**Business requirements document**

Проект:

«Разработка системы выявления подозрительных транзакций для банка»

**Содержание документа BRD**

[1.1. Цель документа 3](#_heading=h.syoqkrx351v1)

[1.2. Область применения 3](#_heading=h.xv5zmtj1eck8)

[1.3. Термины и определения 4](#_heading=h.vneb0k365rtj)

[2.1. Общая информация 6](#_heading=h.v0ok12u3dmnb)

[2.2. Бизнес-контекст 6](#_heading=h.g621696a8lrj)

[2.3. Основные заинтересованные стороны (стейкхолдеры) 7](#_heading=h.r65hay371jfi)

[2.4. Ограничения и допущения 8](#_heading=h.a4jr7sv7yrrd)

[БИЗНЕС-ЦЕЛИ И ЗАДАЧИ 9](#_heading=h.ivkol8ow822o)

[3.1. Описание бизнес-проблемы 10](#_heading=h.kuj5zd9m7bbd)

[3.2. Цель проекта 10](#_heading=h.gmafsi0ywux)

[3.3. Критерии успеха 11](#_heading=h.6amsadjuorbk)

[ТРЕБОВАНИЯ К БИЗНЕС-ЗАДАЧЕ 13](#_heading=h.kuuiqtgeauwt)

[4.1. Бизнес-требования 13](#_heading=h.bjbg98x0orpl)

[4.2. Бизнес-правила 13](#_heading=h.kni1wajum1sp)

[4.3. Пользовательские требования 14](#_heading=h.upgd4iicmuuk)

[4.3. Функциональные требования 15](#_heading=h.12tur2tzjmcq)

[4.4. Ограничения 16](#_heading=h.klpg7vfj2uq3)

[БИЗНЕС-ПРОЦЕССЫ И СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ 17](#_heading=h.vbj2taco845z)

[5.1. Описание текущих процессов 17](#_heading=h.8fqxuncb5m17)

[5.2. Описание целевых процессов 17](#_heading=h.5unjhbt6svvd)

[5.3. Основные сценарии использования (Use Cases)](#_heading=h.dxjey95simtr) [18](#_heading=h.kqoygh2jt62h)

[ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ СИСТЕМАМИ 20](#_heading=h.c1oig3swkqsb)

[6.1. Описание интеграций 20](#_heading=h.qp8hkr8yedeg)

[6.2. Зависимости от внешних систем и сервисов 20](#_heading=h.vpy149bu64g0)

[ОЦЕНКА РИСКОВ 21](#_heading=h.lhx4tz5kgolv)

[7.1. Основные риски проекта 21](#_heading=h.esnocs5w092t)

[7.2. Меры по их снижению 21](#_heading=h.eawbcl97qbai)

[КРИТЕРИИ ПРИЕМКИ 23](#_heading=h.oxiqm2vtpq35)

[ПРИЛОЖЕНИЯ 24](#_heading=h.tvmqdqtz3j3p)

**ВВЕДЕНИЕ**

# 1.1. Цель документа

Цель данного документа — зафиксировать и согласовать бизнес-требования для разработки системы автоматического выявления подозрительных транзакций в банке. В документе описываются задачи, функциональные требования, архитектура системы, а также обеспечиваемые результаты.

# 1.2. Область применения

Этот документ служит основой для дальнейшей разработки и внедрения системы, будет полезен всем участникам проекта.

# 1.3. Термины и определения

| **Термин** | **Определение** |
| --- | --- |
| **BRD (Business Requirements Document)** | Документ, описывающий бизнес-требования, цели и ожидаемые результаты проекта. |
| **Стейкхолдеры (Stakeholders)** | Лица или организации, заинтересованные в успехе проекта (руководство банка, IT-отдел, регуляторы и др.). |
| **AML (Anti-Money Laundering)** | Политика противодействия отмыванию денег. |
| **CFT (Counter-Terrorism Financing)** | Меры по борьбе с финансированием терроризма. |
| **GDPR (General Data Protection Regulation)** | Общий регламент по защите персональных данных в ЕС. |
| **DWH (Data Warehouse)** | Хранилище данных для аналитики и отчетности. |
| **PostgreSQL** | Реляционная СУБД для хранения структурированных данных. |
| **Yandex DataLens** | Инструмент для визуализации данных и создания дашбордов. |
| **Подозрительная транзакция** | Операция, соответствующая критериям риска (например, крупная сумма, аномальное время/место). |
| **Веб-дашборд** | Интерфейс для визуализации данных о транзакциях в реальном времени. |
| **Метрики подозрительных транзакций** | Критерии для автоматического определения подозрительных операций (например, лимиты сумм). |
| **Витрина данных** | Готовый набор данных для анализа, сформированный из DWH. |

**1.4. Ссылочные документы**

Стандарт информационной безопасности банка:

* ГОСТ Р 50.1.111-2016
* ГОСТ 28147-89

Соответствие:

* + ФЗ-152 «О персональных данных»
  + 115-ФЗ «О противодействии отмыванию доходов»
  + Приказы ЦБ РФ по защите финансовых данных

**ОПИСАНИЕ ПРОДУКТА**

# 2.1. Общая информация

Продукт представляет собой систему для анализа банковских транзакций, которая будет интегрирована с основными источниками данных банка, такими как информация о клиентах, транзакциях, геолокации совершения операций, а также страна получателя перевода.

