

# Доступное мобильное банковское приложение

## Введение

В рамках практической работы представлены требования к доступному мобильному банковскому приложению.

В рамках практической работы требования представлены к пилотной версии приложения с ограниченным функционалом.

Ключевой особенностью текущего приложения является значительный акцент на цифровой доступности, требования к которой описаны в части “Нефункциональные требования”.

Мобильное банковское приложение разрабатывается для банка малого размера с численностью в 10000 зарегистрированных клиентов.

## Область действия

В рамках пилотной версии в приложении доступен функционал содержания и управления банковской дебетовой карты, осуществление денежных операций с дебетовой карты, управление профилем клиента.

Что система делает:

- Позволяет оформить заявку на дебетовую карту
- Позволяет осуществить вход в аккаунт клиента
- Демонстрирует историю совершенных операций с дебетовой картой
- Позволяет перевести денежные средства по номеру телефона
  - В другой банк
  - Генерирует чек совершенной операции
- Позволяет перевести денежные средства по номеру карты
- Позволяет оплатить покупку/счёт через функцию “Сканировать QR-код”
- Позволяет управлять функциями и настройками дебетовой карты
  - Позволяет заблокировать/заморозить
  - Демонстрирует реквизиты счёта
  - Позволяет установить лимиты на использование средств с баланса дебетовой карты
  - Генерирует “Реквизиты счёта”, “QR-код для пополнения”
- Позволяет управлять настройками профиля клиента
  - Позволяет установить фотографию профиля
  - Позволяет добавлять документы клиента

Что система не делает:

- Управление Кэшбэком и бонусами
- Содержание более 1 дебетовой карты
  - Содержание кредитной карты

- Содержание накопительного счёта
  - Содержание инвестиционного счёта
- Совершение операции перевода
  - “Междуд счетами”
  - “В другую страну”
  - “По реквизитам”
- Совершение операции платежа в сторонних сервисах
  - Мобильная связь
  - ЖКХ
  - Госуслуги
  - Интернет
  - ...
- Управление чатом

Выгоды/цели:

- Предоставить клиенту (конечному пользователю) доступ к удобному использованию базовых первичных функций дебетовой карты

## Определения, акронимы и сокращения

### Термины (единое понимание)

- Мобильное банковское приложение (МБА) — клиентское iOS/Android-приложение пилотной версии для управления одной дебетовой картой, переводов/оплат и профиля клиента.
- Пилотная версия — ограниченный по функционалу релиз, фокус на базовых операциях по дебетовой карте и цифровой доступности.
- Клиент — конечный пользователь банка, входящий по номеру телефона + SMS-код + PIN.
- Дебетовая карта — основной продукт пилота (не более одной карты на клиента); имеет баланс, статус (active/frozen/blocked) и реквизиты.
- Счёт (Account) — счёт, связанный с дебетовой картой (в пилоте 1:1); содержит реквизиты для пополнения/платежей.
- Операция (Operation) — транзакционное событие по карте/счёту ( списание/зачисление ) с суммой, валютой, статусом и временем; может иметь детализацию Transfer или QrPayment (взаимоисключающие).
- Перевод по телефону — перевод по номеру телефона с выбором банка получателя из списка банков, где номер зарегистрирован.
- Перевод по карте — перевод по номеру карты, если карта найдена во внешней “банковской базе” (сервис проверки).
- QR-оплата — оплата по данным из QR-кода с использованием камеры и подтверждением списания.
- Чек/квитанция (PDF) — генерируемый документ по операции; доступен предпросмотр и системное «Поделиться».
- Реквизиты счёта — набор банковских реквизитов (номер договора, БИК, ИНН и т. п.) + возможность отправить PDF.

- QR-код для пополнения — QR для пополнения счёта; может быть отправлен как PDF.
- Профиль клиента — раздел с персональными данными, фото профиля, документами и контактом поддержки.
- Документы клиента — загружаемые клиентом документы (паспорт/ИНН и др.) с добавлением до 10 фото на документ и последующей проверкой сотрудником банка.
- Блокировка карты (blocked) — статус, при котором операции недоступны; разблокировка невозможна самостоятельно (только сотрудником банка).
- Заморозка карты (frozen) — временная приостановка операций; разморозка доступна клиенту самостоятельно.
- Лимит на траты — ограничение расходов на период “неделя/месяц”, с отклонением операций при превышении.
- Цифровая доступность — требования к доступности UI/контента для пользователей, включая скринридеры и альтернативы нетекстовому контенту.

## Акронимы и сокращения

- FR (Functional Requirements) — функциональные требования, пронумерованные FR-1 … FR-62.
- PR (Performance Requirements) — требования к производительности.
- RR (Reliability Requirements) — требования к надежности/доступности/восстановлению.
- SR (Security Requirements) — требования к безопасности.
- UR (Usability Requirements) — требования к удобству использования.
- MR (Maintainability Requirements) — сопровождаемость (модульность, тесты, обработка ошибок, feature flags и т. п.).
- PRt (Portability Requirements) — портируемость (iOS/Android и версии ОС).
- AR (Accessibility Requirements) — требования цифровой доступности.
- UI (User Interface) — требования к пользовательскому интерфейсу.
- PI (Program Interfaces) — требования к программным интерфейсам/API и интеграциям.
- CI (Communication Interfaces) — требования к интерфейсам связи/сетевому взаимодействию.
- OTP — одноразовый код (в контексте SMS/OTP-провайдера и эндпоинтов /auth/otp/\*).
- PIN — 4-значный PIN-код для доступа и (отдельно) для физической карты.

## Обзор документа

1. Введение:
  - а. Область действия
  - б. Определения, акронимы и сокращения
  - с. Обзор документа
2. Общее описание
  - а. Взаимодействие с продуктом
  - б. Функции продукта

- c. Пользователи и характеристики
  - d. Окружение и ограничения
  - e. Предположения и зависимости
3. Архитектура экранов / функционал приложения: последовательное описание экранов и переходов.
  4. Функциональные требования: требования формализованы в “система должна…”, разнесены по разделам (автентификация, операции, переводы, QR, карта, лимиты, реквизиты, профиль).
  5. Нефункциональные требования:
    - a. производительность PR,
    - b. надежность RR,
    - c. безопасность SR,
    - d. удобство UR,
    - e. сопровождаемость MR,
    - f. портируемость PRt,
    - g. доступность AR.
  6. Требования к интерфейсам:
    - a. UI-гайды,
    - b. API/интеграции (PI),
    - c. Интерфейсы связи (CI).
  7. Требования к данным:
    - a. Логическая модель данных
    - b. Требования к хранению
    - c. Требование к целостности

## Общее описание

### Взаимодействие с продуктом

Мобильное банковское приложение является компонентом экосистемы банковского приложения. Экосистема состоит из следующих компонентов:

- Приложение для внутренних сотрудников банка
- Терминал для пополнения средств

### Как МБА взаимодействует с другим ПО/сервисами

#### 1) Backend банка (основной контур)

- Все вызовы — по HTTPS/TLS ≥ 1.2, JSON, единый формат ошибок и корреляции requestId/correlationId.
- Критичные операции (переводы/оплаты) идемпотентны через Idempotency-Key.

#### 2) Внешний SMS/OTP провайдер (через backend-адаптер)

- Отправка/проверка одноразовых кодов; протокол HTTPS (или SMPP у провайдера), endpoints /auth/otp/send и /auth/otp/verify.

### 3) Внешние справочники для маршрутизации

- “Телефон → банки” для переводов по номеру телефона (возвращает список банков-участников).
- “Карта → банк/валидность” (BIN/PAN) для проверки номера карты и банка-эмитента.

### 4) Платёжный оркестратор (routing layer)

- Единый сервис, который выбирает маршрут (внутрибанковский/межбанковский, пример — СБП) и приводит протоколы к единому контракту.

### 5) Сервис генерации PDF

- Формирование чека/квитанции по operationId, поддержка деградации при недоступности.

## Как МБА взаимодействует с аппаратным обеспечением

- Камера: используется для сканирования QR-кода через системные интерфейсы iOS/Android.
- Системный шаринг: передача PDF через стандартный механизм ОС (“Поделиться/Отправить”).
- Доступ к фото/камере: загрузка фото профиля и фото документов через системные диалоги (камера/галерея).

## Взаимодействие с базами данных (логика хранения)

МБА напрямую с БД не работает — только через backend. В документе описано:

- транзакционные данные (клиенты/счета/карты/операции) — реляционная БД,
- файлы (фото документов, PDF чеки, PDF реквизиты) — объектное/файловое хранилище, в БД — ссылки/метаданные.

## ФУНКЦИИ продукта

- Регистрация клиента
- Аутентификация по номеру телефона
- Подтверждение входа по SMS-коду
- Аутентификация по PIN-коду
- Выход из аккаунта
- Просмотр баланса дебетовой карты
- Просмотр последних 4 цифр номера карты
- Просмотр истории операций

- Фильтрация операций по дате
- Просмотр деталей операции
- Перевод денежных средств по номеру телефона
- Выбор банка получателя при переводе по телефону
- Перевод денежных средств по номеру карты
- Генерация чека операции
- Просмотр PDF-чека операции
- Отправка (шаринг) PDF-чека
- Сканирование QR-кода
- Оплата по QR-коду
- Управление дебетовой картой
- Блокировка дебетовой карты
- Заморозка дебетовой карты
- Разморозка дебетовой карты
- Просмотр реквизитов карты
- Установка PIN-кода для физической карты
- Установка лимита на траты по карте
- Контроль лимита и отклонение операций при превышении
- Просмотр реквизитов счёта
- Генерация PDF с реквизитами счёта
- Просмотр QR-кода для пополнения счёта
- Генерация PDF с QR-кодом пополнения
- Просмотр профиля клиента
- Добавление фотографии профиля
- Удаление фотографии профиля
- Просмотр документов клиента
- Добавление документов клиента
- Загрузка фотографий документов
- Просмотр статуса сохранения документов

## Пользователи и характеристики

Мобильное приложение направлено на использование конечным пользователем - клиентом.

