Объявление о продлении срока конкурса

Дата: « 16 » марта 2026 года

ОАО «Керемет Банк» объявляет о продлении срока предоставления коммерческих предложений на поставку программного обеспечения Интернет-банкинга для дистанционного банковского обслуживания **до 15:00 часов 20.03.2026 года.**

1. Поставщики могут участвовать в процедуре закупок независимо от страны происхождения;

2. Для участия в запросе цен, Вам требуется предоставить коммерческое предложение на русском или кыргызском языках, предложение должно сопровождаться соответствующей спецификацией предлагаемого программного решения, стоимостью и сроком внедрения.

3. Формат обращения нарочно по указанному адресу или электронной по почте:

   Сектор закупок ОАО «Керемет Банк»
   Кыргызская Республика; 720001
   г. Бишкек, ул. Тоголок Молдо 40/4, каб. № 209
   Бегимкулов Алымкул – Заведующий сектором закупок.
   Электронная почта: tender@keremetbank.kg

4. Цена должна быть указана **KGS\USD**, с учетом:

   - всех налогов и сборов, предусмотренных законодательством Кыргызской Республики;
   - предложение должно действовать не менее 30 дней;
   - крайний срок предоставления Вашего ценового предложения **«20» марта 2026 года, 15:00 местного времени**. Заявки от участников принятые позже указанного срока рассмотрению не подлежат.

5. Необходимо указать окончательную стоимость продажи без оговорок, предпочтение будет дано участнику, соответствующему всем требованиям технической спецификации и предложившему наименьшую стоимость.

6. Необходимо предоставить свидетельство о регистрации, копию Устава, учредительного договора и решение о назначении руководителя;

7. Квалификационные требования

№	Наименование	Требования

8.1	Опыт реализации проектов	Наличие опыта внедрения систем интернет-банкинга и/или мобильного банкинга не менее 3-х лет и не менее 3-х успешно реализованных проектов.
8.2	Финансовая устойчивость	Предоставление финансовой отчетности за последний отчетный год
8.3	Налоговая задолженность	Предоставление справки об отсутствии задолженности по налогам
8.4	Регистрации компании	Предоставлении копии свидетельства о регистрации юридического лица
8.5	Руководства компании	Приказ о назначении руководителя и копия паспорт
8.6	Квалификация специалистов	Наличие квалифицированной команды для разработки и внедрения системы
8.7	Информационная безопасность	Решение должно соответствовать требованиям безопасности банковских систем
8.8	Санкционные ограничения	Компания и ее владельцы не должны находиться в санкционных списках
8.9	Гарантийные обязательства	Предоставление гарантийное техническое обслуживание не менее 12 месяцев

Предмет закупки: Программное обеспечение Интернет-банкинга для дистанционного банковского обслуживания

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Интернет/мобильный-банкинг для физических/юридических лиц

Web-интернет-банкинг, PWA-контур. Интеграции через интеграционную подсистему Банка. Антифрод и комплаенс.

Версия: 1.5.4

Документ предназначен для: Вендора/Разработчиков, Бизнес-аналитиков, Архитекторов, QA, DevOps, Project/Product Management.

Оглавление

Термины и сокращения

Термин	Определение
Web/PWA	Интернет-банкинг (Web) и PWA.
PWA	Progressive Web App - устанавливаемое веб-приложение с поддержкой offline и push.
Internal/External Gateway API	Интеграционная подсистема Банка; единая точка взаимодействия с АБС/CRM/гос. системами и др.
АБС	Автоматизированная банковская система ЦФТ-Банк (core banking).
Processing / Карточный модуль	Система процессинга карт (Элкарт и др.).
OTP	Одноразовый пароль (SMS-OTP / TOTP).
TOTP	Time-based One-Time Password (Google Authenticator и аналоги).
eKYC	Удалённая идентификация/верификация клиента (видеосессия, проверка документов).
AML/CFT	Противодействие легализации доходов/финансированию терроризма.
RBA/SCA	Risk-Based / Strong Customer Authentication - усиленная аутентификация по риску.
Open API	Внешние API по согласованию (баланс/выписки и др.).
Retail APP	Система дистанционного банковского облуживания физических лиц
ИБЮЛ	Интернет-банкинг для юридических лиц

1. Общие положения

1.1. Цели и ожидаемый результат

Цель проекта - создать современный digital-канал Банка (Web-интернет-банкинг + PWA-контур), который обеспечивает полный набор розничных и корпоративных банковских операций, устойчив к санкционным рискам (в т.ч. недоступности магазинов приложений), соответствует требованиям регулятора и реализует высокий уровень UX, безопасности и наблюдаемости.

1.2. Область охвата

В документе описываются: функциональные возможности каналов (Web и PWA), серверной части (сервисы/транзакционное ядро), админ-панели, интеграций через интеграционную подсистему, требования по безопасности/антифроду/логированию, нефункциональные требования и критерии приемки.

1.3. Регуляторные требования

Реализуемые цифровые каналы дистанционного банковского обслуживания должны полностью соответствовать НПА Национального банка Кыргызской Республики и другим законодательным актам Кыргызской Республики, включая, но не ограничиваясь следующими требованиями:

- **Информационная безопасность банков** - https://www.nbkr.kg/contout.jsp?item=2145&lang=RUS&material=106193
- **Персональные данные -** https://shailoo.gov.kg/media/anarbek/2018/01/27/5_LVH1Za7.pdf
- **QR-платежи и переводы -** https://www.nbkr.kg/contout.jsp?item=106&lang=RUS&material=115144
- **Удалённое/дистанционное обслуживание (минимальные требования) -** https://www.nbkr.kg/contout.jsp?item=106&lang=RUS&material=103037
- **Удалённая идентификация и верификация (видео) -** https://www.nbkr.kg/contout.jsp?item=103&lang=RUS&material=121851
- **AML/CFT и хранение -** https://fiu.gov.kg/upload/law/82/1534304422.pdf
- **Кредитование через дистанционные каналы, «период охлаждения», контрольный звонок, доступность для ЛОВЗ -** Норматив по кредитному риску вводит определение «периода охлаждения» для онлайн-кредитов, ограничивает суммы кредитов по типу ЭП, требует минимальный период охлаждения (например, 4 часа/12 часов в зависимости от суммы) и контрольный звонок при суммах свыше порога, с учетом антифрод-профиля. Также установлены особенности договора: составление на государственном языке и при необходимости на официальном; требования к читаемости и размеру шрифта (не менее 12, и не менее 16 для клиентов с нарушением зрения), а также по запросу клиента - звуковое воспроизведение/сурдоперевод. Это напрямую диктует функциональные требования к кредитному модулю, уведомлениям, антифроду и accessibility. - https://www.nbkr.kg/contout.jsp?item=103&lang=RUS&material=125990
- **Расчет и раскрытие ЭПС (годовая эффективная процентная ставка) -** https://www.nbkr.kg/contout.jsp?item=103&lang=RUS&material=118746
- **Самозапрет на кредиты -** https://www.nbkr.kg/DOC/26012026/000000000066562.pdf

1.4. Допущения и ограничения

- Все интеграции с государственными органами и внутренними системами (АБС/CRM/Processing/AML/Black List и др.) выполняются исключительно через внутреннюю интеграционную подсистему Internal/External Gateway API.
- Авторизация/аутентификация и выдача токенов доступа организуются централизованно; клиентские каналы не имеют прямых интеграций с backend-системами в обход интеграционной подсистемы.
- Транзакционное ядро интернет-банкинга является единой точкой оркестрации финансовых операций и обеспечивает идемпотентность, аудит и согласованность статусов.
- PWA рассматривается как полноценный канал: установка «на главный экран», offline для части сценариев, уведомления через web-push и альтернативные каналы.

