Пакет для службы безопасности и комплаенса

Как устроена защита данных, какие меры реализованы по требованиям регулятора и где проходит граница ответственности. Сводка собрана из страниц «Безопасность», «Центр доверия» и «Политика конфиденциальности» на rwafin.ru. Чего на этих страницах нет — помечено явно.

Как читать. Описаны меры, заложенные в архитектуру продуктов RWA Fin. Это не заключение о соответствии вашей системы требованиям: аттестация и оценка соответствия вашей системы выполняются на вашей стороне. Строки на жёлтом фоне в анкете ниже — сведения, которые не опубликованы и уточняются при пилоте или предоставляются на отдельных условиях.

1. Коротко для службы безопасности

- **Данные в РФ.** Персональные данные граждан РФ хранятся и обрабатываются на серверах в России — на вашей инфраструктуре или в российском облаке (242-ФЗ, 152-ФЗ).
- **Шифрование и доступ.** Шифрование БД на уровне колонок (AES-256-GCM), ролевая модель по принципу наименьших привилегий, журналирование привилегированных действий, многофакторная аутентификация (TOTP / SMS).
- **Аудит-след.** Журнал в режиме «только добавление» с цепочкой хешей SHA-256: правка задним числом обнаруживается при проверке цепочки. Срок хранения — 5 лет (115-ФЗ).
- **Изоляция организаций.** Данные каждой организации изолированы на уровне арендатора и базы данных (RLS); ключи доступа к API хранятся только в виде хеша.
- **Проверяемая поставка.** В продуктах, где это предусмотрено: контейнер или служба на вашем сервере, перечень компонентов (SBOM), подпись образа, изолированный запуск, остановка при небезопасной конфигурации.
- **Граница ответственности.** Продукты — программное обеспечение: подпись, подачу сведений, решения об обслуживании и допуске клиентов и ответственность по закону выполняет клиент. Аттестация и оценка соответствия вашей системы — отдельный этап на вашей стороне.

2. Требование регулятора → что реализовано

Нормы и меры по таблице «Центра доверия». Формулировки сохранены без расширения.

Требование	Норма	Что реализовано в продукте
Локализация ПДн граждан РФ	242-ФЗ, 152-ФЗ	Хранение и первичная обработка ПДн — на серверах в РФ (VK Cloud, RuVDS, Yandex Cloud или инфраструктура клиента).
Защита информационных систем ПДн	ФСТЭК, Приказ 21	Разграничение доступа, шифрование БД (AES-256), контроль целостности, регистрация событий.
Безопасность финансовых организаций	ГОСТ Р 57580.1-2017, Положение ЦБ 757-П	Архитектура каждого продукта проектируется под требования к защите информации финансовых организаций.
Аудит-след операций ПОД/ФТ	115-ФЗ	Журнал «только добавление» с цепочкой SHA-256; срок хранения — 5 лет.
Обработка ЦФА и цифровой валюты	282-ФЗ, 418-ФЗ, 466-ФЗ	Квалификация инструментов, отчётность, выпуск — через ОИС из реестра Банка России.

Требование	Норма	Что реализовано в продукте
Критическая информационная инфраструктура	187-ФЗ	Меры под требования КИИ — при интеграции в контур банка или НФО; категорирование объектов проводит заказчик.
Хранение сведений о сделках и операциях	282-ФЗ ст. 39, 40	Срок хранения задаётся настройкой по роли: сведения о клиентах, сделках и адресах-идентификаторах — не менее 10 лет со дня сделки; информация хранится на территории РФ; материалы ПОД/ФТ — не менее 5 лет (115-ФЗ).
Депозитарная тайна и ключи доступа	282-ФЗ ст. 29	Ключи доступа к адресам-идентификаторам не попадают в журналы и выгрузки; запросы госорганов — только по закрытому перечню категорий, каждое раскрытие записывается; адреса показываются в маске.
Закрытость правил цифрового анализа	282-ФЗ ст. 35 ч. 6–7	Реестр правил — в отдельном закрытом хранилище с журналом доступа; версии правил хранятся и выгружаются для направления в Банк России в течение пяти рабочих дней.
Защита клиентского ПО	282-ФЗ ст. 45 ч. 15–18	Угрозы выявляет средство защиты партнёра, прошедшее оценку соответствия (выбор — на пилоте); SDK связывает его сигналы с операцией до её совершения и ведёт журнал согласий и отказов. Собственной оценки соответствия у SDK нет.
Целостность и состав поставки	ГОСТ Р 57580, ФСТЭК Приказ 21 (меры для хоста)	В продуктах, где это предусмотрено: контейнер или служба на вашем сервере, SBOM, подпись образа, изолированный запуск, остановка запуска при небезопасной конфигурации.
Изоляция данных организаций	152-ФЗ, ФСТЭК Приказ 21	Изоляция по арендатору, ключи арендатора хранятся только в виде хеша, ролевая модель; данные одной организации другой не видны.
Граница ответственности	282-ФЗ ст. 32 ч. 5, ст. 35 ч. 12	RWA Fin — разработчик ПО: не оператор информационной системы, не цифровой депозитарий, не тестирующее лицо и не поставщик услуг цифрового анализа из реестра.