## Окружение и ограничения

### Платформенное окружение

Клиентская часть (мобильное приложение):

- Платформы:
  - iOS
  - Android
- Поддерживаемые версии ОС:
  - iOS — не менее 2 последних major-версий
  - Android — не менее 3 последних major-версий

- Типы устройств:
  - смартфоны
  - планшеты
- Требования к устройствам:
  - наличие камеры (для сканирования QR-кодов),
  - поддержка системного хранилища (Keychain / Keystore),
  - поддержка системного механизма «Поделиться».

Ограничения клиентской части:

- Приложение не поддерживает веб-браузеры (нет web-версии).
- Приложение не должно работать на устройствах без камеры (QR-функционал недоступен).
- Приложение должно обеспечивать единый функционал на iOS и Android без различий в ключевых сценариях.

## Серверное окружение

Backend-система банка:

- Тип взаимодействия: клиент–сервер
- Протоколы:
  - HTTPS поверх TCP/IP
  - TLS версии не ниже 1.2
- Формат данных:
  - JSON (UTF-8)
  - даты/время — ISO 8601
- Архитектурные требования:
  - отсутствие единой точки отказа (минимум 2 экземпляра критических сервисов),
  - поддержка идемпотентности финансовых операций.

Хранилища данных:

- Реляционная база данных:
  - клиенты, счета, карты, операции, лимиты
- Объектное или файловое хранилище:
  - фотографии документов,
  - PDF-чек операций,
  - PDF-реквизиты и QR-коды

Внешние системы и сервисы (ограничения интеграций)

- SMS / OTP-провайдер (внешний)
- Справочник «телефон → банки»
- Справочник «карта → банк / валидность»
- Платёжный оркестратор (внутренний или внешний)
- Сервис генерации PDF

Ограничения:

- Все внешние интеграции должны быть доступны по защищённым каналам.
- Недоступность внешнего сервиса не должна приводить к краху приложения (контролируемая деградация).
- Генерация PDF не является критической функцией и может быть временно недоступна.

## Предположения и зависимости

### Предположения (Assumptions)

- Пользователь имеет:
  - действующий номер телефона, способный принимать SMS,
  - стабильное интернет-соединение во время выполнения операций входа, переводов и оплат.
- Пользователь использует:
  - устройство без root/jailbreak либо принимает ограничения функционала при их наличии.
- Камера устройства:
  - исправна и доступна для использования приложением.
- Пользователь:
  - корректно вводит персональные данные при регистрации,
  - несёт ответственность за сохранность своего PIN-кода.
- Возраст пользователя на момент оформления карты:
  - не менее 14 лет.
- Баланс карты:
  - не может быть отрицательным (овердрафт не предусмотрен).

### Зависимости (Dependencies)

Технические зависимости:

- Доступность backend-систем банка.
- Доступность SMS/OTP-провайдера для аутентификации.
- Корректная работа внешних справочников (телефон/карта).
- Корректная работа платёжного контура (внутрибанковские и межбанковские маршруты).
- Корректная работа сервиса генерации PDF.

Организационные зависимости:

- Проверка и подтверждение документов клиента выполняется сотрудниками банка через внутреннее приложение.
- Снятие блокировки дебетовой карты возможно только сотрудником банка, не самим клиентом.

- Пополнение счёта через QR-код предполагает наличие внешних платёжных каналов или терминалов пополнения, интегрированных с backend банка.

## Внешние факторы, влияющие на разработку

- Изменения требований регуляторов (финансовое и банковское законодательство).
- Изменения API или SLA у внешних провайдеров (SMS, платежи, справочники).
- Ограничения и изменения в политиках iOS App Store и Google Play.
- Рост нагрузки выше расчётных показателей пилотной версии.
- Требования по цифровой доступности, которые могут повлиять на UI/UX и сроки реализации.

## Детальные требования

### Архитектура экранов / функционал приложения

#### 1. Экран “Вход в приложение”

- Предлагает ввести номер телефона
  - Приложение выполняет переход на экран “Получить код с телефона”

#### 2. Экран “Получить код с телефона”

- Предлагает ввести код из смс, отправленный на указанный номер телефона
- Предлагает отправить код ещё раз через 30 секунд
- Номер телефона проверяется на наличие его в бд среди клиентов, проверяется корректность введённого кода из смс
  - Введённый код из смс указан неверно -> отображение надписи “Код из смс указан неверно, попробуйте ввести код ещё раз”
  - Введённый код из смс указан верно, клиент по указанному номеру зарегистрирован -> приложение выполняет переход на экран “Ввести PIN-код”
  - Введённый код из смс указан верно, клиент по указанному номеру не зарегистрирован -> приложение выполняет переход на экран “Стать клиентом”

#### 3. Экран “Ввести PIN-код”

- Предлагает ввести 4-х значный PIN-код
- Проверяет корректность введённого PIN-кода
  - Введённый PIN-код из смс указан неверно -> отображение некорректности в виде подсветки полей ввода красным цветом
  - Введённый PIN-код из смс указан верно -> приложение выполняет переход на раздел “Главная”
- Предлагает выйти из аккаунта
  - При нажатии на “Выйти” приложение выполняет переход на экран “Вход в приложение”

#### 4. Экран “Стать клиентом”

- a. Предлагает оформить дебетовую карту, ввести первичную информацию:
  - i. ФИО
  - ii. Электронная почта
  - iii. Дата рождения
- b. Верифицирует дату рождения
  - i. Если количество лет (тек. дата - дата рождения) < 14 лет -> отображение “Дата рождения не соответствует критериям оформления карты, клиенту должно быть более 14 лет”
  - ii. Если количество лет (тек. дата - дата рождения) > 14 лет -> приложение выполняет переход на экран “Успешно оформленная заявка”

#### 5. Экран “Успешно оформленная заявка”

- a. Отображает текст “Вы успешно оформили заявку! В течение 30 минут с вами свяжется представитель банка для уточнения деталей оформления карты.”

#### 6. Раздел “Главная”

- a. Отображает:
  - i. “Все операции” - история операций. При нажатии приложение выполняет переход на экран “Операции”
  - ii. “Перевести по телефону” - перевод средств по номеру телефона. При нажатии приложение выполняет переход на экран “Кому перевести”
  - iii. “Перевести по номеру карты” - перевод средств по номеру карты. При нажатии приложение выполняет переход на экран “По номеру карты”
  - iv. “Сканировать QR-код” - сканирование QR-код для оплаты покупки. При нажатии приложение запускает модуль камеры и открывает интерфейс сканирования QR-кода
  - v. “Дебетовая карта” - управление дебетовой карты. При нажатии приложение выполняет переход на экран “Дебетовая карта”
- b. В области элемента “Дебетовая карта” отображает баланс дебетовой карты и последние 4 цифры дебетовой карты
- c. Содержит нижнюю панель навигации между основными разделами приложения:
  - i. Раздел “Главная”
  - ii. Раздел “Мой профиль”

#### 7. Экран “Операции”

- a. Отображает список всех совершенных операций с дебетовой карты
  - i. Операции отсортированы по дате совершения операции по убыванию
  - ii. Операции сгруппированы по дням совершения операции
  - iii. В элементе “Операция” содержится информация о Получателе/Отправителе денежных средств, сумме денежных средств
- b. Доступна фильтрация по дате совершения операции

- c. При нажатии на совершенную операцию приложение выполняет переход на экран "Детали операции"
- d. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Главная"

## 8. Экран "Детали операции"

- a. Отображает:
  - i. Время и дата совершения операция
  - ii. Получатель/Отправитель денежных средств
  - iii. Сумма денежных средств
- b. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Операции"

## 9. Экран "Кому перевести"

- a. Предлагает ввести номер телефона или Имя из Контактов
  - i. По умолчанию установлен российский код страны - +7
  - ii. При нажатии на Код страны приложение выполняет переход на экран "Выберите страну"
- b. При вводе номера телефона не из Контактов приложение выполняет поиск номера телефона в бд всех номеров всех банков
  - i. Если номер телефона существует в бд -> отображает элемент "Номер телефона"
  - ii. Если номер телефона не существует в бд -> отображает пустой список
- c. Отображает список Контактов
  - i. Первым элементов в списке предлагается "Себе" - номер телефона, привязанный к аккаунту клиента
  - ii. После первого элемента элементы списка отсортированы по названию контакта по возрастанию
  - iii. В элементе "Контакт" содержится информация о названии контакта и номере телефона
- d. При нажатии на элемент "Контакт" или на элемент "Номер телефона" приложение выполняет переход на экран "Перевод по телефону"
- e. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на раздел "Главная"

## 10. Экран "Выберите страну"

- a. Предлагает ввести название страны или выбрать элемент из списка стран
- b. При вводе названия страны приложение выполняет поиск страны в бд всех стран
- c. Элементы списка стран отсортированы по названию страны по возрастанию
- d. При нажатии на элемент "Страна" приложение выполняет переход на экран "Кому перевести" и устанавливает выбранный код страны