2. Целевая модель решения

2.1. Каналы и компоненты

Решения состоят из клиентских каналов (Web, PWA, опционально Android) и серверной платформы (API-шлюз/Back-end/микросервисы/транзакционное ядро), интегрированной с Internal/External Gateway API.

2.2. Высокоуровневая архитектура взаимодействия

Клиентские приложения обращаются к Back-end приложения. Back-end управляет сессиями, агрегацией данных и оркестрацией сценариев, а все вызовы к системам Банка/гос-сервисам выполняются через Internal/External Gateway API. Прямые вызовы из приложений к АБС/Processing/CRM запрещены.

2.3. Технические принципы

- **Безопасность по принципу «Security by Design».**
  Архитектура системы должна изначально проектироваться с учётом требований информационной безопасности и защиты финансовых операций. Доступ пользователей к системе должен осуществляться с использованием многофакторной аутентификации (MFA). Для повышения уровня безопасности должна применяться привязка устройства пользователя к учётной записи (device binding). Пользователям и системным компонентам предоставляются только те права, которые необходимы для выполнения их функций.
- Журналирование и аудит операций.
  Все финансовые операции должны иметь полный аудит выполнения. Фиксируются этапы операции (created, validated, confirmed, executing, completed, failed, reversed). Журнал должен хранить детали операции (идентификатор операции, пользователя, сумму, получателя, статус операции, технические детали выполнения). Срок хранения журналов - не менее 2 лет.
- Надежность выполнения операций и обработка повторных запросов.
  Все финансовые и сервисные операции должны быть реализованы с поддержкой идемпотентности, при которой повторное выполнение запроса не приводит к повторному выполнению операции или дублированию транзакции. Должны быть предусмотрены механизмы повторных попыток выполнения операций (retry), контроль таймаутов.
- Управление параметрами системы.
  Основные параметры функционирования системы должны настраиваться без внесения изменений в программный код. Через административный интерфейс должна обеспечиваться возможность управления лимитами операций, параметрами двухфакторной аутентификации, структурой банковских услуг, тарифными параметрами и иными настройками системы. Все изменения конфигурации должны фиксироваться в журнале аудита.
- Надёжность PWA решения.
  Решение должно поддерживать работу в формате Progressive Web Application (PWA), обеспечивать корректную работу при кратковременных потерях соединения, восстановление пользовательской сессии и возможность централизованного обновления приложения.

- Мониторинг системы.
  Должен быть реализован централизованный сбор логов, метрик производительности и трассировки выполнения операций.

3. Дорожная карта реализации RETAIL APP

В настоящем разделе отображена общая сводная информация по ожидаемому процессу реализации и запуска цифрового канала ДБО с различным набором функционала.

3.1. Release 0 (R0) – Информационный банкинг (1 месяц)

Цель - запуск минимально жизнеспособной версии приложения (MVP) с возможностью просмотра информации по счетам и продуктам клиента. **ВАЖНО** из релиза строго исключены любые переводы/платежи/оплата услуг; выпуск/перевыпуск карт, изменение лимитов; онлайн eKYC и др., включены только информационные сервисы.

3.1.1. Авторизация

- вход по логину/паролю
- MFA (SMS / OTP)
- управление сессиями

3.1.2. Профиль клиента

- данные клиента
- контактные данные
- смена пароля

3.1.3. Счета

- список счетов
- остатки
- валюта счета
- статус счета

3.1.4. История операций

- выписка по счету
- фильтрация операций
- поиск

3.1.5. Карты

- список карт
- статус карты
- срок действия
- последние операции

3.1.6. Уведомления

- push уведомления
- SMS уведомления

3.1.7. Административная панель

- управление пользователями
- блокировка клиентов
- просмотр логов
- управление лимитами

3.2. Release 1 (R1) – Базовые транзакции (3 месяца)

Цель - запуск основных финансовых операций.

3.2.1. Открытие в онлайне

- счета
- карты (заявка на выпуск)

3.2.2. Платежи

- переводы между своими счетами
- переводы внутри банка
- межбанковские переводы

3.2.3. Платежи за услуги

- мобильная связь
- интернет
- коммунальные услуги
- государственные услуги
- другие платежи из имеющегося каталога

3.2.4. P2P переводы

- счету по номеру карты
- по номеру телефона
- по QR

3.2.5. Шаблоны платежей

- сохранение шаблонов платежей
- повтор платежей

3.3. Release 2 (R2) – Банковские продукты (6 месяцев)

Цель – создание полноценного цифрового канала дистанционного банковского обслуживания.

3.3.1. Депозиты

- открытие депозита
- пролонгация
- закрытие

3.3.2. Кредиты

- просмотр кредитов
- график платежей
- заявки на кредит

3.3.3. Карты

- блокировка карты
- разблокировка
- изменение лимитов
- перевыпуск карты

3.3.4. eKYC

- Онлайн онбординг
- Обновление анкетных данных

3.3.5. Виртуальные активы

- Открытие кошелька виртуальных активов
- Переводы исходящие/входящие
- Получение выписок по кошельку

3.3.6. Государственные услуги

- Штрафы, счета
- «Мой дом», «Мои авто»

4. Дорожная карта реализации ИБЮЛ

В настоящем разделе отображена общая сводная информация по ожидаемому процессу реализации и запуска цифрового канала ДБО с различным набором функционала.

4.1. Release 0 (R0) – Информационный банкинг (1 месяц)

Цель - запуск минимальной версии системы интернет-банкинга для корпоративных клиентов с возможностью просмотра счетов и операций. **ВАЖНО**: из релиза строго исключены любые платежные операции, валютные операции, кассовые операции и операции торгового финансирования! Реализуются только информационные функции!

4.1.1. Авторизация

- вход по логину/паролю
- MFA (SMS / OTP / токен)
- управление сессиями

4.1.2. Профиль компании

- данные организации
- реквизиты компании
- контактные данные
- список пользователей компании

4.1.3. Пользователи и роли

- список пользователей
- роли пользователей
- просмотр прав доступа

4.1.4. Счета компании

- список счетов
- остатки по счетам
- валюта счета
- статус счета

4.1.5. История операций

- выписка по счетам
- фильтрация операций
- поиск операций
- экспорт выписки

4.1.6. Карты компании

- список корпоративных карт
- статус карты
- срок действия
- последние операции

4.1.7. Документы

- банковские выписки
- справки банка
- документы по счетам

4.1.8. Уведомления

- push уведомления
- SMS уведомления
- уведомления о событиях

4.1.9 Административная панель банка

- управление компаниями
- блокировка пользователей
- просмотр логов
- управление лимитами

4.2. Release 1 (R1) – Базовые платежи юридических лиц (3 месяца)

Цель - запуск базовых платежных операций компаний.

4.2.1 Платежные поручения

- создание платежного поручения
- редактирование платежа
- отправка платежа в банк
- просмотр статуса платежа

4.2.2 Подписание платежей

- 1-я подпись
- 2-я подпись
- маршруты согласования

4.2.3 Шаблоны платежей

- сохранение шаблонов
- повтор платежа

4.2.4 Массовые платежи

- загрузка платежных файлов
- пакетные платежи
- массовые выплаты

4.2.5 Платежи в бюджет

- налоговые платежи
- платежи в государственные органы

4.2.6 Платежи за услуги

- коммунальные услуги
- связь
- другие платежи из каталога

4.2.7 Управление пользователями

- создание пользователей
- назначение ролей
- управление правами доступа

4.3. Release 2 (R2) – Корпоративные банковские операции (6 месяцев)

Цель - полноценное дистанционное обслуживание корпоративных клиентов.