3. Данные и инфраструктура

Тема	Что предусмотрено
Данные — на инфраструктуре в РФ	Развёртывание на инфраструктуре клиента или в частном облаке заказчика; ПДн граждан РФ хранятся и обрабатываются на серверах в России (242-ФЗ).
Шифрование и доступ	Шифрование БД AES-256, ролевая модель доступа, журналирование действий, маскирование ПДн в служебных журналах (152-ФЗ).
Платёжные данные (PCI-DSS v4)	Для сценариев с вводом банковской карты: PAN — токенизация на входе, в открытом виде не хранится; CVV не сохраняется в браузере и не попадает в журналы; HSM для криптоматериала — опция; предусмотрена интеграция с Vault (HashiCorp, Yandex Lockbox).
Роли и «четыре глаза»	Раздельные роли — администратор, аналитик, комплаенс-офицер, аудитор только для чтения, интеграционный сервис. Утверждение набора правил, запуск выпуска и раскрытие данных требуют подтверждения вторым сотрудником.
Воспроизводимость решений	Каждое решение хранит версию правил, исходные данные и автора; состояние восстанавливается из журнала событий, подмена записи обнаруживается при проверке цепочки хешей.
Выгрузка данных по договору	API с документацией по запросу и выгрузка ваших данных в согласованном формате; условия выгрузки при завершении договора фиксируются в договоре.
Хранение по классам данных	Матрица сроков по классам данных: 10 / 5 / 3 года; удаление — после истечения всех применимых сроков.

4. Принципы архитектуры

Принцип	Содержание
Эшелонированная защита	Многоуровневая модель ИБ по ГОСТ Р 57580: периметр, прикладная аутентификация, шифрование на уровне БД, ролевая модель, журналирование событий ИБ.
Нулевое доверие	Каждый вызов между сервисами проходит аутентификацию и авторизацию через взаимный TLS-сертификат; «доверенной внутренней сети» нет.
Контроль целостности журнала	Запись связана с предыдущей цепочкой SHA-256, режим «только добавление», хранение 5 лет по 115-ФЗ.
Наименьшие привилегии	Каждая роль и сервис получают минимально необходимый набор прав (с учётом разграничения доступа по Положению 757-П).
Криптографическая гибкость	Алгоритмы вынесены в конфигурацию, что упрощает переход на ГОСТ 34.11-2018 и ГОСТ 34.12-2018; состав криптопровайдеров, применение СКЗИ с действующими сертификатами и миграция ключей согласуются в проекте.
Прозрачность для регулятора	Файлы отчётности для Банка России, Росфинмониторинга и ФНС готовятся из единого источника аудит-следа; перечень форм и версии форматов согласуем в проекте, проверку и отправку выполняет ваша организация.

5. Граница ответственности

Где заканчивается продукт и начинается ответственность клиента по закону.

Кто	Что делает
Программа	Собирает данные, доказательства и сроки: хранит версии правил и решений, считает сроки, готовит черновики сведений и сообщений, собирает пакеты доказательств, журналирует действия с цепочкой хешей, разграничивает роли и изолирует данные организаций.
Ваша организация	Принимает решения и отвечает по закону: подписывает и подаёт сведения, принимает решения об обслуживании и допуске клиентов, направляет сообщения в Росфинмониторинг, проводит цифровой анализ и тестирование (ст. 35 ч. 12, ст. 32 ч. 5), проходит аттестацию и оценку соответствия своей системы.
RWA Fin	Разработчик программного обеспечения. Не оператор информационной системы, не цифровой депозитарий, не тестирующее лицо и не поставщик услуг цифрового анализа из реестра; регулируемые операции проводят клиенты и их партнёры, имеющие право на такую деятельность.