- e. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Кому перевести"
11. Экран "Перевод по телефону"
- a. Отображает:
    - i. Баланс дебетовой карты
    - ii. Номер телефона получателя и название контакта (при наличии)
    - iii. Список банков, в которых зарегистрирован номер телефона
    - iv. Поле ввода суммы перевода
    - v. Поле ввода сообщения получателю
    - vi. Кнопка "Перевести"
  - b. Предлагает выбрать банк-получателя среди списка банков, в которых зарегистрирован номер телефона
    - i. Нажатие другого банка устанавливает банк-получателя перевода
  - c. Предлагает ввести сумму перевода в поле ввода суммы
    - i. Сумма является положительным числом с двумя знаками после запятой
    - ii. Минимальное число = 0,01. При отсутствии минимального числа суммы перевода кнопка "Перевести" становится недоступной
  - d. При введении суммы перевода приложение верифицирует указанное число с текущим балансом дебетовой карты
    - i. Если указанное число < баланса дебетовой карты -> кнопка "Перевести" становится доступной для нажатия
    - ii. Если указанное число > баланса дебетовой карты -> кнопка "Перевести" становится недоступной для нажатия
  - e. Предлагает ввести сообщение перевода в поле ввода сообщения получателю
    - i. Текст сообщения имеет ограничение в 100 символов
  - f. Предлагает осуществить перевод нажатием кнопки "Перевести"
    - i. Если кнопка "Перевести" является доступной, при нажатии осуществляется перевод, баланс дебетовой карты уменьшается на сумму перевода, приложение выполняет переход на экран "Чек перевода"
  - g. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Кому перевести"
12. Экран "Чек перевода"
- a. Отображает:
    - i. Банк-получателя
    - ii. Название контакта (при наличии)
    - iii. Номер телефона
    - iv. Сумма перевода в формате "-[сумма перевода]"
    - v. Кнопка "Квитанция"
    - vi. Кнопка "Готово"
  - b. При нажатии кнопки "Квитанция" приложение генерирует чек в формате pdf, в котором отображено:
    - i. Время и дата совершенной операции

- ii. Сумма операции
    - iii. Отправитель
    - iv. Телефон получателя
    - v. Получатель
    - vi. Подпись и печать чекодателя
  - c. Сгенерированный чек отображается как предпросмотр чека в мобильном приложении и имеет кнопку "Поделиться"
  - d. При нажатии кнопки "Поделиться" приложение инициирует механизм системного обмена файлами с ОС и передаёт pdf-файл ОС
  - e. При нажатии на кнопку "Готово" приложение выполняет переход на раздел "Главная"
  - f. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на раздел "Главная"
13. Экран "По номеру карты"
- a. Предлагает ввести номер карты
  - b. При вводе номера карты приложение выполняет поиск номера карты в бд всех номеров всех банков
    - i. Если номер карты не существует в бд -> отображает надпись "Карта не найдена", кнопка "Перевести становится недоступной"
  - c. Предлагает ввести сумму перевода в поле ввода суммы
    - i. Сумма является положительным числом с двумя знаками после запятой
    - ii. Минимальное число = 0,01. При отсутствии минимального числа суммы перевода кнопка "Перевести" становится недоступной
  - d. При введении суммы перевода приложение верифицирует указанное число с текущим балансом дебетовой карты
    - i. Если указанное число < баланса дебетовой карты -> кнопка "Перевести" становится доступной для нажатия
    - ii. Если указанное число > баланса дебетовой карты -> кнопка "Перевести" становится недоступной для нажатия
  - e. Предлагает осуществить перевод нажатием кнопки "Перевести"
    - i. Если кнопка "Перевести" является доступной, при нажатии осуществляется перевод, баланс дебетовой карты уменьшается на сумму перевода, приложение выполняет переход на экран "Чек перевода"
  - f. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на раздел "Главная"
14. Функция "Сканировать QR-код"
- a. Использует механизм камеры для сканирования QR-код
  - b. При наведении на QR-код механизм камеры сканирует QR-код и приложение осуществляет переход на экран "Оплатить QR-код"
15. Экран "Оплатить QR-код"
- a. Отображает:
    - i. Баланс дебетовой карты
    - ii. Наименование организации-получателя

- iii. Лицевой счёт получателя
  - iv. Сумма оплаты
  - v. Кнопка “Оплатить”
- b. Приложение верифицирует сумму оплаты с текущим балансом дебетовой карты
- i. Если сумма оплаты < баланса дебетовой карты -> кнопка “Оплатить” становится доступной для нажатия
  - ii. Если сумма оплаты > баланса дебетовой карты -> кнопка “Оплатить” становится недоступной для нажатия
- c. Предлагает осуществить оплату по QR-коду нажатием кнопки “Оплатить”
- i. Если кнопка “Оплатить” является доступной, при нажатии осуществляется оплата по QR-коду, баланс дебетовой карты уменьшается на сумму оплаты, приложение выполняет переход на экран “Чек перевода”
- d. Имеет визуальную кнопку “Вернуться”, отображающаяся как “стрелка влево”, при нажатии на которой приложение выполняет переход на функция “Сканировать QR-код”

## 16. Экран “Дебетовая карта”

- a. Отображает:
- i. Баланс дебетовой карты
  - ii. “Управление дебетовой карты” - управление функциями и настройками дебетовой карты. При нажатии приложение выполняет переход на экран “Функции и настройки дебетовой карты”
  - iii. “Операции по счету” - история совершенных операций по счету. При нажатии приложение выполняет переход на экран “Операции”
  - iv. “Оплатить по QR-коду” - функционал осуществления оплаты по QR-коду. При нажатии приложение открывает функцию “Сканировать QR-код”
  - v. “Перевести по номеру телефона” - функционал осуществления перевода по номеру телефона. При нажатии приложение выполняет переход на экран “Кому перевести”
  - vi. “Реквизиты счёта” - отображение реквизитов счётов. При нажатии приложение выполняет переход на экран “Реквизиты счёта”
  - vii. “QR-код для пополнение” - отображение QR-кода для пополнения счёта. При нажатии приложение выполняет переход на экран “QR-код для пополнение”
- b. Имеет визуальную кнопку “Вернуться”, отображающаяся как “стрелка влево”, при нажатии на которой приложение выполняет переход на раздел “Главная”

## 17. Экран “Функции и настройки дебетовой карты”

- a. Предлагает “Блокировать” карту
- i. При нажатии на кнопку “Блокировать” приложение выполняет блокировку карту
  - ii. Приложение “блокирует” карту - присваивает карте статус “заблокированный”

- iii. Карты со статусом “заблокированный” недоступны для осуществления операций перевода/оплаты и пополнения
    - iv. Для вывода оставшихся средств на “заблокированной” карте клиенту необходимо связаться с поддержкой банка
    - v. Перевести карту из статуса “заблокированный” в статус “доступный” невозможно самостоятельно, возможно только сотрудниками банка
  - b. Предлагает “Заморозить” карту
    - i. При нажатии на кнопку “Заморозить” приложение выполняет заморозку карту
    - ii. Приложение “замораживает” карту - присваивает карте статус “замороженный”
    - iii. Карты со статусом “замороженный” недоступны для осуществления операций перевода/оплаты и пополнения
    - iv. Перевести карту из статуса “замороженный” в статус “доступный” возможно самостоятельно нажатием “Разморозить”
  - c. Отображает реквизиты карты
    - i. Первоначально отображается последние 4 цифры карты
    - ii. Предлагает отобразить все реквизиты кнопкой “Показать”, нажатием на которую приложение выполняет отображение всех реквизитов карты
  - d. Предлагает установить PIN-код
    - i. При нажатии на кнопку “Установить PIN-код” приложение выполняет переход на экран “Ввести PIN-код”
    - ii. PIN-код устанавливается для физической карты
  - e. Предлагает установить лимит на траты с дебетовой карты:
    - i. При нажатии на кнопку “Установить лимит” приложение выполняет переход на экран “Лимит на траты”
    - f. Имеет визуальную кнопку “Вернуться”, отображающаяся как “стрелка влево”, при нажатии на которой приложение выполняет переход на раздел “Главная”
18. Экран “Лимит на траты”
- a. Предлагает установить лимит на траты через выбор временного интервала - [Месяц, Неделя], указание размера лимита в поле ввода лимита и нажатие кнопки “Готово”
  - b. При выборе временного интервала, указании размера лимита и нажатии кнопки “Готово” приложение устанавливает лимит на дебетовую карту
    - i. Приложение добавляет алгоритм подсчёта средств, задействованных в операциях перевода/оплаты/вывода средств, в установленный временной интервал. По истечению временного интервала подсчёт средств аннулируется
    - ii. Приложение добавляет проверку соответствуию лимиту в процесс осуществления операции перевода/оплаты/вывода средств
    - iii. Приложение отменяет операцию перевода/оплаты/вывода средств при попытки осуществить операцию с суммой, превышающей лимит установленного временного интервала

- c. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Функции и настройки дебетовой карты"
19. Экран "Реквизиты счёта"
- a. Отображает:
    - i. Номер договора
    - ii. Получатель
    - iii. Номер счёта
    - iv. Назначение платежа
    - v. БИК
    - vi. Банк-получатель
    - vii. Корр. счёт
    - viii. ИНН
  - b. Предлагает отправить pdf-файл с содержанием реквизитов счёта кнопкой "Отправить реквизиты"
  - c. При нажатии кнопки "Отправить реквизиты" приложение инициирует механизм системного обмена файлами с ОС и передаёт pdf-файл ОС
  - d. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Дебетовая карта"
20. Экран "QR-код для пополнение"
- a. Отображает QR-код для пополнения
    - i. При сканировании QR-кода другим устройством приложение (другого устройства) выполняет переход на экран "Оплатить QR-код", в котором указаны Наименование организации-получателя, Лицевой счёт получателя клиента
  - b. Предлагает отправить pdf-файл с содержанием QR-кода счёта кнопкой "Отправить QR-код"
  - c. При нажатии кнопки "Отправить QR-код" приложение инициирует механизм системного обмена файлами с ОС и передаёт pdf-файл ОС
  - d. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Дебетовая карта"
21. Раздел "Мой профиль"
- a. Отображает
    - i. "Имя" - имя клиента
    - ii. "Фотография" - фотография клиента. При нажатии на область фотографии приложение инициирует системный интерфейс выбора источника медиафайла с ОС: "Из библиотеки", "Камера"; и предлагает удалить фотографию
    - iii. "Документы" - панель отображения документов, содержащая элементы "Паспорт РФ", "ИНН" и кнопку "Добавить документ". При нажатии на элемент "Паспорт РФ" приложение выполняет переход на экран "Паспорт РФ". При нажатии на элемент "ИНН" приложение выполняет переход на экран "ИНН". При нажатии на кнопку "Добавить документ" приложение выполняет переход на экран "Новый документ"