4.3.1 FX операции

- покупка валюты
- продажа валюты
- конверсия валют
- просмотр курсов

4.3.2 Кассовые операции

- заявка на получение наличных
- заявка на внесение наличных

4.3.3 Зарплатные проекты

- • загрузка зарплатных реестров
  • массовые выплаты зарплаты
  • статус обработки выплат

4.3.4 Корпоративные карты

- управление корпоративными картами
- изменение лимитов
- блокировка карт

4.3.5 Депозиты юридических лиц

- открытие депозита
- пролонгация
- закрытие

4.3.6 Кредиты юридических лиц

- просмотр кредитов
- график платежей
- заявки на кредит

4.3.7 Банковские гарантии

- заявка на выпуск гарантии
- продление гарантии
- просмотр гарантий

4.3.8 Аккредитивы

- заявка на открытие аккредитива
- изменение условий
- статус аккредитива

5. Безопасность, аутентификация и авторизация

Приоритеты: R0 (обязательно для MVP в 1 мес.), R1 (важно для релиза 2-3 мес.), R2 (для релиза 4-6 мес.).

5.1. Модель доступа и роли

R0. Системы должны поддерживать ролевую модель доступа для клиентов, операторов поддержки, администраторов (R2. и интеграционных клиентов Open API). Доступ к функциям управляется правами.
R0. Для банкинга юридических лиц должна поддерживаться корпоративная ролевая модель доступа. Минимальный набор ролей: Инициатор платежей (создание платежных документов), Подписант (подписание и подтверждение платежных документов), Наблюдатель (просмотр без права создания платежей).
R2. Роль Администратор организации (управление пользователями, ролями, лимитами, сессиями, временное делегирование права).

5.2. Клиентская аутентификация (логин/пароль + 2FA)

По следующим сценариям:

- R0. Первичный вход: логин(номер телефона) + пароль + SMS-OTP.
- R0. Ограничение попыток ввода пароля/OTP, блокировки и безопасное восстановление доступа.
- R0. Поддержка биометрии устройства реализуется через WebAuthn/passkeys (platform authenticator) в Web/PWA: после первичной настройки пользователь может входить/подтверждать действия с использованием биометрии (FaceID/TouchID/Fingerprint) как механизма, доступного на устройстве. SMS-OTP остаётся резервным фактором (fallback).
- R1. Возможность заменить SMS-OTP на TOTP (Google Authenticator) как основной второй фактор; SMS остаётся резервным фактором (fallback).
- R1. Привязка устройства (device binding) и управление активными устройствами/сессиями.

5.3. Подтверждение операций по риску (RBA/SCA)

R1. При превышении настраиваемых порогов (разовая сумма, сумма за период, количество операций, новый получатель и др.) или при срабатывании антифрод-правил система должна запрашивать подтверждение вторым фактором (2FA). Пороги и матрица действий настраиваются в админ-панели.

5.4. Безопасное хранение на устройстве

- R0. Хранение токенов/секретов на стороне клиента: для Web/PWA запрещено хранение долгоживущих access-token в localStorage/sessionStorage. Сессии реализуются через защищённые cookies (HttpOnly, Secure, SameSite=strict/lax) либо через краткоживущие токены в памяти процесса. Offline-кэш допускается только для НЕчувствительных данных (статические справочники, UI-кэш), с шифрованием в IndexedDB (WebCrypto) при необходимости.
- R0. Временные данные на устройстве шифруются; чувствительные данные (PIN/пароль) не сохраняются и очищаются из памяти после использования.
- R1. Контроли компрометации устройства/среды: в Web/PWA прямые проверки root/jailbreak/overlay недоступны как гарантируемый механизм. Вместо этого применяются

риск-сигналы (необычные устройства/браузеры, VPN/proxy, девтулзы best-effort, аномальные паттерны), привязка устройства через WebAuthn, поведенческие/антифрод-правила, а также step-up (SCA) или ограничение функций при повышенном риске.

6. Требования к Web и PWA

6.1. Требования к PWA

- R0. Installable PWA (manifest + HTTPS) с установкой «на главный экран» и полноэкранным режимом.
- R0. Offline/неустойчивая сеть: service worker, кэширование статики и «последних известных данных» для критичных экранов (например, список счетов/последние операции).
- R1. Обновление PWA без магазинов приложений, контроль версий и механизм «обязательного обновления» при критичных изменениях.

6.2. Уведомления

- R0. Web-push для PWA/браузера (где поддерживается платформой/браузером) с отдельным сценарием подписки на уведомления и управлением разрешениями.
- R0. Fallback-каналы: SMS/e-mail/Telegram/in-app inbox при недоступности web-push.
- R0. Единый центр уведомлений (in-app inbox) для Web и PWA.

6.3. Минимизация санкционно-чувствимых зависимостей

R2. Внешние SaaS-зависимости (push, crash analytics, SDK мониторинга) должны иметь резервные реализации или возможность полного отключения без потери критического функционала.

7. Функциональные требования для RETAIL APP

Приоритеты: R0 (обязательно для MVP в 1 мес.), R1 (важно для релиза 2-3 мес.), R2 (для релиза 4-6 мес.).

7.1. Онбординг и eKYC

- R0. Онлайн-регистрация клиента по номеру телефона с подтверждением SMS-OTP.
- R2. Удалённая идентификация (eKYC): видеосессия, контроль качества, обязательный кадр «лицо + документ», хранение видеозаписи и кадра в досье клиента.
- R2. Проверка актуальности документа и данных клиента; блокировка критичных операций при неактуальных KYC с предложением обновления анкеты онлайн.
- R1. Экран/центр согласий и приватности с фиксацией версии текста, времени и канала.

7.2. Счета, операции и выписки

- R0. Просмотр списка счетов и актуальных остатков.
- R0. Просмотр и выгрузка выписок/истории в PDF, XLS, CSV.
- R1. История операций с фильтрами и поиском; отображение статусов операций.
- R1. Открытие новых счетов.

7.3. Платежи и переводы

- R1. Me2Me переводы между своими счетами с учетом конвертации.
- R1. Переводы клиентам банка по телефону/счёту/карте/QR (в зависимости от данных).
- R1. Межбанковские переводы P2P (в т.ч. по карте/телефону/QR) через интеграционную подсистему.
- R1. Оплата услуг (коммунальные и партнеры) с многошаговыми формами; шаблоны и автоплатежи.
- R1. Единый поток оплаты услуг (коммунальные и партнеры): 1) Проверка (валидация/получение задолженности по введённым данным через Internal/External Gateway API) - 2) Подтверждение (отображение итоговой суммы/комиссии + SCA по правилам) - 3) Чек (квитанция с обязательными реквизитами, статусом и возможностью поделиться/скачать).
- R1. Возможность сохранять платеж как шаблон после успешной оплаты и запускать «быстрый платеж» из шаблона (1 клик - подтверждение).
- R1. Поддержка «Избранного» и «Часто используемых услуг»: система автоматически ранжирует услуги/провайдеров по частоте и недавности использования, а пользователь может закрепить (pin) избранные услуги/шаблоны на главном экране.
- R1. Предварительное раскрытие комиссии до подтверждения.
- R1. Формирование чека/квитанции с обязательными реквизитами.
- R2. Клиринг и Гросс для (с возможностью приложить PDF документы по платежу)
- R2. Международные платежи (с возможностью приложить PDF документы по платежу)

7.4. QR-платежи

- R1. Сканирование QR и формирование платежа/перевода.
- R1. Генерация собственного QR для приема переводов и оплаты.
- R1. Поддержка статусов QR-операций (создан/ожидает/оплачен/отклонён).

7.5. Карты

- R1. Просмотр баланса и реквизитов карты
- R1. Выписка и история платежей карты
- R2. Управление картой: блокировка/разблокировка, изменение PIN.
- R2. Выпуск виртуальной карты и/или заказ физической карты, отображение статуса.
- R2. Перевыпуск карты в приложении.
- R2. Управление лимитами по карте (в рамках политик банка).