Система будет использовать алгоритмы для анализа транзакций и выявления тех, которые могут быть подозрительными, на основе заранее заданных критериев.

Все данные, используемые системой, будут включать историческую информацию, что позволит повысить точность выявления подозрительных операций и минимизировать риски.

Система будет анализировать данные, выявляя операции, которые не соответствуют стандартам или могут быть связаны с незаконной деятельностью.

С помощью разработанного веб-дашборда будет предоставляться визуализированный отчет, который позволит аналитикам и сотрудникам банка оперативно принимать решения.

# 2.2. Бизнес-контекст

Проект разрабатывается в рамках повышения информационной безопасности и комплаенс-стандартов для банков.

В последние годы наблюдается рост финансовых преступлений, включая мошенничество и отмывание денег, что требует создания систем, способных вовремя выявлять и предотвращать такие операции.

Использование традиционных методов анализа данных, таких как ручной контроль и проверка транзакций, не всегда эффективно в условиях большого объема данных. Поэтому автоматизация процесса анализа с помощью алгоритмов становится необходимым шагом.

Для банка важно:

* Соблюдение норм и стандартов по борьбе с отмыванием денег (AML), финансированием терроризма (CFT) и другими нормативами, установленными финансовыми регуляторами.
* Защита данных клиентов и предотвращение утечек информации.
* Обеспечение эффективности работы сотрудников, упрощение процессов анализа транзакций.

Проект позволяет в полной мере соответствовать требованиям законодательства и эффективно управлять рисками, связанными с подозрительными транзакциями. Внедрение этой системы способствует улучшению внутренней отчетности и повышению доверия клиентов банка к уровню защиты их данных.

# 2.3. Основные заинтересованные стороны (стейкхолдеры)

Руководство банка — заинтересовано в соблюдении нормативных актов и стандартах безопасности, а также в снижении рисков и финансовых потерь.

IT-отдел банка — отвечает за техническую реализацию проекта, интеграцию системы с существующими инфраструктурами банка и настройку алгоритмов.

Аналитики и специалисты по безопасности — используют систему для анализа транзакций, выявления рисков и составления отчетов для регуляторов.

Клиенты банка — конечные пользователи услуг, которые будут уверены в безопасности своих операций и данных благодаря внедрению системы.

Регуляторы (например, Центральный банк или другие финансовые контролирующие органы) — заинтересованы в том, чтобы банк соблюдал законы по борьбе с отмыванием денег и финансовыми преступлениями.

Поставщики внешних данных (например, службы по мониторингу санкционных списков или базы данных с информацией о мошенничестве) — внешние компании, предоставляющие данные для анализа.

Команда по защите данных — группа, которая будет контролировать соблюдение стандартов безопасности данных в процессе разработки и внедрения системы.

# 2.4. Ограничения и допущения

**Ограничения**:

1. Доступ к данным: система будет работать с данными, которые доступны из внутренней инфраструктуры банка и внешних источников. В случае ограниченного доступа к данным или их недостаточной полноте эффективность алгоритмов может снизиться.
2. Технические ограничения: алгоритм может не обеспечивать 100% точность, и потребуется периодическая доработка для улучшения качества классификации подозрительных операций.
3. Задержка в обработке данных: из-за большого объема транзакций может возникнуть задержка в обработке данных в реальном времени, что может повлиять на скорость реакции сотрудников банка.
4. Нормативные ограничения: система должна соответствовать нормативам, таким как GDPR №152-ФЗ, законодательно регулирующим обработку персональных данных. Это может ограничить доступ к определенным данным или методам их обработки.

**Допущения**:

1. Система будет интегрироваться с существующими банковскими информационными системами.
2. Интеграция с внешними источниками данных, такими как санкционные списки, будет выполняться с использованием стандартизированных API и протоколов, что облегчит процесс обновления и синхронизации данных.
3. Алгоритм для выявления подозрительных транзакций будет иметь возможность доработки с учетом возникающих угроз и изменений в поведении пользователей.
4. Программа будет использовать только те данные, которые были согласованы с соответствующими заинтересованными сторонами
5. Все юридические и нормативные обязательства, связанные с защитой данных, будут строго соблюдаться, включая соответствие системе AML/CFT.