- iv. "Выйти из приложения" - выполняет выход из аккаунта. При нажатии приложение выполняет переход на экран "Вход в приложение"
  - v. "Номер поддержки" - номер телефона поддержки банка.
- b. Содержит нижнюю панель навигации между основными разделами приложения:
- i. Раздел "Главная"
  - ii. Раздел "Мой профиль"
22. Экран "Паспорт РФ"
- a. Отображает:
    - i. ФИО клиента
    - ii. ФИО (латинскими буквами) клиента
    - iii. Серия и номер паспорта
    - iv. Дата рождения
    - v. Пол
    - vi. Код подразделения
    - vii. Кем выдан
    - viii. Дата выдачи
    - ix. Адрес по месту постоянной регистрации
    - x. Адрес по месту временной регистрации (при наличии)
  - b. Имеет визуальную кнопку "Вернуться", отображающуюся как "стрелка влево", при нажатии на которой приложение выполняет переход на раздел "Мой профиль"
23. Экран "ИНН"
- a. Отображает:
    - i. ИНН
    - ii. ФИО клиента
    - iii. Дата рождения
  - b. Имеет визуальную кнопку "Вернуться", отображающуюся как "стрелка влево", при нажатии на которой приложение выполняет переход на раздел "Мой профиль"
24. Экран "Новый документ"
- a. Отображает список документов:
    - i. Паспорт РФ
    - ii. Иностранный паспорт
    - iii. ИНН
  - b. При нажатии на элемент списка документа приложение выполняет переход на экран "Добавить [наименование документа]"
  - c. Имеет визуальную кнопку "Вернуться", отображающуюся как "стрелка влево", при нажатии на которой приложение выполняет переход на раздел "Мой профиль"
25. Экран "Добавить [наименование документа]"
- a. Предлагает добавить фотографию документа нажатием на кнопку "Добавить фотографию"
  - b. При нажатии на кнопку "Добавить фотографию" приложение инициирует системный интерфейс выбора источника медиафайла с ОС: "Из библиотеки", "Камера" -> при загрузки медиафайла приложение

- добавляет элемент медиафайла на экран, появляется кнопка "Сохранить"
- i. Доступно добавление до 10 элементов фотографии
  - ii. При нажатии на кнопку "Сохранить" приложение выполняет переход на экран "Фотографии [наименование документа] сохранены"
- c. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Новый документ"
26. Экран "Фотографии [наименование документа] сохранены"
- a. Отображает:
    - i. Надпись "Фотографии [наименование документа] успешно сохранены. В скором времени сотрудник банка проверит состояние фотографий [наименование документа] и [наименование документа] будет добавлено в приложение
    - ii. Кнопка "Готово". При нажатии на кнопку приложение выполняет переход на экран "Новый документ"
  - b. Имеет визуальную кнопку "Вернуться", отображающаяся как "стрелка влево", при нажатии на которой приложение выполняет переход на экран "Новый документ"

## Функциональные требования (FR)

### 1. Аутентификация и регистрация клиента

FR-1

Система должна предоставлять пользователю возможность ввести номер телефона для входа в приложение.

FR-2

Система должна отправлять одноразовый SMS-код на указанный номер телефона.

FR-3

Система должна предоставлять пользователю возможность повторно запросить SMS-код не ранее чем через 30 секунд.

FR-4

Система должна проверять корректность введённого SMS-кода.

FR-5

Система должна отображать сообщение об ошибке при вводе некорректного SMS-кода.

FR-6

Система должна определять, зарегистрирован ли клиент по введённому номеру телефона.

**FR-7**

Система должна переводить зарегистрированного клиента на экран ввода PIN-кода при успешной проверке SMS-кода.

**FR-8**

Система должна переводить незарегистрированного клиента на экран оформления заявки на дебетовую карту.

**FR-9**

Система должна предоставлять возможность ввода 4-значного PIN-кода.

**FR-10**

Система должна проверять корректность введённого PIN-кода.

**FR-11**

Система должна предоставлять возможность выхода из аккаунта.

**FR-12**

Система должна позволять пользователю оформить заявку на дебетовую карту с указанием ФИО, электронной почты и даты рождения.

**FR-13**

Система должна проверять, что возраст клиента на дату подачи заявки составляет не менее 14 лет.

**FR-14**

Система должна отображать сообщение об успешном оформлении заявки на дебетовую карту.

## 2. Главный экран и навигация

**FR-15**

Система должна отображать главный экран после успешной авторизации.

**FR-16**

Система должна отображать баланс дебетовой карты и последние 4 цифры номера карты на главном экране.

**FR-17**

Система должна обеспечивать навигацию между разделами «Главная» и «Мой профиль» через нижнюю панель.

## 3. История операций

**FR-18**

Система должна отображать историю всех операций по дебетовой карте.

**FR-19**

Система должна сортировать операции по дате в порядке убывания.

FR-20

Система должна группировать операции по дням совершения.

FR-21

Система должна предоставлять возможность фильтрации операций по дате.

FR-22

Система должна отображать детальную информацию по выбранной операции.

#### 4. Переводы по номеру телефона

FR-23

Система должна позволять выбрать получателя перевода по номеру телефона или из списка контактов.

FR-24

Система должна выполнять поиск номера телефона в базе банков.

FR-25

Система должна отображать список банков, в которых зарегистрирован номер телефона.

FR-26

Система должна позволять выбрать банк-получатель перевода.

FR-27

Система должна проверять, что сумма перевода является положительным числом не менее 0,01.

FR-28

Система должна проверять, что сумма перевода не превышает баланс дебетовой карты.

FR-29

Система должна выполнять перевод денежных средств по номеру телефона при выполнении всех условий.

FR-30

Система должна уменьшать баланс дебетовой карты на сумму выполненного перевода.

#### 5. Переводы по номеру карты

FR-31

Система должна предоставлять возможность ввода номера карты получателя.

FR-32

Система должна проверять существование номера карты в банковской базе.

FR-33

Система должна запрещать выполнение перевода при отсутствии карты в базе.

FR-34

Система должна выполнять перевод по номеру карты при достаточном балансе.

## 6. Чек операции

FR-35

Система должна отображать чек перевода после успешной операции.

FR-36

Система должна генерировать чек операции в формате PDF.

FR-37

Система должна предоставлять возможность предпросмотра PDF-чека.

FR-38

Система должна предоставлять возможность поделиться PDF-чеком через системный механизм ОС.

## 7. Оплата по QR-коду

FR-39

Система должна использовать камеру устройства для сканирования QR-кода.

FR-40

Система должна извлекать данные платежа из отсканированного QR-кода.

FR-41

Система должна выполнять оплату по QR-коду при достаточном балансе.

FR-42

Система должна уменьшать баланс дебетовой карты на сумму оплаты.

## 8. Управление дебетовой картой

FR-43

Система должна отображать экран управления дебетовой картой.

FR-44

Система должна позволять заблокировать дебетовую карту.

FR-45

Система должна запрещать операции по заблокированной карте.

FR-46

Система должна позволять заморозить дебетовую карту.

FR-47

Система должна позволять самостоятельно разморозить карту.

FR-48

Система должна отображать реквизиты карты полностью по запросу пользователя.

FR-49

Система должна позволять установить PIN-код для физической карты.

## 9. Лимиты по карте

FR-50

Система должна позволять установить лимит на траты по карте на период «неделя» или «месяц».

FR-51

Система должна учитывать все операции при расчёте лимита.

FR-52

Система должна отклонять операции, превышающие установленный лимит.

## 10. Реквизиты счёта и QR-код пополнения

FR-53

Система должна отображать реквизиты счёта клиента.

FR-54

Система должна генерировать PDF-файл с реквизитами счёта.

FR-55

Система должна отображать QR-код для пополнения счёта.

FR-56

Система должна предоставлять возможность отправки QR-кода в формате PDF.

## 11. Профиль клиента и документы

FR-57

Система должна отображать профиль клиента с персональными данными.

FR-58

Система должна позволять добавить или удалить фотографию профиля.

FR-59

Система должна отображать список документов клиента.

FR-60

Система должна позволять добавлять документы с загрузкой до 10 фотографий.

FR-61

Система должна сохранять загруженные фотографии документов.

FR-62

Система должна отображать статус успешного сохранения документов.

## Нефункциональные требования

### Требования к производительности (Performance Requirements, PR)

#### 1. Время отклика системы

PR-1

Время загрузки экрана «Вход в приложение» должно составлять не более 2 секунд при количестве до 1 000 одновременных пользователей.

PR-2

Время проверки SMS-кода и перехода на следующий экран должно составлять не более 1,5 секунд в 95% запросов.

PR-3

Время загрузки раздела «Главная» после успешной авторизации должно быть не более 2 секунд при количестве до 1 000 одновременных пользователей.

PR-4

Время загрузки экрана «Операции» с историей операций должно быть не более 3 секунд при объёме истории до 1 000 операций.

PR-5

Время загрузки экрана «Детали операции» должно быть не более 1,5 секунд.

PR-6

Время отображения экрана перевода (по номеру телефона или карты) должно быть не более 2 секунд.

PR-7

Время выполнения перевода (от нажатия кнопки «Перевести» до отображения экрана «Чек перевода») должно быть не более 3 секунд в 95% случаев.

PR-8

Время генерации PDF-чека операции должно быть не более 3 секунд.

PR-9

Время запуска камеры и готовности к сканированию QR-кода должно быть не более 2 секунд.

PR-10

Время обработки оплаты по QR-коду и отображения чека должно быть не более 3 секунд.

## 2. Пропускная способность

PR-11

Система должна поддерживать обработку не менее 50 операций перевода в секунду без деградации времени отклика.

PR-12

Система должна поддерживать генерацию не менее 30 PDF-чеков в минуту.

PR-13

Система должна обеспечивать загрузку истории операций для не менее 100 запросов в секунду.

PR-14

Система должна обеспечивать корректную обработку не менее 200 запросов в секунду к сервисам аутентификации (SMS-код + PIN).