7.6. Депозиты

- R2. Открытие, пополнение и закрытие депозита онлайн.
- R2. Досрочное закрытие с автоматическим перерасчетом процентов.
- R2. Калькулятор доходности.
- R2. Витрина доходности/прогнозирование.

7.7. Кредиты

- R2. Онлайн-кредит: заявка - скоринг - предодобрение - подписание - выдача.
- R2. Период охлаждения и контрольный звонок (настраиваемо).
- R2. Проверка статуса самозапрета на кредиты перед выдачей.
- R2. Кредитный калькулятор и оценка кредитного потенциала.
- R2. Управление кредитом: график погашения, остаток, досрочное погашение, напоминания, задолженность, начисленные проценты.
- R2. Справки по кредиту/оборотам с выгрузкой PDF.
- R2. Отображение предскорингового балла

7.8. Виртуальные активы

- R2. Открытие/просмотр кошелька виртуальных активов (стейблкоин).
- R2. Перевод виртуальных активов.
- R2. Пополнение кошелька виртуальных активов со своего счёта.
- R2. Пополнение кошелька виртуальных активов со внешних источников.
- R2. Формирование выписок по операциям с кошельком виртуальных активов.

7.9. Госуслуги и интеграции по авто/штрафам

- R2. Гос-сервисы включают: штрафы, авто-штрафы (ПДД), налоги/госплатежи, получение/оплату госпошлин и справок (все перечисленные сценарии) - исключительно через Internal/External Gateway API.
- R2. Поддержать полный цикл: поиск/проверка обязательств - отображение начислений/деталей - формирование платежа - подтверждение (SCA при необходимости) - получение статуса и формирование чека/квитанции.
- R2. Идентификаторы поиска (настраиваемо по типу услуги): ИНН/персональный код, номер постановления/штрафа, госномер авто, серия/номер документа, иные идентификаторы, которые возвращает гос-API через Internal/External Gateway API.
- R2. Для каждого начисления/штрафа отображать: получатель/орган, назначение, период/дата, сумма, комиссия (если есть), крайний срок, статус, уникальный идентификатор начисления.

- R2. После оплаты - обеспечить получение подтверждения от гос-сервиса (при наличии) и хранение результата в истории операций, включая исходные реквизиты и статус (Paid/Failed/Pending).
- R2. Регистрация ИП онлайн (интеграция через Internal/External Gateway API).

7.10. Коммуникации и поддержка

- R0. Курсы валют
- R0. Push-уведомления по событиям (поступления, платежи, статусы заявок) + in-app inbox + резервные каналы для PWA.
- R2. Встроенный чат/тикеты: чат, вложения, SLA, история обращений.
- R2. Механизм уведомлений об изменении тарифов не менее чем за 5 календарных дней.
- R2. Карта АТМ и ПТ Банка (онлайн изменения при перемещении банкомата, терминала)

7.11. UX-требования (минимум)

- R0. Навигация: 3-5 основных пунктов меню и быстрый доступ к частым операциям.
- R0. Главный экран: остатки/карты/последние операции/баннеры/сторис, целевая загрузка ≤ 1 секунд при нормальной сети.
- R1. Платеж: не более 3 шагов (выбор - сумма - подтверждение), минимум полей, автозаполнение из шаблонов.
- R2. Поддержка темной темы и регулировки размера шрифта и поддержка ЛОВЗ.
- R2. Главный экран содержит блок «Избранное/Шаблоны/Часто используемые» (до N элементов, N настраиваемо), позволяющий запускать быстрые платежи без поиска по дереву услуг.
- R2. Рейтинг услуг: сортировка по умолчанию учитывает персональную частоту/недавность, глобальную популярность (агрегированную статистику), а также промо-приоритеты Банка (управляются админкой).

7.12. Шаблоны, избранное, быстрые платежи и автоплатежи

- R1. Создание шаблона: после успешной операции клиент может сохранить шаблон (название, категория, провайдер, реквизиты/идентификатор, сумма по умолчанию - опционально).
- R1. Управление шаблонами: список, поиск, редактирование, удаление, перенос в «Избранное», группировка по категориям.
- R1. Быстрый платеж: запуск платежа из шаблона в один клик с обязательным экраном подтверждения (комиссия/итог/реквизиты) и SCA по правилам Банка.
- R2. Автоплатежи: настройка регулярных платежей (расписание, лимит суммы, уведомления перед списанием, пауза/отмена) с журналом исполнений.
- R2. Защита от ошибочных/дублирующих списаний: идемпотентность, предупреждение при повторной оплате одного начисления (если провайдер возвращает идентификатор начисления), защита от двойного клика.
- R2. Рейтинг услуг/провайдеров: формирование блока «Часто используемые» на основе (a) частоты, (b) недавности, (c) успешности операций; алгоритм ранжирования и веса настраиваются через админ-панель.

8. Функциональные требования для интернет-банкинга юридических лиц

Приоритеты: R0 (обязательно для MVP в 1 мес.), R1 (важно для релиза 2-3 мес.), R2 (для релиза 4-6 мес.), LATER (для релиза 7-10 мес.)

8.1. Онбординг и eKYC

- R0. Для действующих клиентов Банка по номеру телефона с подтверждением SMS-OTP.
- R0. Подключение производится в отделении Банка на основании заявления.
- R0. При первом входе пользователь подтверждает согласие с условиями использования сервиса и политикой конфиденциальности.
- R2. Онлайн онбординг.
- R2. Проверка актуальности документа и данных клиента; блокировка критичных операций при неактуальных KYC .

8.2. Счета, операции и выписки

- R0. Просмотр списка счетов/карт/кошельков виртуальных активов (стейблкоин) и актуальных остатков.
- R0. История операций с фильтрами и поиском; отображение статусов операций, группировка платежей.
- R0. Просмотр и выгрузка выписок/истории в PDF, XLS, CSV.
- R0. Просмотр счетов организации и их остатков с учетом прав пользователя и его роли.
- R1. Открытие счетов/карт/кошельков виртуальных активов (стейблкоин)

8.3. Платежи и переводы

- R1. Me2Me переводы между своими счетами с учетом конвертации с установлением и запросом договорного курса.
- R1. Переводы клиентам банка по телефону/счёту/карте.
- R1. Межбанковские переводы (в т.ч. по карте/телефону) при наличии сервиса через Internal/External Gateway API.
- R1. Оплата услуг (коммунальные и партнеры) с многошаговыми формами; шаблоны и автоплатежи.
- R1. Единый поток оплаты услуг (коммунальные и партнеры): 1) Проверка (валидация/получение задолженности по введённым данным через Internal/External Gateway API) - 2) Подтверждение (отображение итоговой суммы/комиссии + SCA по правилам) - 3) Чек (квитанция с обязательными реквизитами, статусом и возможностью поделиться/скачать).
- R1. Возможность сохранять платеж как шаблон после успешной оплаты и запускать «быстрый платеж» из шаблона (1 клик - подтверждение).
- R1. Поддержка «Избранного» и «Часто используемых услуг»: система автоматически ранжирует услуги/провайдеров по частоте и недавности использования, а пользователь может закрепить (pin) избранные услуги/шаблоны на главном экране.
- R1. Предварительное раскрытие комиссии до подтверждения.
- R1. Формирование чека/квитанции с обязательными реквизитами.