6. Анкета службы безопасности: ответ или пробел

Типовые вопросы банковской проверки вендора. В третьем столбце — где ответ опубликован; жёлтым выделено то, чего на сайте нет.

Вопрос	Ответ по опубликованным сведениям	Статус
Где хранятся персональные данные?	В РФ: на инфраструктуре клиента или в российском облаке (VK Cloud, RuVDS, Yandex Cloud).	Опубликовано: /security.html, /trust.html
Чем шифруются данные в БД?	AES-256-GCM на уровне колонок.	Опубликовано: /security.html
Есть ли многофакторная аутентификация?	Да: TOTP / SMS.	Опубликовано: /security.html
Как защищён обмен между сервисами?	Взаимный TLS-сертификат между сервисами.	Опубликовано: /security.html

Вопрос	Ответ по опубликованным сведениям	Статус
Что с журналами событий?	«Только добавление», цепочка SHA-256, 5 лет (115-ФЗ); ПДн в журналах маскируются.	Опубликовано: /security.html, /trust.html
Как разделены роли?	Пять ролей; критичные действия — с подтверждением вторым сотрудником. Матрица ролей — в пакете под NDA.	Опубликовано: /trust.html
Как изолированы клиенты?	По арендатору и на уровне БД (RLS); ключи API — только хеши, частота запросов ограничена.	Опубликовано: /security.html
Состав поставки и подпись образа?	SBOM и подпись образа — в продуктах, где это предусмотрено. Перечень и порядок проверки — под NDA.	Опубликовано: /trust.html
Резервное копирование и восстановление?	Порядок предоставляется в пакете под NDA. Целевые показатели восстановления (RTO/RPO) не опубликованы.	Не опубликовано — уточняется при пилоте
Независимый аудит или тест на проникновение?	Результаты независимых проверок на сайте не публикуются.	Не опубликовано — уточняется при пилоте
Сертификаты и аттестаты (ISO 27001, аттестат, сертификаты СКЗИ)?	На сайте не заявляются. Аттестация и оценка соответствия вашей системы — на вашей стороне; состав СКЗИ согласуется в проекте.	Не опубликовано — уточняется при пилоте
Порядок реагирования на инциденты ИБ и сроки уведомления?	В описании ГОСТ Р 57580 указан инцидент-менеджмент; сроки и каналы уведомления клиента не опубликованы.	Не опубликовано — уточняется при пилоте
Уровень доступности и поддержки (SLA)?	Уровень доступности и условия поддержки на сайте не опубликованы.	Не опубликовано — уточняется при пилоте
Какие обработчики ПДн привлекаются?	Реестр — в разделе 9 политики конфиденциальности (/privacy.html); он относится к обращениям через сайт и бота: Telegram FZ-LLC (ОАЭ) — сообщения в боте и уведомления о заявках; ООО «ЯНДЕКС» — аналитика посещений; хостинг-провайдер сайта (РФ); ПАО Сбербанк — GigaChat для консультанта по закону.	Опубликовано: /privacy.html
Реквизиты юридического лица?	ИНН и ОГРН предоставляются в процессе регистрации компании и по запросу для комплаенс-проверки вендора; в политике конфиденциальности сведения об операторе публикуются после государственной регистрации ООО «РВАФИН».	Не опубликовано — по запросу
Модель угроз и DPIA?	Модель угроз (ФСТЭК Приказ 21) и шаблон оценки воздействия на ПДн входят в пакет под NDA.	Не опубликовано — по запросу под NDA

7. Документы, которые предоставляются по запросу под NDA

- Архитектурная диаграмма потоков данных
- Модель угроз и меры защиты (ФСТЭК Приказ 21)
- Шаблон DPIA (оценка воздействия на ПДн)
- Матрица ролей и разграничения доступа
- Порядок резервного копирования и восстановления (непрерывность бизнеса)
- Условия экспорта данных при завершении договора
- Перечень компонентов поставки (SBOM) и порядок проверки подписи образа — для продуктов, где они предусмотрены
- Матрица границы ответственности: что делает программа и что остаётся за вашей организацией
- Матрица сроков хранения по классам данных и порядок удаления после истечения всех применимых сроков

Запрос пакета и вопросы по безопасности: **contact@rwafin.ru** (корпоративные запросы, соглашения о неразглашении, договоры на пилот) или форма на rwafin.ru/contacts.html.

Справочный материал на дату выпуска; не является гарантией соответствия, юридическим заключением или публичной офертой. Актуальные формулировки — на страницах rwafin.ru/security.html, rwafin.ru/trust.html, rwafin.ru/privacy.html.