## 3. Одновременные пользователи

PR-15

Система должна корректно функционировать при 1 000 одновременных активных пользователей без снижения заявленных показателей времени отклика.

PR-16

Система должна сохранять работоспособность при кратковременных пиковых нагрузках до 1 500 одновременных пользователей, с допустимым увеличением времени отклика не более чем на 30%.

PR-17

Система должна поддерживать не менее 5 000 зарегистрированных пользователей в рамках пилотной версии.

## 4. Стабильность и деградация

PR-18

При превышении предельной нагрузки система должна переходить в режим контролируемой деградации (отказ от нефункциональных операций, например генерации PDF), сохраняя возможность выполнения критических операций (вход, просмотр баланса).

PR-19

Доля неуспешных запросов при номинальной нагрузке не должна превышать 0,1%.

## 5. Производительность на клиенте

## PR-20

Приложение должно обеспечивать плавность интерфейса с частотой не ниже 50 FPS на устройствах среднего класса.

## PR-21

Приложение не должно потреблять более 300 МБ оперативной памяти при стандартном пользовательском сценарии.

# Требования к надежности (Reliability Requirements, RR)

## 1. Доступность (Uptime)

### RR-1

Доступность серверной части (API и backend-сервисы), обеспечивающей ключевые функции приложения (вход, просмотр баланса, история операций, переводы, оплата по QR), должна составлять не менее 99,9% в месяц.

### RR-2

Доступность функции аутентификации (отправка/проверка SMS-кода и проверка PIN) должна составлять не менее 99,9% в месяц.

### RR-3

Доступность функций платежей/переводов (перевод по телефону, перевод по карте, оплата по QR) должна составлять не менее 99,8% в месяц.

## 2. Частота отказов и уровень ошибок

### RR-4

Доля неуспешных запросов (HTTP 5xx/timeout/ошибка бизнес-логики на стороне сервера при корректном запросе клиента) при номинальной нагрузке не должна превышать 0,1% за сутки.

### RR-5

Для критических операций (вход, создание перевода/оплаты) доля неуспешных запросов не должна превышать 0,05% за сутки.

### RR-6

Система должна обеспечивать идемпотентность операций перевода/оплаты: повторная отправка одного и того же запроса клиентом (из-за потери сети/повтора) не должна приводить к двойному списанию средств.

## 3. Восстановление после сбоев (Recovery)

### RR-7

Целевое время восстановления сервиса после критического отказа (RTO) должно быть не более 30 минут.

RR-8

Целевая потеря данных при аварии (RPO) должна быть не более 5 минут для данных операций (переводы, оплаты, история операций).

RR-9

После восстановления система должна обеспечивать консистентность баланса и истории операций: сумма списаний/зачислений должна соответствовать реальным проведённым операциям, без «потерянных» или «задвоенных» транзакций.

#### 4. Устойчивость к сбоям внешних компонентов

RR-10

При недоступности сервиса отправки SMS система должна корректно информировать пользователя и предоставлять возможность повторить запрос кода позже (без зависания/краха приложения).

RR-11

При временной недоступности внешних справочников (поиск телефонов/карт) система должна либо повторять запрос по стратегии повторов, либо возвращать понятную ошибку и позволять пользователю повторить действие.

RR-12

При недоступности сервиса генерации PDF система должна позволять пользователю завершить сценарий (например, перейти на «Главную»), а генерацию чека пометить как временно недоступную.

#### 5. Поведение при потере сети и офлайн-режим

RR-13

При потере интернет-соединения приложение должно отображать состояние «нет сети» и предотвращать выполнение операций, требующих онлайн-подтверждения (переводы/оплаты).

RR-14

При восстановлении сети приложение должно позволять пользователю повторить последнее действие без необходимости перезапуска приложения.

#### 6. Резервирование и наблюдаемость

RR-15

Критические компоненты backend (API шлюз/баланс/операции/платежи) должны быть развернуты без единой точки отказа (минимум 2 экземпляра в рабочем контуре).

RR-16

Система должна обеспечивать централизованное логирование и мониторинг с алертингом по ключевым метрикам: доступность, latency, доля ошибок, количество отказов критических сценариев.

RR-17

Система должна хранить технические журналы, необходимые для расследования инцидентов по операциям (переводы/оплаты), не менее 90 дней.

## Требования к безопасности (Security Requirements, SR)

### 1. Аутентификация и управление сессией

SR-1

Система должна обеспечивать аутентификацию пользователя по номеру телефона и одноразовому SMS-коду.

SR-2

Система должна требовать ввод PIN-кода для доступа к функционалу приложения после успешного подтверждения SMS-кода.

SR-3

Система должна блокировать возможность повторной отправки SMS-кода до истечения заданного интервала (не менее 30 секунд).

SR-4

Система должна ограничивать количество попыток ввода SMS-кода (не более 5 попыток за 10 минут) с последующей временной блокировкой.

SR-5

Система должна ограничивать количество попыток ввода PIN-кода (не более 5 попыток подряд) с последующей временной блокировкой или требованием повторной аутентификации по SMS.

SR-6

Система должна завершать пользовательскую сессию (logout) по инициативе пользователя и удалять/инвалидировать токены доступа на устройстве.

SR-7

Система должна автоматически завершать сессию при длительном бездействии пользователя (10 минут), требуя повторный ввод PIN.

### 2. Авторизация и контроль доступа

SR-8

Система должна обеспечивать авторизацию всех API-запросов пользователя на сервере (проверка токена/сессии) и запрещать доступ к данным без валидной авторизации.

SR-9

Система должна обеспечивать доступ пользователя только к данным и операциям, относящимся к его аккаунту (баланс, операции, реквизиты, документы).

SR-10

Система должна запрещать выполнение операций по карте, если карта имеет статус «заблокирована» или «заморожена».

### 3. Шифрование данных и защита каналов

SR-11

Все соединения между мобильным приложением и сервером должны выполняться только по защищённому каналу TLS 1.2.

SR-12

Система не должна передавать чувствительные данные (PIN, одноразовые коды, токены) в открытом виде и не должна логировать их.

SR-13

Чувствительные данные, хранимые на устройстве (токены, идентификаторы сессии), должны храниться только в защищённом хранилище ОС (Keychain/Keystore).

SR-14

Чувствительные данные на сервере (например, токены/сессии, персональные данные) должны храниться в зашифрованном виде на уровне хранилища (at-rest encryption).

SR-15

PIN-код пользователя не должен храниться в открытом виде; допускается хранение только криптографического представления (хэш/производный ключ) с использованием современных алгоритмов.

### 4. Защита от атак на API и приложение

SR-16

Система должна применять rate limiting и антифрод-ограничения для чувствительных методов: отправка SMS, проверка SMS, вход, переводы, оплата.

SR-17

Система должна защищаться от перебора (brute force) для SMS-кодов и PIN-кодов (лимиты попыток, задержки, временные блокировки).

SR-18

Система должна защищаться от повторной отправки транзакций (replay): операции перевода/оплаты должны быть идемпотентны и иметь уникальный идентификатор.

SR-19

Система должна валидировать входные данные на сервере (форматы телефона/карты/суммы/сообщения), предотвращая инъекции и некорректные запросы.

SR-20

Система должна использовать защиту от MITM-атак (рекомендуемо: certificate pinning

для мобильного приложения) либо компенсирующие меры, если pinning не используется.

## 5. Безопасность операций и данных пользователя

SR-21

Система должна фиксировать в журнале безопасности критические события: вход/выход, неуспешные попытки входа, блокировки, переводы/оплаты, изменения лимитов, смена статуса карты.

SR-22

Система должна обеспечивать неизменяемость записей о финансовых операциях и возможность аудита (audit trail).

SR-23

Система должна маскировать чувствительные данные в интерфейсе и логах (например, номер карты — только последние 4 цифры).

## 6. Защита устройства и клиентской части

SR-24

Приложение должно запрещать отображение чувствительных экранов в системных снимках/превью многозадачности (например, masking при уходе в background).

SR-25

Приложение должно детектировать небезопасную среду (root/jailbreak, отладка, подмена сертификатов — по возможности) и применять ограничение доступа к критическим операциям либо предупреждать пользователя.

## Требования к удобству использования (Usability Requirements, UR)

UR-1

Новый пользователь должен быть способен войти в приложение (ввести номер телефона, SMS-код, PIN) без обучения менее чем за 2 минуты в 90% случаев.

UR-2

Новый пользователь должен быть способен найти баланс и последние 4 цифры карты на “Главной” менее чем за 10 секунд в 95% случаев.

UR-3

Новый пользователь должен быть способен открыть историю операций и перейти в детали операции без обучения менее чем за 60 секунд в 90% случаев.

UR-4

Новый пользователь должен быть способен выполнить перевод по номеру телефона (выбрать получателя, ввести сумму, отправить) без обучения менее чем за 2,5 минуты в 85% случаев.

#### **UR-5**

Пользователь должен быть способен выполнить перевод по номеру карты (ввести карту, сумму, отправить) без обучения менее чем за 2,5 минуты в 85% случаев.

#### **UR-6**

Пользователь должен быть способен выполнить оплату по QR-коду (запустить сканирование, подтвердить оплату) без обучения менее чем за 2 минуты в 85% случаев.

#### **UR-7**

Количество шагов (экранов) для выполнения типовой операции должно быть ограничено:

- вход: не более 3 экранов (телефон → SMS → PIN),
- перевод: не более 3–4 экранов (выбор получателя → ввод суммы → чек),
- оплата по QR: не более 3 экранов (сканирование → подтверждение → чек).

#### **UR-8**

Все критические ошибки ввода (неверный SMS-код, неверный PIN, недостаточно средств, неверный формат суммы/карты) должны сопровождаться понятным сообщением и подсказкой, что делать дальше; пользователь должен иметь возможность исправить ошибку за 1 попытку без повторного прохождения всего сценария.