- R1. Клиринг и Гросс (при возможности приложить PDF документы по платежу)
- R1. Поддержка многошагового процесса согласования платежей (создание инициатором, подписание одним и более подписантом, просмотр статуса обработки платежа, возможность отмены платежей до подписания и до отправки на обработку).
- R2. Пакетное зачисление через 1 С.
- R2. Международные платежи (с возможностью приложить PDF документы по платежу)

8.4. Конверсионные операции

- R1. Покупка иностранной валюты за национальную валюту
- R1. Продажа иностранной валюты
- R1. Конверсия между иностранными валютами
- R1. Перевод средств между валютными счетами
- R2. Создание заявки на конверсию
- R2. Подтверждение сделки
- R2. Отмена заявки (если не исполнена)
- R2. Просмотр истории FX-операций

8.4. QR-платежи

- R1. Генерация собственного QR для приема переводов и оплаты.
- R2. Сканирование QR и формирование платежа/перевода.
- R2. Поддержка статусов QR-операций (создан/ожидает/оплачен/отклонён).

8.5. Карты

- R0. Просмотр корпоративных карт, привязанных к счетам организации
- R1. Просмотр операций по корпоративным картам сотрудников
- R2. Управление картой: блокировка/разблокировка.
- R2. Выпуск виртуальной карты и/или заказ физической карты, отображение статуса.
- R2. Перевыпуск карты в интерфейсе.
- R2. Управление лимитами по карте.

8.6. Депозиты

- R2. Открытие, пополнение и закрытие депозита онлайн.
- R2. Досрочное закрытие с автоматическим перерасчетом процентов.
- R2. Калькулятор доходности.
- R2. Витрина доходности/прогнозирование.

8.7. Кредиты

- R2. Подача заявки на кредит для юридического лица
- R2. Кредитный калькулятор и оценка кредитного потенциала.
- R2. Управление кредитом: график погашения, остаток, досрочное погашение, напоминания, задолженность, начисленные проценты.
- R2. Справки по кредиту/оборотам с выгрузкой PDF.
- R2. Отображение предскорингового балла

8.8. Виртуальные активы

- R2. Открытие/просмотр кошелька виртуальных активов (стейблкоин).
- R2. Перевод виртуальных активов.
- R2. Пополнение кошелька виртуальных активов со своего счёта.
- R2. Пополнение кошелька виртуальных активов со внешних источников.
- R2. Формирование выписок по операциям с кошельком виртуальных активов.

8.9. Банкнотные операции

- LATER. Создать заявку на получение наличных
- LATER. Создать заявку на внесение наличных
- LATER. Заказать наличные
- LATER. Заявка на инкассацию
- LATER. История кассовых заявок

8.10. Документарные операции (Торговые операции)

- LATER. Заявка на выпуск банковской гарантии
- LATER. Заявка на изменение или продление гарантии
- LATER. Заявка на открытие аккредитива
- LATER. Заявка на изменение условий аккредитива
- LATER. Получение информации о закрытии аккредитива

8.11. Госуслуги и интеграции по авто/штрафам

- R2. Гос-сервисы включают: штрафы, авто-штрафы (ПДД), налоги/госплатежи, получение/оплату госпошлин и справок (все перечисленные сценарии) - исключительно через Internal/External Gateway API.
- R2. Поддержать полный цикл: поиск/проверка обязательств - отображение начислений/деталей - формирование платежа - подтверждение (SCA при необходимости) - получение статуса и формирование чека/квитанции.
- R2. Идентификаторы поиска (настраиваемо по типу услуги): ИНН/персональный код, номер постановления/штрафа, госномер авто, серия/номер документа, иные идентификаторы, которые возвращает гос-API через Internal/External Gateway API.
- R2. Для каждого начисления/штрафа отображать: получатель/орган, назначение, период/дата, сумма, комиссия (если есть), крайний срок, статус, уникальный идентификатор начисления.
- R2. После оплаты - обеспечить получение подтверждения от гос-сервиса (при наличии) и хранение результата в истории операций, включая исходные реквизиты и статус (Paid/Failed/Pending).
- R2. Регистрация ИП онлайн (при наличии процесса и интеграции через Internal/External Gateway API).

8.12. Коммуникации и поддержка

- R0. Web Push-уведомления по событиям (поступления, платежи, статусы заявок).
- R0. Курсы валют.
- R2. Встроенный чат/тикеты: чат, вложения, SLA, история обращений.
- R2. Механизм уведомлений об изменении тарифов не менее чем за 5 календарных дней.
- R2. Карта АТМ и ПТ Банка (онлайн изменения при перемещении банкомата, терминала)

8.13. UX-требования

- R0. Главный экран: остатки на счетах/карты/последние операции, целевая загрузка ≤ 2 секунд при нормальной сети.
- R0. Отображение курсов валют
- R1. Платеж: не более 3 шагов (выбор - сумма - подтверждение), минимум полей, автозаполнение из шаблонов.
- R1. Главный экран содержит блок «Избранное/Шаблоны/Часто используемые» (до N элементов, N настраиваемо), позволяющий запускать быстрые платежи без поиска по дереву услуг.
- R2. Поддержка темной темы и регулировки размера шрифта (доступность).
- R2. Рейтинг услуг: сортировка по умолчанию учитывает персональную частоту/недавность, глобальную популярность (агрегированную статистику), а также промо-приоритеты Банка (управляются админкой).

8.14. Шаблоны, избранное, быстрые платежи и автоплатежи

- R1. Создание шаблона: после успешной операции клиент может сохранить шаблон (название, категория, провайдер, реквизиты/идентификатор, сумма по умолчанию - опционально).
- R1. Управление шаблонами: список, поиск, редактирование, удаление, перенос в «Избранное», группировка по категориям.
- R1. Быстрый платеж: запуск платежа из шаблона в один клик с обязательным экраном подтверждения (комиссия/итог/реквизиты) и SCA по правилам Банка.
- R2. Автоплатежи: настройка регулярных платежей (расписание, лимит суммы, уведомления перед списанием, пауза/отмена) с журналом исполнений.
- R2. Защита от ошибочных/дублирующих списаний: идемпотентность, предупреждение при повторной оплате одного начисления (если провайдер возвращает идентификатор начисления), защита от двойного клика.
- R2. Рейтинг услуг/провайдеров: формирование блока «Часто используемые» на основе (a) частоты, (b) недавности, (c) успешности операций; алгоритм ранжирования и веса настраиваются через админ-панель.

9. Административная панель

Админ-панель позволяет настраивать параметры цифрового канала без участия разработки, с разграничением прав и полным аудитом действий администраторов.

9.1. Каталог услуг и партнеров

- R2. Настройка подключений к поставщикам коммунальных услуг и партнерам через Internal/External Gateway API (активация/деактивация, параметры маршрутизации).
- R2. Построение и редактирование «дерева услуг»: категории - подкатегории - провайдеры - продукты.
- R2. Конструктор форм оплаты: поля, маски/валидации, подсказки, зависимые поля.
- R2. Настройка схемы провайдера: какие шаги доступны (проверка/подтверждение/чек), какие поля обязательны, какие реквизиты должны быть возвращены для чека/квитанции.
- R2. Управление отображением услуг на витрине: «избранные услуги Банка», промо-карточки, приоритеты категорий, веса ранжирования для блока «Часто используемые».
- R2. Настройка политик шаблонов/автоплатежей: разрешённость по типам услуг, лимиты, необходимость SCA при исполнении автоплатежа, уведомления до/после списания.

9.2. Лимиты и пороги подтверждения

- R2. Настройка порогов RBA/SCA: разовая сумма, сумма за период, количество операций, новый получатель и др.
- R2. Настройка пользовательских лимитов в рамках политик банка.
- R2. Управление правилами обязательного подтверждения (2FA) и сценариями отказа/удержания.

9.3. Контент и уведомления

- R1. Шаблоны уведомлений (push/SMS/e-mail/in-app) с языками (RUS/KG/EN) и версионированием.
- R1. CMS-контур баннеров/объявлений с deep-links и таргетингом.
- R1. Механизм обязательных уведомлений (например, тарифы) и подтверждение прочтения.

9.4. Антифрод и Manual Review

- R2. Управление антифрод-правилами: включение/выключение, пороги, матрица действий (allow/step-up/hold/block/manual review).
- R2. Очередь ручного разбора, фиксация решений, комментарии, SLA.