# БИЗНЕС-ЦЕЛИ И ЗАДАЧИ

# 3.1. Описание бизнес-проблемы

В последние годы банки сталкиваются с ростом мошеннических операций и высокими рисками, связанными с отмыванием денег и финансированием терроризма. В условиях глобализации финансовых рынков и быстрого технологического прогресса, банки испытывают всё новые и новые вызовы. Мошенники становятся всё более изобретательными, а количество транзакций — растёт с каждым днём.

Традиционные методы мониторинга, которые включают ручную проверку и аналитические подходы, уже не справляются с этим объёмом данных и не всегда успевают реагировать на быстро меняющиеся угрозы. Процесс ручного контроля операций требует много времени и часто подвергает систему риску пропуска подозрительных действий. Когда количество операций увеличивается, вероятность ошибок возрастает, и, как результат, значительные угрозы могут быть не замечены. При этом, банки обязаны соблюдать строгие нормы и стандарты, такие как предотвращение отмывания денег (AML) и борьба с терроризмом (CFT), а также другие национальные и международные требования. Внедрение таких стандартов вручную становится трудным и неэффективным, что создаёт дополнительные сложности.

Поэтому, для эффективного анализа транзакций необходимы современные технологии. Без автоматизации и применения алгоритмического анализа, банк не сможет быть уверенным в своевременном выявлении рисков и их устранении. Решение этих проблем требует создания системы, которая будет отслеживать аномалии, автоматически и без ошибок.

# 3.2. Цель проекта

Цель проекта — разработать систему для автоматического выявления подозрительных транзакций, которые могут быть связаны с мошенничеством, отмыванием денег или финансированием терроризма.

Основной задачей является повышение безопасности банковских операций и минимизация упущенных угроз. Это также обеспечит соблюдение внутренних стандартов безопасности и требований регулирующих органов.

Для достижения этой цели будет разработан алгоритм, который на основе заданных критериев будет анализировать каждую транзакцию, выявлять отклонения и аномалии. Система будет интегрироваться с данными банка — информацией о клиентах, истории транзакций, географическими данными и данными о получателях переводов. Это позволит обеспечить комплексный анализ и формирование предупреждений о возможных рисках.

В рамках проекта будет создан веб-дашборд для удобной визуализации результатов анализа. Через этот интерфейс сотрудники банка смогут отслеживать подозрительные операции в реальном времени, оперативно принимать меры и проводить дополнительный анализ. Важным аспектом является создание интуитивно понятного интерфейса, который даст пользователям всю необходимую информацию для принятия решений.

Проект включает задачи обеспечения безопасности данных. Все транзакции и персональные данные клиентов будут защищены с применением современных методов шифрования и защиты от несанкционированного доступа.

# 3.3. Критерии успеха

Успех проекта будет оцениваться по нескольким ключевым критериям.

Во-первых, это точность работы алгоритма. Алгоритм должен минимизировать количество ложных срабатываний и при этом обнаруживать все подозрительные транзакции. Ожидаемая точность работы алгоритма — 95% и выше, что гарантирует надежность системы и минимизирует количество пропущенных операций.

Во-вторых, критерием успеха является производительность системы. Система должна справляться с большими объёмами данных, обрабатывая не менее 5 000 транзакций в день. Время обработки каждой транзакции должно быть минимальным, чтобы аналитики могли получать результаты в реальном времени без задержек.

Интеграция с существующими банковскими платформами и источниками данных также является важным показателем. Данные должны поступать в систему вовремя и в нужном формате, что обеспечит бесперебойную работу системы.

Пользовательский интерфейс веб-дашборда должен быть удобным и функциональным, чтобы сотрудники банка могли легко фильтровать и анализировать данные.

# ТРЕБОВАНИЯ К БИЗНЕС-ЗАДАЧЕ

# 4.1. Бизнес-требования

БТ1. Разработать алгоритм для обнаружения подозрительных транзакций на основе заданных критериев.

# 4.2. Бизнес-правила

БП1. Банковские операции на сумму более 100 000 рублей являются метрикой подозрительности.

БП2. Банковские операции в ночное время (с 00:00 до 06:00) являются метрикой подозрительности.

БП3. Резкое изменение геолокации (аномалии в перемещении клиента на расстояние более 500 км) является метрикой подозрительности.

БП4. Увеличение числа транзакций (если клиент совершает более 7 транзакций за последние 2 часа) является метрикой подозрительности.

БП5. Несколько попыток переводов денежных средств малыми (несколько транзакций в течение 1 часа от 1000 руболей, сумма транзакций 20000) являются метрикой подозрительности.

БП6. Неопознанные категории перевода являются метрикой подозрительности.

БП7. Переводы в "рискованные" страны являются метрикой подозрительности.

Б8. Если возраст клиента более 60 лет это является метрикой подозрительности.

БП9. Пользователь с ролью "Руководитель" имеет доступ к персональным данным клиента банка, пользователь с ролью "Сотрудник" такого доступа не имеет ".