#### **UR-9**

Навигация должна быть предсказуемой: на всех вторичных экранах должна быть доступна функция «Назад», возвращающая пользователя в логически предыдущий экран, а основные разделы должны быть доступны через нижнюю навигацию.

#### **UR-10**

Новый пользователь должен быть способен добавить документ (выбрать тип, загрузить фото, сохранить) без обучения менее чем за 3 минуты в 85% случаев.

### **Требования к сопровождаемости (Maintainability Requirements, MR)**

#### **MR-1**

Код приложения должен быть разделён на модули по доменам:

- Аутентификация,
- Главная,
- Операции,
- Переводы,
- QR-оплата,
- Дебетовая карта/настройки,
- Профиль/Документы,
- Общий UI/Навигация.

#### **MR-2**

Бизнес-логика должна быть отделена от UI: компоненты интерфейса не должны

содержать логику выполнения операций (перевод, проверка лимитов, валидации) кроме отображения состояния и отправки событий.

#### MR-3

Взаимодействие с сервером должно быть реализовано через единый слой API-клиента (единая точка настройки базового URL, таймаутов, обработчиков ошибок, авторизации и логирования).

#### MR-4

Все конфигурационные параметры (например: таймауты, интервалы повторной отправки SMS, ограничения длины сообщений, лимиты попыток) должны быть вынесены в конфигурацию и не «зашиты» в коде.

#### MR-5

Код должен быть покрыт автоматическими тестами:

- критические сценарии (вход, просмотр операций, перевод, QR-оплата, блокировка/заморозка карты) должны иметь юнит- и/или интеграционные тесты,
- целевой минимум покрытия бизнес-логики — не менее 70%.

#### MR-6

Система должна использовать централизованную обработку ошибок: единый механизм классификации ошибок (сеть/сервер/валидация/бизнес-ограничения) и единый формат отображения сообщений пользователю.

#### MR-7

Изменения в одном модуле не должны требовать модификации более чем 2 других модулей (требование к слабой связности и минимизации «сквозных» зависимостей).

#### MR-8

Для всех публичных интерфейсов модулей (API-клиент, репозитории, сервисы домена) должна быть доступна документация (минимум: назначение, входы/выходы, ошибки) и единый стиль кодирования.

#### MR-9

Приложение должно поддерживать механизм feature flags (включение/выключение функций без релиза новой версии приложения) минимум для: переводы, QR-оплата, генерация PDF, загрузка документов.

#### MR-10

Сборка и релиз должны быть воспроизводимыми: проект должен собираться в CI, а pipeline должен включать обязательные шаги линтинга, тестов и статического анализа с падением сборки при критических ошибках.

### Требования к портируемости (Portability Requirements, PRt)

#### PRt-1

Мобильное приложение должно поддерживать запуск и корректную работу на

платформах iOS и Android без функциональных различий в ключевых пользовательских сценариях.

#### PRt-2

Приложение должно поддерживать актуальные и предыдущие основные версии операционных систем:

- iOS — не менее 2 последних major-версий,
- Android — не менее 3 последних major-версий.

#### PRt-3

Приложение должно корректно работать на устройствах с различными размерами экранов и разрешениями (смартфоны и планшеты), без потери доступности функционала и читаемости интерфейса.

#### PRt-4

Взаимодействие с платформенно-зависимыми функциями (камера, хранилище, системный шаринг) должно быть реализовано через абстрактный слой, минимизирующий зависимость бизнес-логики от конкретной ОС.

#### PRt-5

Сборка и конфигурация приложения должны быть воспроизводимыми для каждой платформы и не требовать изменения бизнес-логики при добавлении или обновлении поддерживающей платформы.

### Требования к цифровой доступности (Accessibility Requirements, AR)

#### AR-1

Весь нетекстовый контент, представленный пользователю, имеет текстовую альтернативу, которая выполняет ту же функцию

#### AR-2

Информация, структура и связи, передаваемые посредством представления, могут быть определены программно или доступны в текстовом виде.

#### AR-3

Когда последовательность представления контента влияет на его смысл, правильная последовательность чтения может быть определена программно.

#### AR-4

Инструкции, предназначенные для понимания и использования контента, не опираются исключительно на сенсорные характеристики компонентов, такие как форма, цвет, размер, визуальное расположение, ориентация или звук.

#### AR-5

Цвет не используется как единственное визуальное средство передачи информации, обозначения действия, побуждения к действию или выделения визуального элемента.

## AR-6

Все функциональные возможности контента доступны через жестовый интерфейс навигации по фокусу без необходимости соблюдать определенные интервалы между выполнением отдельных касаний, за исключением случаев, когда базовая функция требует ввода данных, зависящего от траектории движения пользователя, а не только от конечных точек.

## AR-7

Если элемент интерфейса в мобильном приложении может получить фокус с помощью скринридера (жестовой навигации/перемещения фокуса доступности), то пользователь должен иметь возможность убрать фокус с этого элемента и перейти к следующему/предыдущему элементу только средствами скринридера, без дополнительных действий вне стандартных жестов. Если для выхода из элемента требуется нестандартное действие (например, особый жест, кнопка «Закрыть», смена режима навигации), приложение должно явно сообщать пользователю, как это сделать (озвучиваемая подсказка и/или доступная метка элемента управления).

## AR-8

Страницы имеют заголовки, описывающие тему или назначение.

## AR-9

Если страницу можно пройти последовательно и последовательность навигации влияет на смысл или работоспособность, то компоненты, на которых можно сфокусироваться, получают фокус в порядке, сохраняющем смысл и работоспособность.

## AR-10

Для компонентов пользовательского интерфейса с подписями, содержащими текст или изображения текста, название содержит текст, который отображается визуально.

## AR-11

Когда любой компонент пользовательского интерфейса получает фокус, это не приводит к изменению контекста.

## AR-12

Изменение настроек любого компонента пользовательского интерфейса не приводит автоматически к изменению контекста, если только пользователь не был проинформирован о таком поведении компонента перед его использованием.

## AR-13

Подписи или инструкции предоставляются, когда для получения контента требуется участие пользователя.

## AR-14

Для всех компонентов пользовательского интерфейса (включая, помимо прочего, элементы форм, ссылки и компоненты, созданные с помощью скриптов) имя и роль могут быть определены программно; состояния, свойства и значения, которые может устанавливать пользователь, могут быть установлены программно; а уведомление об

изменениях этих элементов доступно пользовательским агентам, включая вспомогательные технологии.

## Требования к интерфейсам

### Пользовательские интерфейсы (UI)

UI-1.

Пользовательский интерфейс приложения должен быть реализован на основе единой дизайн-системы, включающей:

- набор базовых компонентов (кнопки, поля ввода, списки, карточки, заголовки),
- правила отступов, размеров и скруглений,
- единые состояния компонентов (default, active, disabled, error).

UI-2.

Все экраны приложения должны соответствовать единому структурному шаблону, включающему:

- верхнюю панель с заголовком экрана,
- контентную область с основной задачей экрана,
- единственную основную кнопку действия (Primary CTA), если экран предполагает действие пользователя.

UI-3.

Интерфейс должен использовать унифицированные навигационные элементы:

- иконка «Назад» в виде стрелки влево на всех вторичных экранах,
- нижнюю навигационную панель только для основных разделов приложения,
- одинаковое визуальное поведение навигационных элементов на всех экранах.

UI-4.

Финансовые данные в интерфейсе должны отображаться по единым правилам:

- баланс и суммы операций визуально выделяются как ключевая информация,
- используется единый формат отображения денежных значений,
- списание и зачисление различаются не только цветом, но и знаковым/текстовым обозначением.

UI-5.

Все элементы ввода данных должны соответствовать единому UI-стандарту:

- наличие текстовой подписи поля,

- отображение подсказки или примера формата ввода,
- единое визуальное оформление ошибок ввода, расположенных рядом с полем.

UI-6.

Кнопки в интерфейсе должны быть типизированы и визуально различимы:

- основное действие (Primary),
- вторичное действие (Secondary),
- неактивное состояние (Disabled),
- деструктивное действие (например, блокировка карты).

UI-7.

Все списки и карточки должны использовать единый визуальный паттерн:

- одинаковая высота элементов списка,
- единая структура карточек (заголовок → описание → дополнительная информация),
- визуальное разделение элементов списка без перегрузки экрана.

UI-8.

Экраны, отображающие результат пользовательского действия (успех/завершение), должны быть оформлены единообразно и включать:

- краткое подтверждение результата,
- визуально отделённый блок ключевых данных операции,
- чётко обозначенное дальнейшее действие пользователя.

UI-9.

Интерфейс должен применять единые правила визуальной защиты чувствительных данных:

- маскирование данных по умолчанию,
- явное пользовательское действие для раскрытия информации,
- визуальное обозначение состояния «данные скрыты / данные показаны».

UI-10.

Пользовательский интерфейс должен обеспечивать визуальную и поведенческую консистентность, при которой:

- одинаковые элементы выглядят и работают одинаково на всех экранах,
- одинаковые действия пользователя приводят к одинаковым визуальным результатам,
- изменения состояния интерфейса всегда визуально очевидны пользователю.

## Программные интерфейсы (PI)

### PI-1. Единый транспорт и безопасность API

Все внешние и внутренние API-вызовы мобильного клиента к backend должны выполняться по HTTPS с принудительным использованием TLS не ниже 1.2 и проверкой сертификата сервера (pinning — как отдельная опция).

### PI-2. Единый формат данных API

Backend API должен принимать и возвращать данные в JSON (UTF-8) по единым правилам:

- единый envelope ошибок,
- единые поля корреляции/трассировки (`requestId`, `correlationId`),
- единый формат дат/времени (ISO 8601).

### PI-3. Идемпотентность платежных запросов

Все запросы, создающие финансовую операцию (перевод/оплата), должны быть идемпотентными: клиент передаёт `Idempotency-Key`, backend гарантирует отсутствие двойного списания при повторе.