9.5. Аудит админ-действий

- R0. Все изменения в админ-панели должны логироваться: кто/когда/что изменил, значения до/после.

10. Интеграции

Приоритеты: R0 (обязательно для MVP в 1 мес.), R1 (важно для релиза 2-3 мес.), R2 (для релиза 4-6 мес.).

10.1. Общие требования

- Единый контракт: REST/JSON поверх HTTPS (или стандарт Internal/External Gateway API) с версионированием.
- Корреляция: Correlation-Id и Request-Id во всех вызовах.
- Идемпотентность: Idempotency-Key для операций, влияющих на баланс/статусы.
- Единая модель ошибок и человеко-читаемые сообщения.
- Параметризуемые таймауты/ретраи и детерминированные финальные статусы.

10.2. Логический каталог интеграций

Ниже приведён логический каталог интеграций на уровне доменов. Физические endpoint'ы, схемы запросов/ответов и кодовые справочники ошибок являются частью интерфейсных спецификаций Internal/External Gateway API. Для каждого домена обязательно фиксируются: корреляция (Correlation-Id/Request-Id), идемпотентность (Idempotency-Key) для операций списания/изменения статусов, таймауты/ретраи и финальная модель статусов.

Контур / интеграция (через Internal/External Gateway API)	Сценарии	Тип (sync/ async)	Обязательные операции	Таймауты /ретраи (настраиваемо)	Идемпотентность / статусы / примечания
Identity & Auth (Internal/External Gateway API)	SMS-OTP, подключение/смена TOTP (Google Auth)	sync	InitiateOtp, VerifyOtp, EnrollTotp, VerifyTotp,	p95 ≤ 500 мс (read), ≤ 2–3 с (challenge); ретраи только на технические ошибки	Device binding; лимиты попыток; блокировки; журнал событий безопасности
CBS/Core banking	Счета, остатки, выписки, внутренние переводы	sync + async статусы	GetAccounts, GetBalance, GetStatement, CreateTransfer, GetTransferStatus, GetCustomer GetCustomerInfo	Create: таймаут ≤ 5–10 с; ретраи с backoff; read ≤ 2 с	CreateTransfer строго по Idempotency-Key; статусы: Accepted/InProcess/ Completed/Rejected /Unknown

Card Processing	Карты, лимиты, выписки по картам, card-to-card (если доступно), блокировка/разблокировка	sync + async статусы	GetCards, GetCardLimits, SetCardLimits, GetCardStatement, CreateCardTransfer, GetStatus	Create: ≤ 5–10 с; read ≤ 2 с; ретраи по политике INTERNAL/EXTERNAL GATEWAY API	Idempotency на CreateCardTransfer/ SetCardLimits; аудит изменений лимитов
CRM	Лиды/обращения, сегменты	sync	CreateLead, GetClientFlags	≤ 2 с; ретраи ограничены	- усиленная проверка/антифрод; аудит до/после
AML / Black list screening	Проверки по клиенту/получателю/счёту, флаги риска, решения комплаенса	sync	ScreenClient, ScreenCounterparty, GetRiskFlags	≤ 2–5 с (по SLA INTERNAL/EXTERNAL GATEWAY API); ретраи ограничены	Результаты скрининга кэшируются с TTL; обязательная трассировка решения
Anti-Fraud Engine	Risk scoring по событиям входа/операций, решения allow/step-up/hold/block/manual review	sync + async (hold)	EvaluateLogin, EvaluateTransaction, GetDecision, ResolveHold	≤ 1–2 с; ретраи только при тех. сбоях	Decision обязателен перед критичными Confirm; хранить reason codes
Гос-сервисы (MVP: штрафы/авто-штрафы/налоги/справки)	Поиск начислений, проверка реквизитов, оплата, статус	sync + async статусы	Check, Confirm, GetStatus	Check ≤ 5 с; Confirm ≤ 10 с; ретраи по тех. ошибкам	Confirm строго идемпотентен; финальные статусы и чек обязательны
Коммунальные и партнерские услуги	Единый поток: 1) проверка - 2) подтверждение -	sync + async статусы	Check, Confirm, GetStatus,	Check ≤ 5 с; Confirm ≤ 10 с; ретраи по тех. ошибкам	Idempotency на Confirm; чек содержит обязательные реквизиты (админ-настройка)
Уведомления / OTP	SMS-OTP, push/in-app, e-mail; шаблоны;	async	SendOtp, VerifyOtp (через	≤ 2–5 с; ретраи с DLQ	Лимиты рассылок; защита от brute force; трейсинг

	журнал доставки		Identity), SendNotification, DeliveryStatus		end-to-end
Электронная подпись (SES/AES/QES)	Подписание договоров/заявок/поручений, проверка подписи, TSA	sync + async (статусы подписи)	PrepareDocument, Sign, Verify, GetSignStatus, Timestamp	≤ 10–30 с на подпись (по провайдеру); ретраи осторожно	Хранить сертификатную цепочку, timestamp, хэш, доказательства; реестр подписанных документов
Open API Gateway	Consent, scopes, доступ к балансам/выпискам для внешних клиентов	sync	CreateConsent, Activate/RevokeConsent, Token, GetAccounts/Balance/Statement	≤ 2 с; rate limits обязательны	OAuth2/OIDC; квоты по client_id/consent_id/IP; аудит и security events

Контур	Назначение	Через Internal/External Gateway API	Примечания
АБС	Счета, балансы, проводки, выписки, кредиты/депозиты.	Да	Через транзакционное ядро.
Processing/Карты	Карты, лимиты, PIN, токенизация.	Да	PCI-контур отдельно.
CRM	Профиль, заявки, лиды, коммуникации.	Да	Единый профиль.
AML/Black List	Проверки получателей/операций, стоп-факторы.	Да	Влияет на RBA.
Гос-сервисы	Штрафы/налоги/справки/авто-сервисы.	Да	По доступности.
SMS/Push провайдеры	OTP и уведомления.	Да	Резервирование провайдера.
Fraud-prevention system	Антифрод система	Да	Система на стадии закупки

10.3. Сквозная трассировка

- R2. Сквозной Correlation-Id от клиента до Internal/External Gateway API и обратно.

- R2. Сохранение request/response payload с маскированием чувствительных данных.
- R2. Поддержка distributed tracing (по возможности).

11. Транзакционное ядро ДБО (Transaction Core)

Приоритеты: R0 (обязательно для MVP в 1 мес.), R1 (важно для релиза 2-3 мес.), R2 (для релиза 4-6 мес.).

11.1. Назначение

Транзакционное ядро обеспечивает безопасное, идемпотентное и наблюдаемое проведение операций с АБС и карточным модулем через Internal/External Gateway API.

11.2. Статусы операции

Статус	Описание
Created	Создана и валидирована.
RiskCheck	Выполнены антифрод/AML проверки.
Confirmed	Подтверждена клиентом (2FA).
Executing	Исполняется в АБС/Processing через Internal/External Gateway API.
Succeeded	Успешно завершена, квитанция сформирована.
Failed	Отклонена с причиной.
Reversed	Компенсирована/отменена после частичного выполнения.
ManualReview	Требует ручного разбора.

11.3. Технические требования

- R1. Дедупликация и идемпотентность на уровне БД (уникальные ключи в разрезе клиента и операции).
- R1. Полный аудит и хранение технических деталей (с маскированием).
- R2. Outbox/Inbox, ретраи с backoff, DLQ/Manual Review для неразрешимых ошибок.
- R2. Сверка статусов (reconciliation) при неопределенности ответа от Internal/External Gateway API/бэкендов.