БП10. Система должна соответствовать стандартам безопасности данных, принятым в банковской отрасли. Все данные, передаваемые и хранимые в системе, должны быть защищены с использованием шифрования и других современных технологий защиты. Применение таких стандартов, как GDPR и PCI DSS, обязательно.

# 4.3. Пользовательские требования

ПТ1. Информация о подозрительных транзакциях должна выводиться на веб-дашборд.

ПТ2. На дашборде должна выводиться таблица с подозрительными операциями (фильтры: дата, сумма, тип, статус) с полями: Номер транзакции, Клиент (ID/имя), Сумма и валюта, Дата и время, Категория операции, Статус (новые, проверенные, подтверждённые как мошенничество).

ПТ3. На дашборде должна выводиться оценка риска каждой транзакции.

ПТ4. "На дашборде должно выводиться причины подозрительности транзакции. Например список: "Необычное место", "Высокая сумма".

ПТ5. На дашборд должно быть несколько слоев.

ПТ6. "На дашборде работают пользователи с разными ролями: "Сотрудник", "Руководитель".

ПТ7. На дашборде должно выводиться количество транзакций за период (день/неделя/месяц).

ПТ8. На дашборде должно выводиться количество подозрительных транзакций в динамике.

ПТ9. На дашборде должна выводиться доля подозрительных операций.

ПТ10. На дашборде должна выводиться сумма подозрительных транзакций в рублях и в % от общего объема.

ПТ11. На дашборде должна выводиться таблица с подозрительными операциями, включая информацию по регионам.

ПТ12. На дашборде должны выводиться топ-5 подозрительных категорий (по количеству и сумме).

ПТ13. На дашборде должна выводиться география транзакций (карта с аномальными операциями).

ПТ14. На дашборде. должны выводиться временные аномалии (график по часам/дням).

ПТ15. На дашборде должна быть возможность экспорта данных в таблицу эксель.

# 4.3. Функциональные требования

ФТ1. Система должна обеспечивать функционал для обнаружения подозрительных транзакций, руководствуясь набором чётко прописанных бизнес-правил.

ФТ2. Дополнительно система должна иметь возможность генерировать и отображать отчёты на веб-дашборде. Отчёты должны содержать таблицы с фильтрацией по различным критериям, таким как статус транзакции (новая, проверенная, подтверждённая как мошенничество), сумма операции, категория операции и географические аномалии. Также нужно предусмотреть отображение динамики числа подозрительных транзакций, их доли и суммы как в абсолютных цифрах, так и в процентах от общего объёма операций банка.

ФТ3. Система должна определять подозрительность и уровень риска транзакции на основе сопоставления метрик подозрительности.

ФТ4. Система должна позволять настройку ролей для пользователей дашборда. Таким образом, у сотрудников с разными уровнями доступа будет возможность анализа данных в соответствии с их ролями.

# 4.4. Ограничения

Система должна работать в рамках существующих технических ограничений банка. Это означает, что интеграция с внутренними и внешними системами банка должна проходить без существенных изменений в архитектуре.

Если не удастся интегрировать какие-либо внешние источники данных, система должна предложить альтернативные методы получения нужной информации.

# БИЗНЕС-ПРОЦЕССЫ И СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

# 5.1. Описание текущих процессов

На данный момент в банке отсутствует регламентированный бизнес-процесс мониторинга подозрительных операций. Транзакции не подвергаются анализу в реальном времени. Данные о транзакциях фиксируются и сохраняются в хранилище данных банка.

# 5.2. Описание целевых процессов

Целевой бизнес процесс представляет из себя информационную систему для контроля подозрительных транзакций. Данные о транзакциях забираются из банка и размещаются на слой сырых данных. Из слоя сырых данных данные трансформируются и размещаются в ядро базы данных системы, далее они трансформируются на основе метрик определения подозрительных транзакций (бизнес правил) и формируют витрину данных, откуда попадают на дашборд. На дашборде происходит семантическая группировка и демонстрация данных, для дальнейшего анализа.

# 5.3. Основные сценарии использования (Use Cases)

# ПС1. Обновить данные через скрипт (ETL).

1. Системный аналитик запускает скрипт.
2. Система переносит данные из источника в витрину данных.

# ПС2. Авторизоваться в системе.

1. Пользователь вводит логин и пароль, нажимает кнопку войти.
2. Система авторизует пользователя.

# ПС3. Обновление данных источника данных.

1. Пользователь авторизуется в приложении DataLens.
2. Нажимает кнопку “Датасеты”.
3. Система открывает форму с датасетом.
4. Пользователь выбирает датасет и нажимает кнопку “Обновить поля”.
5. Система синхронизирует данные с базой данных.

