поиск доменов, похожих на ваш (расстояние редактирования, punycode). Подписанный «пульс» SDK (периодический сигнал о том, что SDK работает): если пульс пропал, откатился или не проходит проверку, сервер считает SDK нейтрализованным и применяет блокировку — молчание не означает «чисто».

Защиту не обойти, просто отключив её или подсунув клон приложения.

Доказательства по спорной операции

Каждое решение пишется в журнал с цепочкой хешей и привязкой к операции; разрыв цепочки обнаруживается при проверке. По спорной операции выгружается выписка: вердикт, причина, сигналы, момент и доказательство целостности цепочки — без персональных данных и ключей. Выписку выдаёт только одноразовый допуск по подписанному полномочию с ролью экспорта, на ограниченное время и для одной операции; выдача оставляет квитанцию раскрытия. Срок хранения — не менее пяти лет, досрочная очистка блокируется (ст. 40). Нарушение ч. 17 обязывает цифровой депозитарий возместить клиенту стоимость цифровых валют при наличии постановления о возбуждении уголовного дела (ч. 22): выписка помогает подтвердить, что отказ состоялся или оснований для него не было.

В споре есть проверяемый след, а сама выгрузка контролируется и не становится каналом утечки.

Аналитика угроз и повторные инциденты

Отчёт для службы ИБ: разбивка угроз по классам, платформам и серьёзности, повторяющиеся устройства, динамика к прошлому периоду, выгрузка в JSON и Markdown. Устройство опознаётся хешем с солью вашей организации: инциденты с одного телефона связываются в паттерн (ферма эмуляторов, повторные атаки), а превышение порога повторов поднимает серьёзность вплоть до отказа. Сырые атрибуты устройства не хранятся, у разных организаций хеши разные, поэтому сопоставить клиентов между ними нельзя.

Видно, что и откуда атакуют вашу клиентскую базу, а не только отчёт для регулятора.

Нормы по датам и подтверждение внедрения профиля

Нормативные параметры (даты вступления, пороги, признак услуги по ст. 18 ч. 8 п. 3, шаблон отчёта) лежат в подписанном пакете с версией, окном действия и номером отката: устройство не может включить норму раньше срока или повысить её статус. Принятие регуляторного профиля фиксируется подписанным подтверждением вашей организации с квитанцией; состояние (принят, ожидается, просрочен) выгружается файлом с контрольной суммой, подлинность проверяется служебной командой. Повтор того же подтверждения безопасен и дубль не создаёт.

Можно показать, какую версию правил и когда приняла в эксплуатацию именно ваша организация.

Платформы, API и развёртывание

Единый формат вердикта (схема device-integrity) для Android-библиотеки, Swift-пакета iOS и веб-агента; веб-агент подписывает данные операции и проверяет адрес сайта на подмену. Серверная часть — REST API с описанием OpenAPI: ключи API по организациям, ограничение частоты запросов, раздельные данные организаций, подписанные политики, консоль оператора. Развёртывание на вашей инфраструктуре в России (контейнер или системная служба), телеметрия не покидает вашу среду. В поставке — SBOM (перечень компонентов), воспроизводимая сборка библиотеки и таблица соответствия контролям OWASP MASVS-RESILIENCE: для проверки партнёрами и подготовки к оценке соответствия.

Мобильная команда встраивает один контракт, а служба ИБ получает прозрачную поставку.

Формат работы

Начинаем с пилота на данных заказчика: срок и стоимость определяем по опроснику под задачу, объём и критерии приёмки фиксируем до старта.

- **SDK + серверная политика** — для обменника / депозитария
- **Интеграционный трек** — для обменника / депозитария, которому нужно средство с оценкой соответствия

Нормативная база

- Закон о цифровых валютах № 282-ФЗ, ст. 45 ч. 15–18 — средства защиты клиентского ПО, прошедшие оценку соответствия; отказ в операции
- 184-ФЗ + ФСТЭК / ФСБ — оценка соответствия средства защиты информации (профиль в конфигурации)
- ФСТЭК Приказ 21 — меры защиты клиентской части и хранилища телеметрии
- ст. 40 — хранение телеметрии инцидентов на территории РФ 5 лет, предоставление ФСБ
- ст. 45 ч. 23–25 — исключения: юрлица и ИП, квалифицированные инвесторы-физлица и нерезиденты в пределах 1 и 3 млн ₽ (ч. 23), торговые цифровые счета и субсчета к клиринговым (ч. 24); ч. 25 снимает только задержку по ч. 7, а не проверку устройства
- 152-ФЗ + ст. 29 — маскирование ПДн, ключи доступа к адресам не захватываются
- Требования ст. 45 вступают с 01.09.2027; профиль оценки соответствия ФСТЭК / ФСБ задаётся в настройках
- Закон № 282-ФЗ, ст. 18 ч. 8 п. 3 и ст. 45 ч. 15–16 — у обменника обязанность применять средство защиты и предлагать его клиенту возникает при оказании услуги по предоставлению клиентам программных или технических средств для сделок купли-продажи цифровых валют с самим обменником; у цифрового депозитария — по факту деятельности. Признак задаётся в настройках организации
- Закон № 282-ФЗ, ст. 45 ч. 1–14 и 20 — проверка получателя и принадлежности счёта, 48-часовая задержка при переводе свыше 100 тыс. ₽ на адрес вне депозитария и свыше 300 тыс. ₽ третьим лицам (ч. 7), хранение обращений клиентов пять лет (ч. 20) выполняет учётный и антифрод-контур вашей организации; SDK передаёт ему вердикт устройства и журнал
- Закон № 282-ФЗ, ст. 45 ч. 22 — при нарушении ч. 17 цифровой депозитарий возмещает клиенту стоимость цифровых валют (при наличии постановления о возбуждении уголовного дела); пооперационная выписка с цепочкой хешей помогает подтвердить, что отказ состоялся или оснований для него не было
- Закон № 282-ФЗ, ст. 45 ч. 26 и ст. 56 ч. 3 — взаимодействие с государственной информационной системой противодействия правонарушениям (41-ФЗ) идёт в порядке, который установит Правительство; ст. 45 действует с 01.09.2027, и нормы включаются в SDK по дате вступления, не раньше

Запросить опросник для пилота: rwafin.ru/contacts.html · **Подробнее:** rwafin.ru/products/client-security-sdk.html

Актуально на 07.11.2026. Обзор не является публичной офертой и юридической консультацией; условия — в договоре.