12. Open API для ИБЮЛ (баланс и выписки)

Данные раздел имеет низкий приоритет, но будет преимуществом при наличии запрашиваемого функционала

12.1. Функции

- Получение списка счетов.
- Получение баланса/доступного остатка по счету.
- Получение выписки/операций за период (пагинация, фильтры).
- Webhook о поступлении/изменении статуса операции.

12.2. Безопасность

- OAuth2/OIDC с scopes и согласиями клиента.
- mTLS и/или подписанные запросы по политике банка.
- Rate limit, квоты и мониторинг злоупотреблений.
- Полный аудит вызовов Open API.

12.3. Потребители, согласия и жизненный цикл доступа

- Потребители Open API: (а) партнерские финтех-сервисы/агрегаторы, (б) корпоративные клиенты и их учетные системы, (в) внутренние продукты Банка (если требуется единый публичный шлюз).
- Выдача доступа - только по согласиям клиента (consent) через цифровой канал Банка: клиент выбирает счет(а), период/тип данных и объем прав (scopes).
- Согласие имеет жизненный цикл: создано - активно - приостановлено - отозвано/истекло; клиент может управлять согласиями в профиле (просмотр, отзыв).
- OAuth2 Authorization Code + PKCE для клиентских сценариев; сервис-к-сервису (B2B) - client_credentials + mTLS/подпись запросов по политике.

12.4. Квоты, лимиты и эксплуатация

- Rate limiting и квоты на уровне API Gateway по client_id/consent_id/IP (настраиваемо). Минимальный профиль для MVP: лимит запросов + burst control + защита от перебора/сканирования.
- Договорная модель: тарифы/квоты (если применяется) привязываются к приложению-потребителю; поддержка мониторинга и алертов по превышению квот.
- Версионирование API и обратная совместимость: деприкации только с уведомлением и периодом миграции.
- Полный аудит: кто запрашивал данные, какие счета/периоды, какие scopes; хранение логов по правилам комплаенса.

13. Совместимость с антифрод

Антифрод-контур реализует поведенческий анализ, риск-профилирование и decisioning (allow/step-up/hold/block/manual review) в привязке к операциям и событиям безопасности. Представленные ниже пункты 11.1 и 11.2 имеют приоритет R1.

13.1. Критерии

1. Аномальная частота транзакций (резкий рост количества исходящих/входящих операций).
2. Групповая аномальная активность (рост активности группы клиентов по схожим параметрам).
3. Аномальный размер транзакций (нетипичные суммы/категории).
4. Аномальная география (IP/новое устройство/VPN/прокси).
5. Аномальное время операций (нетипичное время суток/день недели).
6. Многократные неудачные попытки входа.
7. Частая смена контактных данных перед крупными транзакциями.
8. Совпадение с известными схемами мошенничества.
9. Частые возвраты/отмены.
10. Подозрительные получатели.
11. Дробление на множество получателей.
12. Аномальные источники пополнения.
13. Частое привязывание/отвязывание карт/аккаунтов.
14. Аномальные изменения в режимах доступа (новые способы авторизации).
15. Несоответствие анкетных данных частоте/суммам операций.
16. Быстрое дробление/укрупнение с выводом в другой банк.
17. Пополнение карты разными лицами с последующим выводом.
18. Операции выше установленного корпоративного лимита.
19. Операции вне рабочего времени организации
20. Операции с новыми получателями
21. Иные критерии Банка.

13.2. Поддержка антифрод операций

- ALLOW - разрешить.
- STEP-UP - запросить 2FA/TOTP.
- HOLD - задержка и дополнительная проверка.
- BLOCK - блокировка операции/сессии.
- MANUAL REVIEW - ручной разбор.

14. Журналирование и аудит

14.1. События, подлежащие логированию

- R0. Вход/выход, смена пароля, смена факторов 2FA, привязка/отвязка устройства.
- R0. Изменения профиля (контакты, паспортные данные, согласия).
- R0. Админ-действия (изменение лимитов, правил, дерева услуг).
- R0. Интеграционные вызовы (request/response метаданные, тайминги, коды ошибок) - с маскированием чувствительных данных.
- R1. Создание/подтверждение/исполнение финансовых операций и их статусы.
- R1. События антифрода (срабатывания правил, решения, кейсы manual review).

14.2. Атрибуты журнала

- R0. Timestamp (UTC и локальная зона), тип события, уровень (INFO/WARN/ERROR), результат (success/fail), код ошибки/причина.
- R0. Идентификаторы: client_id (внутренний), username/phone (маскируется), session_id, device_id (stable per device binding), correlation_id/request_id, idempotency_key (для операций).
- R0. Атрибуты устройства/среды: модель устройства (если доступно), ОС и версия, браузер/движок, app/pwa version, язык/локаль, timezone, разрешение экрана, признаки эмулятора (best-effort).
- R0. Сетевые атрибуты: IP, ASN/провайдер (если доступно), тип сети (wifi/cell), признаки VPN/Proxy/Tor (best-effort), гео-страна/город (по политике), user agent (полный).
- R0. Атрибуты аутентификации: метод входа (пароль+SMS/TOTP/WebAuthn), факт step-up, количество попыток, результат проверки device binding, риск-скор (если применимо).
- R1. Для финансовых операций: реквизиты (маскировать PAN/PII), суммы/валюты, комиссия, получатель (идентификаторы), статусы по стадиям (инициировано/подтверждено/исполнено/отклонено), ссылки на чек/документ.

Поле	Описание
Correlation-Id / Trace-Id	Сквозная корреляция по всем сервисам и INTERNAL/EXTERNAL GATEWAY API.
Request-Id	Идемпотентный идентификатор запроса в разрезе клиента.
Client-Id / User-Id	Идентификатор клиента (и сессии).
Channel	Web / PWA / Open API.
Device info	OS, версия, модель, appVersion, browser (для PWA), deviceId/fingerprint.
Network	IP, ASN (если доступно), VPN/proxy flags, гео (если разрешено).
Operation	Тип операции, сумма/валюта, получатель (в маскированном виде).
Result	Статус, коды ошибок, latency, retry count.

14.3. Параметры хранения логов

- R0. Логи хранятся не менее 2 лет (или дольше - если срок хранения первичных данных больше).

- R2. Защита от удаления/модификации, контроль попыток отключения журналирования как инцидента.
- R2. Ежедневный мониторинг логов и реагирование на нестандартные ситуации.

15. Комплаенс блок

15.1. Персональные данные и согласия

- R0. Центр «Согласия и приватность»: хранение факта согласия, версия текста, время, канал.
- R1. Шифрование при передаче (TLS), минимизация хранения ПД на устройстве.
- R2. Возможность предоставить субъекту информацию о наличии/обработке его ПД и доступ к ним (выгрузка/просмотр).

15.2. AML/CFT и архив

- R0. Хранение клиентских досье/документов и данных по операциям не менее 5 лет после прекращения отношений/разовой операции.
- R0. Хранение сопровождающей информации по электронным переводам (отправитель/получатель) также не менее 5 лет.
- R0. Механизмы выборки/экспорта по запросам комплаенса и регулятора.