# ПС4. Открыть дашборд.

# Пользователь авторизуется в приложении DataLens.

# Система открывает рабочее пространство.

# Пользователь нажимает кнопку “Дашборды” и выбирает дошборд.

# Система открывает выбранный дашборд.

**ПС5. Посмотреть общую статистику о подозрительных транзакциях.**

**Предусловие:** ПС4.

1. Пользователь нажимает на вкладку «Общая статистика».
2. Система отображает информацию об общей сумме подозрительных/обычных транзакций с разбивкой на графике по дням/неделям/месяцам.
3. Пользователь изменяет селекторы: период, детализация периода, метка подозрительности, категория операции.
4. Система перестраивает графики согласно выбранным селекторам.

**ПС6. Посмотреть сводную информацию о подозрительных транзакциях.**

**Предусловие:** ПС4.

1. Пользователь нажимает на вкладку «Анализ подозрительных транзакций».
2. Система отображает геоаналитику по транзакциям, тепловую карту распределения по часам, топ 10 подозрительных категорий.
3. Пользователь изменяет фильтры: тип операций, категория операции, чек бокс «операции в и скованных странах», единицы измерения диаграмм, выбирает промежуток времени.
4. Система перестраивает графики согласно выбранным селекторам.

**ПС7. Посмотреть детализацию транзакций**

**Предусловие:** ПС4.

1. Пользователь нажимает на вкладку «Детализация транзакций».
2. Система отображает таблицу детализации подозрительных транзакций с распределением.
3. Пользователь изменяет селектор: что выводить в таблице (сумму, количество среднюю оценку риска), тип анализа(категории, статусы), метку подозрительности, статусы риска, категории), регион.
4. Система строит таблицу согласно выбранным селекторам.
5. Пользователь нажимает кнопку экспорта.
6. Система экспортирует таблицу в формат xlsx.

**ПС8. Посмотреть детализацию причин подозрительности**

**Предусловие:** ПС4.

1. Пользователь нажимает на вкладку «Анализ причин подозрительности».
2. Система отображает тепловую карту распределения рисков по сегментам клиентов, таблицу причин подозрительности, таблицу причин подозритедьности по категориям.
3. Пользователь изменяет селекторы: метка подозрительности, категории операций, причины подозрительности, ограничения по возрасту.
4. Система перестраивает графики согласно выбранным селекторам.
5. Пользователь нажимает кнопку экспорта.
6. Система экспортирует таблицу в формат xlsx.

# ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ СИСТЕМАМИ

# 6.1. Описание интеграций

Система интегрируется в базу данных банка и получает из хранилища таблицы с данными клиентов, банковских счетов, банковских карт, транзакций.

Система интегрируется к стороннему сервису у которого получает актуальный список стран и городов, включая список рискованных стран.

Система интегрируется с приложением Yandex Datalens для вывода информации на дашборды.

# 6.2. Зависимости от внешних систем и сервисов

**DWH Банка**

* Тип: Обязательный
* Функция: Источник данных.

**DWH внутренняя (Сервер, PostgeSQL СУБД)**

* Тип: Обязательный
* Функция: Хранение и трансформация данных, формирование витрин

**Yandex DataLens**

* Тип: Обязательный
* Функция: Визуализация данных

# ОЦЕНКА РИСКОВ

# 7.1. Основные риски проекта

|  |  |  |
| --- | --- | --- |
| **Риск** | **Вероятность** | **Влияние на проект** |
| Недостаточная производительность системы | Средняя | Низкое |
| Проблемы с безопасностью данных | Средняя | Низкое |
| Изменение требований заказчика | Высокая | Высокое |
| Конфликты между стейкхолдерами. | Средняя | Среднее |
| Изменения на рынке (экономические кризисы, санкции) | Высокая | Высокое |

# 7.2. Меры по их снижению

**Риск: Недостаточная производительность системы.**

* Меры: Провести нагрузочное тестирование.
* Оптимизация запросов к БД.

**Риск: Проблемы с безопасностью данных.**

* Меры: Регулярные аудиты безопасности.

**Риск: Изменение требований заказчика.**

* Использовать Agile с короткими итерациями для своевременного выявления изменений.
* Регулярные демонстрации продукта заказчику (раз в 2 недели).

**Риск: Конфликты между стейкхолдерами.**

* Меры: Приоритезация требований от стейкхолдеров в зависимости от зоны ответственности.

**Риск: Изменения на рынке (экономические кризисы, санкции).**

Меры:Поиск альтернативных рынков сбыта.

# КРИТЕРИИ ПРИЕМКИ

Проект считается завершенным, когда выполнены **все** следующие условия:

1. **Реализация всех требований**
   * Все функциональные и нефункциональные требования из BRD реализованы и протестированы.
   * Нет критических багов (Severity 1 и 2) в финальной версии продукта.
2. **Подписание акта сдачи-приемки (АСП)**
   * Заказчик подтверждает соответствие продукта требованиям документации.
   * Все изменения (если были) задокументированы и согласованы.
3. **Завершение тестирования и аудита**

Проведены:

* + - Функциональное тестирование (QA-отчет, если требуется).
    - Нагрузочное тестирование (если требуется).
    - Security-аудит (для проектов с данными пользователей).