### PI-4. Интеграция с сервисом отправки SMS (OTP)

Система должна интегрироваться с внешним SMS/OTP-провайдером через выделенный адаптер:

- протокол: HTTPS (REST) или SMPP (если у провайдера так),
- формат: JSON (или провайдерский),
- обязательные параметры: телефон, шаблон/тип OTP, TTL, канал доставки,
- обязательные ответы: `messageId`, статус доставки/ошибки.

Endpoints backend:

- POST /auth/otp/send
- POST /auth/otp/verify

### PI-5. Интеграция со справочником “телефон → банки” (маршрутизация переводов)

Backend должен иметь интерфейс к внешнему справочнику, который по номеру телефона возвращает:

- список банков, где зарегистрирован получатель,
- идентификаторы банков/участников для маршрутизации платежа.

### PI-6. Интеграция со справочником “карта → банк/валидность”

Backend должен иметь интерфейс к внешнему сервису проверки номера карты (BIN/пан/валидность/принадлежность):

- протокол: HTTPS (REST),
- ответ: найдено/не найдено, банк-эмитент/маршрут, маска отображения.

#### PI-7. Единый платежный оркестратор (routing layer)

В backend должен быть единый сервис-оркестратор платежей, который:

- принимает запрос на перевод/оплату,
- выбирает маршрут: внутрибанковский или межбанковский (например, через СБП),
- приводит разные внешние протоколы к единому внутреннему контракту,
- возвращает единый статус операции клиенту.

#### PI-8. Перевод по телефону: контракт операции

Backend должен предоставить API операции “перевод по телефону”, включающее:

- получателя (телефон E.164),
- выбранный банк-получатель (из списка справочника),
- сумму, валюту,
- сообщение получателю (если есть),
- признаки комиссий/лимитов (если применимо),
- ответ с operationId, статусом, данными для чека.

Endpoints backend:

- POST /payments/transfers/phone
- GET /payments/operations/{operationId}

#### PI-9. Перевод по номеру карты: контракт операции

Backend должен предоставить API операции “перевод по карте”, включающее:

- получатель (tokenized PAN или PAN в защищённом виде),
- сумму, валюту,
- ответ с operationId, статусом, данными для чека.

Endpoints backend:

- POST /payments/transfers/card

#### PI-10. QR-оплата: контракт операции

Backend должен поддерживать два режима интеграции для QR-платежа:

1. decode-on-client: клиент отправляет уже распарсенные реквизиты из QR;
2. decode-on-server: клиент отправляет сырой payload QR, сервер декодирует.

Endpoints backend:

- POST /payments/qr/decode (если decode-on-server)
- POST /payments/qr/pay

#### PI-11. Генерация чека/квитанции в PDF

Backend должен иметь интерфейс к сервису генерации PDF, который по operationId формирует PDF:

- протокол: HTTPS,
- выход: PDF (application/pdf) + метаданные (имя файла, размер, hash),
- поддержка деградации: если сервис недоступен — операция всё равно считается завершённой, а PDF помечается “временно недоступно”.

Endpoints backend:

- GET /receipts/{operationId}.pdf
- GET /receipts/{operationId}/status

#### PI-12. Файлы и системный шаринг (мобильная ОС)

Клиент должен использовать стандартные механизмы ОС для:

- выбора фото (камера/галерея),
- доступа к камере для сканирования,
- системного “Поделиться” для PDF.

На стороне backend это отражается контрактами:

- загрузка файлов: POST /profile/documents/{type}/photos
- получение метаданных/статуса: GET /profile/documents

#### PI-13. Профиль и документы: контракты

Backend должен предоставить API для профиля и документов:

- получение профиля,
- загрузка/удаление фото профиля,
- список документов и их статусы,
- загрузка до N фотографий документа, с ответом о принятии и статусом проверки.

Endpoints backend:

- GET /profile

- PUT /profile/photo
- DELETE /profile/photo
- GET /profile/documents
- POST /profile/documents/{docType}/photos

PI-14. Кarta/счёт: реквизиты и QR пополнения

Backend должен предоставить API:

- реквизиты счёта (в JSON),
- генерация PDF реквизитов,
- генерация QR для пополнения (payload + картинка при необходимости),
- генерация PDF с QR.

Endpoints backend:

- GET /accounts/{accountId}/details
- GET /accounts/{accountId}/details.pdf
- GET /accounts/{accountId}/topup/qr
- GET /accounts/{accountId}/topup/qr.pdf

PI-15. Наблюдаемость интеграций (технические требования к интерфейсам)

Для всех интеграций (SMS, справочники, платежный контур, PDF) должны быть реализованы:

- таймауты, retries с backoff, circuit breaker,
- логирование без чувствительных данных,
- метрики latency/error-rate по каждому внешнему провайдеру,
- корреляция по requestId.

## Интерфейсы связи (CI)

CI-1.

Мобильное приложение должно взаимодействовать с backend-сервисами исключительно по HTTPS поверх TCP/IP.

CI-2.

Все соединения между мобильным приложением и сервером должны использовать TLS версии не ниже 1.2.

CI-3.

Система не должна допускать взаимодействие по незашифрованному HTTP, а также по любым протоколам, не обеспечивающим шифрование канала (для API-трафика).

CI-4.

Интеграция backend с внешними системами (SMS/OTP, справочники телефонов/карт, генерация PDF) должна выполняться по защищённым сетевым протоколам, эквивалентным по уровню защиты каналу клиентскому (HTTPS + TLS ≥ 1.2).

CI-5.

Вызов камеры для сканирования QR-кода должен выполняться через системные (платформенные) интерфейсы iOS/Android без прямого сетевого доступа из модуля камеры (сеть используется только на следующих шагах: декодирование/оплата через backend).

CI-6.

Передача PDF-файлов “Поделиться”/“Отправить” должна выполняться через системные механизмы ОС (без прямого сетевого протокола со стороны приложения); приложение передаёт ОС файл/URI, а сетевую доставку выполняют выбранные приложения/службы ОС.

CI-7.

Для всех сетевых запросов (к backend и внешним сервисам через backend) должны быть заданы таймауты на соединение и ожидание ответа, согласованные с требованиями времени отклика ключевых операций (вход, переводы, QR, PDF).

CI-8.

Система должна поддерживать повтор сетевых запросов в сценариях временной недоступности сервисов/сети, с контролируемой стратегией повторов (например, backoff), при этом не допуская дублей финансовых операций.

CI-9.

При отсутствии интернет-соединения приложение должно отображать состояние “нет сети” и блокировать сетевые операции, требующие онлайн-подтверждения (переводы/оплаты).

CI-10.

Запросы, создающие финансовую операцию (перевод/оплата), должны быть идемпотентными на уровне сетевого взаимодействия: повторная отправка “того же” запроса (из-за ретраев/потери сети) не должна приводить к двойному списанию.

CI-11.

Сетевое взаимодействие должно быть реализовано единообразно для iOS и Android, без функциональных различий в ключевых сценариях.

## Требования к данным

### Логическая модель данных

Customer

Название атрибута	Описание	Формат данных
customer_id	Идентификатор клиента (PK)	UUID
phone	Номер телефона	VARCHAR(15)
last_name	Фамилия клиента	VARCHAR(100)
first_name	Имя клиента	VARCHAR(100)
middle_name	Отчество клиента (может отсутствовать)	VARCHAR(100), NULL
email	Адрес электронной почты	VARCHAR(255)
birth_date	Дата рождения клиента	DATE
profile_photo_id	Идентификатор фотографии профиля	UUID, NULL
status	Статус клиента (active / blocked)	VARCHAR(20)
created_at	Дата и время создания клиента	TIMESTAMP
updated_at	Дата и время последнего обновления	TIMESTAMP

Связи:

- Customer 1 — 0..N CardApplication  
Клиент может подавать заявки (в т.ч. повторно/история); заявка может существовать до появления клиента.
- Customer 1 — 0..1 DebitCard  
В пилоте: у клиента может быть не более одной дебетовой карты.
- Customer 1 — 0..1 Account  
В пилоте логично 1 счёт под 1 карту (или счёт создаётся вместе с картой).
- Customer 1 — 0..N Document  
У клиента может быть несколько документов (паспорт/ИНН и т.д.).

CardApplication

<b>Название атрибута</b>	<b>Описание</b>	<b>Формат данных</b>
application_id	Идентификатор заявки (PK)	UUID
phone	Номер телефона заявителя	VARCHAR(15)
last_name	Фамилия заявителя	VARCHAR(100)
first_name	Имя заявителя	VARCHAR(100)
middle_name	Отчество заявителя	VARCHAR(100), NULL
email	Email заявителя	VARCHAR(255)
birth_date	Дата рождения	DATE
age_check_passed	Признак прохождения проверки возраста	BOOLEAN
status	Статус заявки	VARCHAR(30)
submitted_at	Дата и время подачи заявки	TIMESTAMP
processed_at	Дата и время обработки заявки	TIMESTAMP, NULL

## DebitCard

<b>Название атрибута</b>	<b>Описание</b>	<b>Формат данных</b>
debit_card_id	Идентификатор карты (PK)	UUID
customer_id	Идентификатор владельца карты (FK → Customer)	UUID
pan_masked_last4	Последние 4 цифры номера карты	CHAR(4)
pan_token	Токенизованный номер карты	VARCHAR(255)
status	Статус карты (active / frozen / blocked)	VARCHAR(20)
balance_amount	Текущий баланс карты	DECIMAL(15,2)
currency	Валюта карты	CHAR(3)
opened_at	Дата открытия карты	TIMESTAMP
blocked_at	Дата блокировки карты	TIMESTAMP, NULL

frozen_at	Дата заморозки карты	TIMESTAMP, NULL
-----------	----------------------	-----------------

Связи:

- DebitCard N — 1 Customer  
Каждая карта принадлежит одному клиенту.
- DebitCard 1 — 1 Account  
В пилоте карта связана с одним счётом (и наоборот).
- DebitCard 1 — 0..1 CardSpendingLimit  
Лимит либо установлен, либо нет; один активный лимит на карту.
- DebitCard 1 — 0..N Operation  
По карте выполняются операции (списания/зачисления).