15.3. Электронная подпись

- R0. Поддержка ЭП для согласий/заявок/договоров.
- R2. Электронный реестр документов, подписанных ЭП.
- R2. Выгрузка документов пользователю и уполномоченным подразделениям.
- R2. Модель ЭП включает два уровня: (1) Простая ЭП (SES) - подтверждение юридически значимого действия через SCA (SMS-OTP/TOTP/biometric) с фиксацией доказательной базы (time, device, IP, document hash); (2) Усиленная/квалифицированная ЭП (AES/QES) - при подписании договоров/кредитных документов, если требуется законодательством/политикой Банка.
- R2. Для физических лиц (retail): подтверждение юридически значимых действий и высокорисковых операций выполняется через SCA (SMS-OTP или TOTP/Google Authenticator, при наличии - биометрия устройства). Требование SCA настраивается по порогам суммы/количества/разовой суммы и по типу операции (в админ-панели).
- R1. Для ИБЮЛ: поддержать много-подписантный процесс (инициатор + 1..N подписантов/утверждающих) в зависимости от настроек организации, прав пользователей и порогов сумм. Варианты: (а) единоличный подписант; (б) два подписанта (Подписант-1 и Подписант-2) последовательно или параллельно; (в) расширенная схема N-of-M (опционально).
- R1. Для юридических лиц должна поддерживаться настройка лимитов подписания платежей в зависимости от суммы операции и роли пользователя.
- R1. Методы подтверждения/подписания для юр. лиц: TOTP/Google Authenticator (как SCA) и/или AES/QES (квалифицированная ЭП) через провайдера. Параметры ИБЮЛ должен позволять назначать требуемый метод по типу операции и сумме (например: до порога - TOTP, выше порога - QES обязательно для одного или всех подписантов).
- R1. Параметры подписания настраивается в админ-панели: матрица «тип операции × сумма × валюта × тип клиента (ФЛ/ЮЛ) × роль/права» - требуемое число подписантов, порядок (seq/parallel), допустимые методы (SMS/TOTP/QES), время жизни заявки на подпись, правила отмены/повтора.

- R1. Состояния для корпоративных заявок/операций: Draft - PendingSignatures - PartiallySigned (если seq) - Signed - SentToProcessing - Completed/Rejected/Expired/Cancelled. Все переходы фиксируются в аудите; инициатор видит «кто/когда подписал/отклонил» и причину.
- R1. Провайдер ЭП: внешняя служба/провайдер, выбранный Банком и интегрированный через Internal/External Gateway API (cloud signing или выдача/проверка сертификатов). Подпись выполняется в защищенном контуре (HSM/Key Management) по политике ИБ.
- R1. Форматы документов и подписи (минимум): PDF/A + PAdES для договоров/квитанций; XML + XAdES для обмена с гос-сервисами; CMS/PKCS#7 + CAdES для вложенных данных. Поддержка отметки времени (TSA) и проверки валидности подписи.
- R1. Реестр подписанных документов: хранить документ, хэш, тип подписи, идентификатор сессии/consent, цепочку сертификатов, timestamp, статус проверки, а также ссылки на события аудита.
- R1. Пользовательский поток: предварительный просмотр - подтверждение согласия/подписания - получение результата - доступ к документу (скачать/поделиться) и история подписаний.

16. Нефункциональные требования (NFR)

16.1. Производительность

- R2. Расчетная нагрузка для MVP: ≥ 100 000 активных клиентов (MAU). Пиковая финансовая нагрузка: 30–100 транзакций/сек (TPS) на уровень платформы; сценарии чтения (баланс/история) должны масштабироваться минимум до 5× от TPS.
- R1. Главный экран: целевое время загрузки ≤ 2 секунд при нормальной сети и прогретом кэше.
- R1. API-латентность (p95): для чтения данных ≤ 500 мс; для критичных операций - по согласованным SLO.
- R2. Поддержка пиковых нагрузок (массовое подключение, сезонные пики); обязательное нагрузочное тестирование (2–3× от ожидаемой нагрузки).

Целевые показатели SLA/SLO (уточняются в рамках нагрузочного тестирования и пилота):

Показатель	Цель (MVP)	Примечание
Активные клиенты (MAU)	≥ 100 000	При необходимости расширяется без изменения архитектуры (горизонтальное масштабирование).
Пиковая нагрузка транзакций	20–80 TPS	Финансовые операции (платежи/переводы). Чтение - минимум 5× TPS.
Латентность API чтения (p95)	≤ 500 мс	Баланс/список счетов/история при прогретом кэше.
Латентность критичных операций (E2E)	≤ 2–3 сек	До статуса «принято/подтверждено»; финальный статус может быть асинхронным.
Доступность платформы (SLA)	≥ 99.9%/мес	Плановые окна обслуживания оговариваются отдельно.
Ошибка сервера (5xx) на критичных API	≤ 0.1%	SLO; алерты при отклонении.
RTO / RPO	≤ 30 мин / ≤ 5 мин	Для транзакционных данных и ключевых сервисов.

16.2. Доступность

- R0. PWA offline: корректная работа при нестабильной сети и кэш «последних известных данных» для ключевых экранов.
- R2. Доступность (SLA) серверной части: ≥ 99.9% в месяц (плановые окна - отдельно по регламенту). Целевой SLO: error rate ≤ 0.1% (5xx) на критичных API; RTO ≤ 30 минут, RPO ≤ 5 минут (для критичных транзакционных данных).
- R2. Graceful degradation: при недоступности части интеграций пользователь получает понятный статус и возможность повторить позже.

16.3. Безопасность

- R0. Соответствие OWASP MASVS/ASVS (как минимум базовые требования).
- R0. TLS 1.2+ (рекомендуется TLS 1.3) везде, HSTS, корректный TLS-hardening. Для Web/PWA certificate pinning не поддерживается стандартными браузерами; защита от MITM

обеспечивается через строгий TLS, HSTS, Certificate Transparency-мониторинг, WAF/Anti-Bot и обязательный WebAuthn для критичных действий.

- R0. Маскирование чувствительных данных в логах, экранах и при шеринге.
- R1. Защита от MITM/Replay: nonce/timestamp/подписи запросов для критичных операций (по согласованию).
- R2. Так как ограничения скриншотов и overlay-детектирование не могут быть гарантированно обеспечены в Web/PWA. Для защиты данных на чувствительных экранах применяются: watermark/маркировка, маскирование данных по умолчанию (show-on-hold), блок экспорта/копирования best-effort, auto-logout при уходе в фон/таймауте, анти-кликджекинг (CSP frame-ancestors), защита от XSS/инъекций (CSP, SRI, строгая политика зависимостей), а также риск-скоринг и step-up для подозрительных сценариев.

16.4. Доступность и локализация

- R0. Мультиязычность: RUS/KG/EN (минимум).
- R2. Регулировка размера шрифта (Small/Normal/Large), поддержка screen reader.
- R2. Темная тема (авто по системным настройкам).

16.5. Архитектурные требования

Ниже представлены ожидаемые подходы по архитектуре:

- База данных кластер PostgreSQL
- Используемый софт не должен иметь доп лицензии
- Использование платного софт/библиотеки по согласованию заказчика
- Все сервисы должны иметь интеграционный Health Check
- Не хранить данные/файлы в Docker
- Оркестратор K8
- Операционная система Debian
- Микросервисная архитектура с возможностью горизонтального масштабирования с путем увеличения экземпляров сервисов без влияния на создание блокировок в БД и порождения дублей
- Документация функционала, развертки, поддержки программного решения
- Список типовых ошибок и реагирование на них
- Управление системой через админ. панель
- Кэш Dragonfly (Аналог Redis)
- Очередь RabbitMQ
- Backend на .Net

17. Тестирование и критерии приемки

17.1. Виды тестирования

- Функциональное тестирование (test cases по всем R0 сценариям).
- Интеграционное тестирование с Internal/External Gateway API (контракты, таймауты, ретраи).
- Нагрузочное тестирование (в т.ч. пиковые сценарии).
- Тестирование безопасности (SAST/DAST, pentest, проверки Web/PWA, анализ зависимостей, управление уязвимостями).
- UAT с бизнес-подразделениями и протокол приемки.

17.2. DoD (Definition of Done) для релиза

- Все R0 функции реализованы и покрыты тестами.
- Документация (архитектура, контракты, инструкции эксплуатации) поставлена.
- Мониторинг/алерты настроены, runbooks подготовлены.
- Проведено нагрузочное тестирование и исправлены критические узкие места.

Проведен security review и устранены критические