1. **Документация передана**

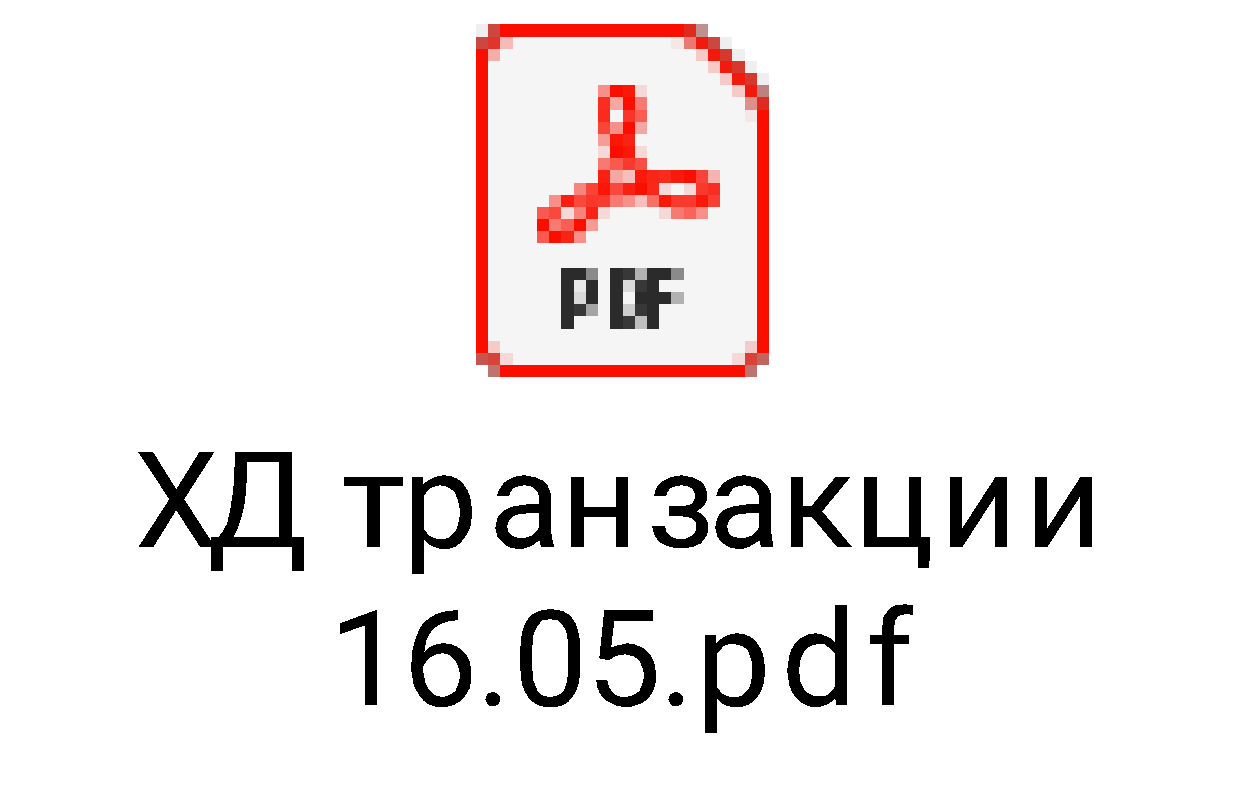
Переданы:

* + - BRD.
    - FSD.

1. **Обучение пользователей**
   * Проведены тренинг-сессии для ключевых стейкхолдеров.
2. **Финансовые и юридические аспекты**
   * Закрыты все финансовые обязательства (оплата, лицензии).