Account

Название атрибута	Описание	Формат данных
account_id	Идентификатор счёта (PK)	UUID
customer_id	Идентификатор владельца счёта (FK → Customer)	UUID
contract_number	Номер договора	VARCHAR(50)
recipient_name	Получатель платежа	VARCHAR(255)
account_number	Номер счёта	VARCHAR(34)
payment_purpose	Назначение платежа	VARCHAR(255)
bic	БИК банка	VARCHAR(9)
bank_name	Наименование банка получателя	VARCHAR(255)
correspondent_account	Корреспондентский счёт	VARCHAR(34)
inn	ИНН получателя	VARCHAR(12)

Связи:

- Account N — 1 Customer  
Счёт принадлежит клиенту.
- Account 1 — 0..N Operation  
История операций по счёту.
- Account 1 — 1 DebitCard  
В пилоте счёт привязан к карте (1:1).

## Operation

Название атрибута	Описание	Формат данных
operation_id	Идентификатор операции (PK)	UUID
account_id	Счёт операции (FK → Account)	UUID
debit_card_id	Карта операции (FK → DebitCard)	UUID
type	Тип операции	VARCHAR(30)
direction	Направление (debit / credit)	VARCHAR(10)
amount	Сумма операции	DECIMAL(15,2)
currency	Валюта операции	CHAR(3)
occurred_at	Дата и время операции	TIMESTAMP
counterparty_name	Получатель / отправитель	VARCHAR(255)
status	Статус операции	VARCHAR(20)
decline_reason	Причина отказа	VARCHAR(255), NULL
idempotency_key	Ключ идемпотентности	VARCHAR(100)

### Связи:

- Operation N — 1 Account  
Операция относится к счёту.
- Operation N — 1 DebitCard  
Операция относится к карте (в пилоте можно хранить и account\_id, и debit\_card\_id).
- Operation 1 — 0..1 Transfer  
Если операция является переводом — есть запись Transfer.
- Operation 1 — 0..1 QrPayment  
Если операция является QR-оплатой — есть запись QrPayment.

## Transfer

Название атрибута	Описание	Формат данных
transfer_id	Идентификатор перевода (PK)	UUID
operation_id	Связанная операция (FK → Operation)	UUID

transfer_kind	Тип перевода (by_phone / by_card)	VARCHAR(20)
sender_account_id	Счёт отправителя	UUID
recipient_phone	Телефон получателя	VARCHAR(15), NULL
recipient_card_token	Токен карты получателя	VARCHAR(255), NULL
recipient_bank_id	Банк получателя	UUID, NULL
recipient_name	Имя получателя	VARCHAR(255)
message	Сообщение получателю	VARCHAR(100), NULL
amount	Сумма перевода	DECIMAL(15,2)
currency	Валюта	CHAR(3)
status	Статус перевода	VARCHAR(20)
created_at	Дата создания	TIMESTAMP

Связи:

- Transfer 1 — 1 Operation  
Transfer — это “детализация” операции типа перевод (строго один к одному).
- Transfer N — 1 Account (через )  
Перевод инициируется со счёта от sender\_account\_idавителя.

## QrPayment

Название атрибута	Описание	Формат данных
qr_payment_id	Идентификатор QR-платежа (PK)	UUID
operation_id	Связанная операция (FK → Operation)	UUID
qr_raw_payload	Содержимое QR-кода	TEXT
merchant_name	Организация-получатель	VARCHAR(255)
beneficiary_account	Лицевой счёт получателя	VARCHAR(50)
amount	Сумма платежа	DECIMAL(15,2)
currency	Валюта платежа	CHAR(3)
status	Статус платежа	VARCHAR(20)
created_at	Дата создания	TIMESTAMP

Связи:

- QrPayment 1 — 1 Operation  
QrPayment — детализация операции типа QR-оплата (1:1)

## CardSpendingLimit

Название атрибута	Описание	Формат данных
limit_id	Идентификатор лимита (PK)	UUID
debit_card_id	Карта, к которой применён лимит	UUID
period	Период лимита (week / month)	VARCHAR(10)
limit_amount	Значение лимита	DECIMAL(15,2)
currency	Валюта лимита	CHAR(3)
spent_amount	Потраченная сумма в периоде	DECIMAL(15,2)
status	Статус лимита	VARCHAR(20)
updated_at	Дата изменения лимита	TIMESTAMP

Связи:

- CardSpendingLimit 1 — 1 DebitCard  
Лимит задаётся для конкретной карты (обычно один активный лимит на карту).

## Document

Название атрибута	Описание	Формат данных
document_id	Идентификатор документа (PK)	UUID
customer_id	Владелец документа (FK → Customer)	UUID
type	Тип документа	VARCHAR(30)
status	Статус проверки документа	VARCHAR(20)
created_at	Дата загрузки документа	TIMESTAMP
updated_at	Дата обновления документа	TIMESTAMP

Связи:

- Document N — 1 Customer  
Документ принадлежит клиенту.
- Document 1 — 0..N DocumentPhoto  
У одного документа может быть до 10 фотографий.

## DocumentPhoto

Название атрибута	Описание	Формат данных
photo_id	Идентификатор фотографии (PK)	UUID
document_id	Документ, к которому относится фото	UUID
file_url	Ссылка на файл изображения	VARCHAR(500)
order_index	Порядковый номер фото	INTEGER
uploaded_at	Дата загрузки	TIMESTAMP

### Связи:

- DocumentPhoto N — 1 Document  
Фото относится к одному документу.

## Требования к хранению

### Объём данных и рост

#### STOR-1

Должна быть определена модель роста данных минимум на 12 месяцев, учитывая количество клиентов, операций, документов и файлов, с резервом под пиковые нагрузки.

#### STOR-2

Транзакционные данные (клиенты, счета, карты, операции) должны храниться в реляционной БД.  
Файлы (фото документов, PDF-чек, PDF реквизитов) должны храниться в объектном или файловом хранилище, а в БД — только ссылки и метаданные.

#### STOR-3

История операций должна храниться в полном объёме с возможностью масштабирования (индексация, партиционирование по дате при достижении порогов объёма).

#### STOR-4

Система должна поддерживать хранение до 10 фотографий на один документ клиента, с сохранением связей между документом и его файлами.

## **STOR-5**

Должны быть определены и задокументированы сроки хранения для:

- данных клиентов и продуктов,
- операций и чеков,
- документов клиента,
- технических и временных данных (OTP, сессии).

## **Резервное копирование и восстановление**

### **STOR-6**

Для транзакционных данных должны быть установлены целевые показатели допустимой потери данных (RPO) и времени восстановления (RTO), зафиксированные в SLA/SLO.

### **STOR-7**

Должны выполняться регулярные резервные копии базы данных (полные и инкрементальные/журнальные), обеспечивающие достижение заданного RPO.

### **STOR-8**

Файлы документов и PDF должны быть защищены от потери с помощью резервного копирования или встроенного механизма репликации/версионирования.

### **STOR-9**

Все резервные копии (БД и файлов) должны храниться в зашифрованном виде с контролируемым доступом к ключам шифрования.

### **STOR-10**

Должны проводиться регулярные тесты восстановления данных из резервных копий с фиксацией результатов и фактического времени восстановления.

## **Архивирование и жизненный цикл данных**

### **STOR-11**

Операции старше установленного срока должны переводиться в архивный слой хранения с сохранением возможности последующего доступа и выгрузки.

### **STOR-12**

Данные за последний активный период должны храниться в высокопроизводительном хранилище, архивные — в более дешёвом слое с увеличенным временем доступа.

### **STOR-13**

Технические логи, сессии и временные данные безопасности должны автоматически архивироваться или удаляться по истечении установленного срока хранения.

### **STOR-14**

Для документов клиента должны быть определены правила архивирования и удаления после закрытия продукта или аккаунта в соответствии с юридическими требованиями.

## **Контроль и мониторинг**

## STOR-15

Должен быть настроен мониторинг объёма данных (БД, файлы, бэкапы) с оповещениями при достижении порогов использования хранилища.

## Требования к целостности

### INT-1

Поле phone должно быть обязательным и быть уникальным в пределах клиентов.

### INT-2

last\_name, first\_name обязательны; middle\_name допускается NULL.

Ограничения: только буквы (кириллица/латиница) + допустимые символы (пробел/дефис), без цифр и спецсимволов. Длина каждого поля ограничена.

### INT-3

email должен соответствовать базовому формату email (локальная часть@домен). Для клиента допускается политика уникальности (TBD), но формат обязателен.

### INT-4

birth\_date обязательна; при регистрации/подаче заявки возраст должен быть не менее 14 лет (валидация на уровне бизнес-логики).

### INT-5

Все amount, balance\_amount, limit\_amount должны быть  $> 0$  для списаний/платежей; для переводов и QR-платежей минимальная сумма  $\geq 0.01$ .

currency должна быть в формате ISO-4217 (CHAR(3)).

### INT-6

Операции типа списание не должны проводиться при недостаточном балансе. Баланс не должен уходить в отрицательное значение (если не предусмотрен овердрафт — в пилоте не предусмотрен).

### INT-7

Если установлен лимит, то  $limit\_amount > 0$ , period  $\in \{\text{week}, \text{month}\}$ .

Операции, превышающие остаток лимита в периоде, должны отклоняться. spent\_amount не может быть отрицательным.

### INT-8

Все FK должны ссылаться на существующие записи (Customer, Account, DebitCard, Document).

Для Operation: допускается не более одной детализации — либо Transfer, либо QrPayment (взаимоисключающие записи 0..1).

### INT-9

Для всех создающих списание/перевод/оплату запросов должен использоваться idempotency\_key (уникальный в пределах клиента/операции), чтобы исключить двойное проведение при повторе запроса.

INT-10

Для одного Document допускается максимум 10 DocumentPhoto.

order\_index уникален в рамках одного документа и находится в диапазоне 1..10.

Ссылка на файл (file\_url) обязательна.