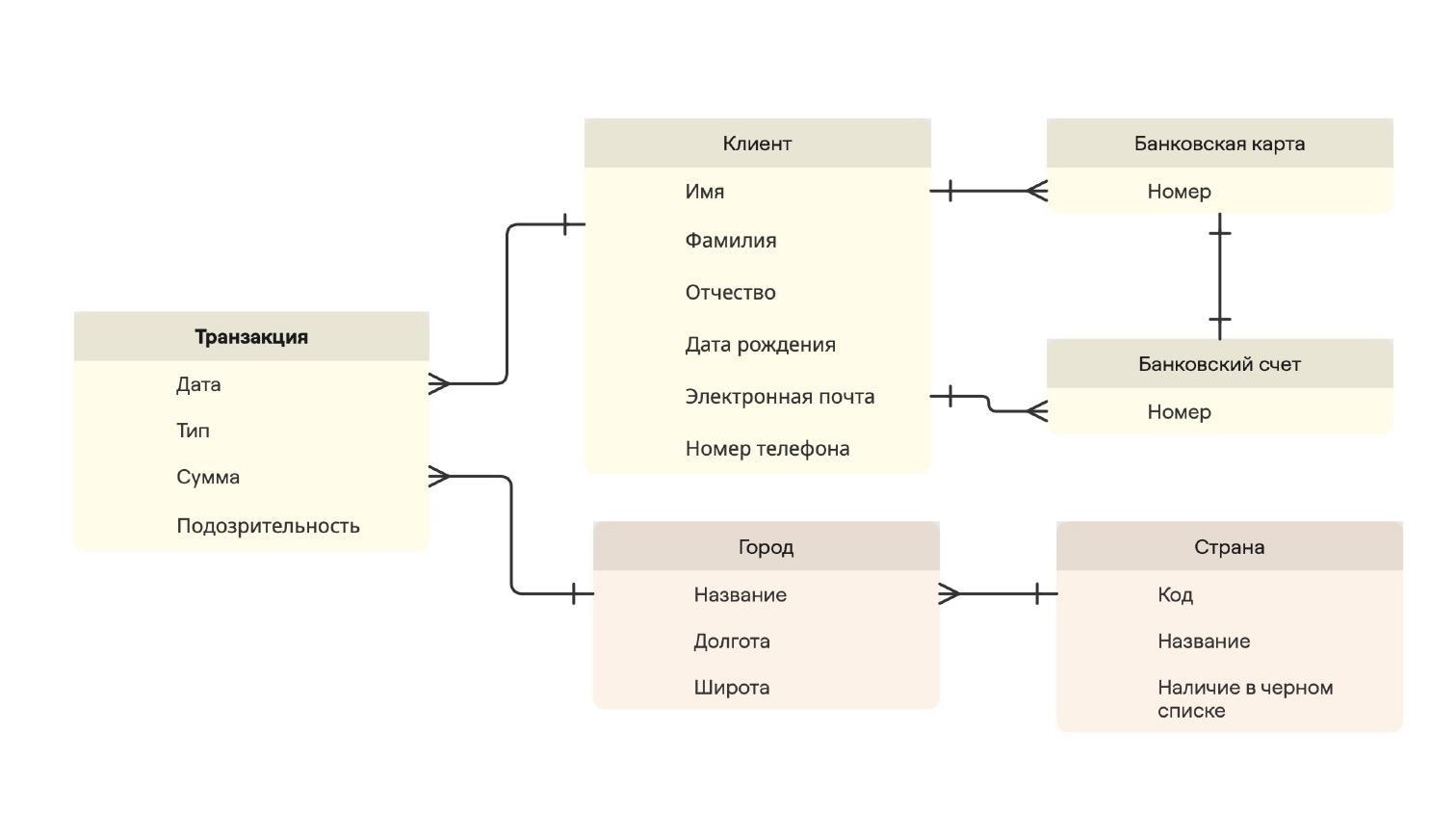
# ПРИЛОЖЕНИЯ

Приложение 1. BPMN Диаграмма бизнес процесса.

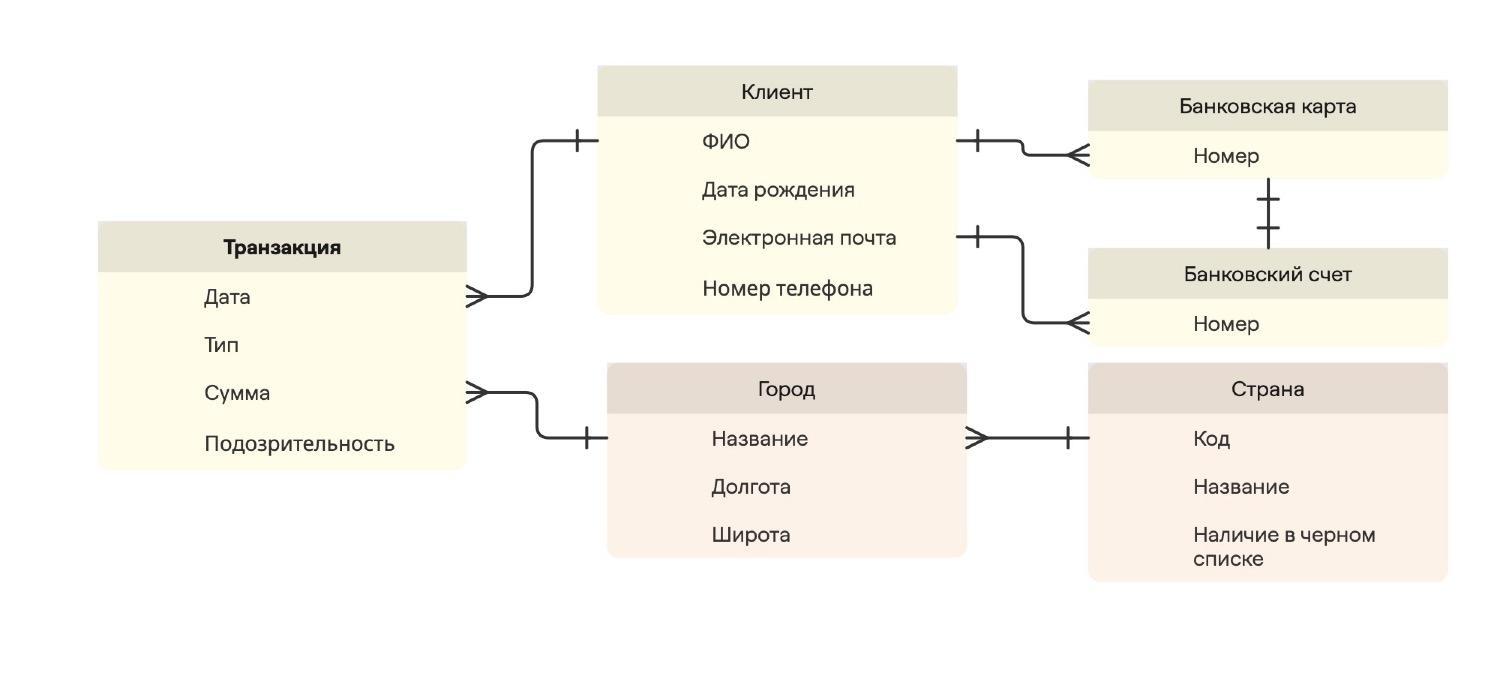


Приложение 2. Диаграмма сценариев использования

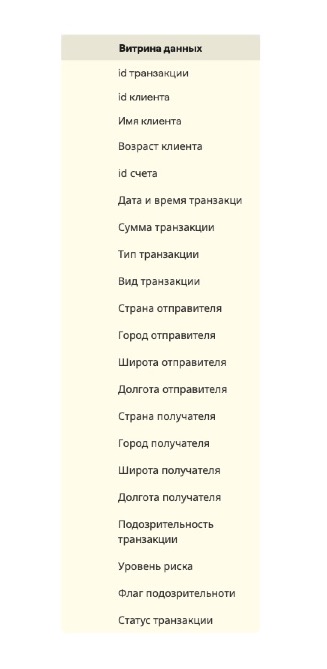
Приложение 3. Концептуальная диаграмма банк/стейджинг



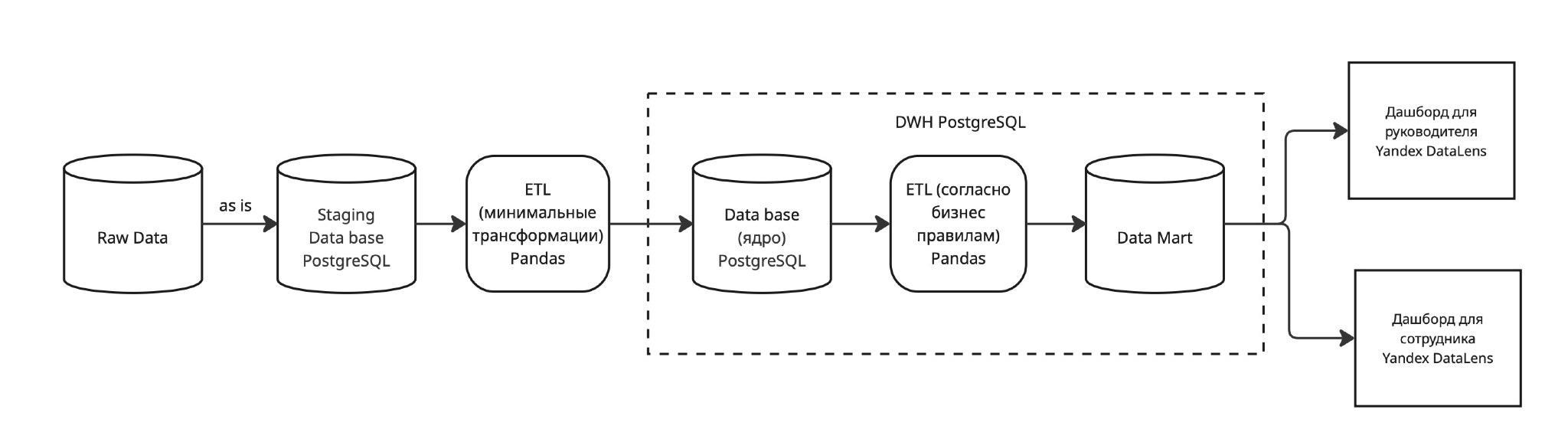
Приложение 3.2 Конценптуальная ER диаграмма ядра



Приложение 3.3 Конценптуальная ER витрины данных



Приложение 4. Архитектура



Приложение 4. Макеты дашборда

