«ПОДТВЕРЖДАЮ»
АКБ «Банк развития бизнеса»
Заместитель председателя правления:
О.Вохидов

«1» май 2026 г.
№ 354

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

«Разработка, внедрение и техническая поддержка мобильной банковской платформы «BRB» для физических лиц»

на 80 листах

действует с «____» _____2026 г.

СОГЛАСОВАНО
и.о. Директора департамента
Цифрового бизнеса
_____ Г. Мавланов
подпись

_____
дата

СОГЛАСОВАНО
Директор центра
Информационной безопасности
_____Б.Шамсиев
подпись

_____
дата

СОГЛАСОВАНО
Директор департамента
Информационных технологий
_____З. Орифхожаев
подпись

_____
дата

Ташкент – 2026 г.

Оглавление

Сокращения и определения

НИББД	Национальная информационная база банковских депозиторов
МП	Мобильная платформа — это программная среда (операционная система), обеспечивающая работу приложений на смартфонах и планшетах.
O'z DST	Государственный стандарт Республики Узбекистан
ТЗ	Техническое задание. Исходный документ на проектирование технического объекта, устанавливает основное назначение разрабатываемого объекта, его технические характеристики, предписание по выполнению необходимых стадий создания документации и её состав, а также специальные требования
ЕЭИСВО	Единая электронная информационная система внешнеторговых операций
СУБД	Система управления базами данных
Online	Состояние подключения к компьютерной сети, при котором пользователь имеет доступ к различным ресурсам и сервисам, таким как: интернет-сайты, электронная почта, онлайн-банкинг и т.д.
Пользователь	Пользователь информационной системы – это лицо (группа лиц, организация), пользующееся услугами информационной системы.
UzASBO	Автоматизированная система бюджетных организаций Узбекистана
USB-Token	Устройство-носитель ключевой информации, позволяющее упростить и обезопасить процедуру идентификации и аутентификации пользователя
RTO	Recovery Time Objective — целевое время восстановления; максимально допустимый промежуток времени, в течение которого система может оставаться недоступной в случае сбоя.
RPO	Recovery Point Objective — целевая точка восстановления; максимально допустимый период, за который могут быть потеряны данные (значение «0» означает требование полной сохранности данных за счет синхронной репликации).
SIEM	Security Information and Event Management — система управления событиями и информационной безопасностью, обеспечивающая анализ логов в реальном времени и оперативное оповещение об инцидентах.
MFA	Multi-Factor Authentication — многофакторная аутентификация; метод подтверждения доступа, требующий одновременного использования нескольких независимых факторов.
Device Binding	Механизм аппаратной привязки учетной записи пользователя к уникальным идентификаторам его мобильного устройства для защиты от несанкционированного доступа.
Root / Jailbreak	Наличие прав суперпользователя в операционной системе

	мобильного устройства, полученных в обход ограничений производителя, что критически снижает уровень безопасности.
RBAC	Role-Based Access Control — управление доступом на основе ролей; метод ограничения прав доступа, при котором полномочия назначаются в соответствии с должностными обязанностями.
PCI DSS	Payment Card Industry Data Security Standard — международный стандарт безопасности данных индустрии платежных карт, обязательный при хранении, обработке или передаче карточных данных.
PAN Masking	Маскирование номера карты; технология скрытия части цифр номера карты при их отображении в интерфейсах или печати в чеках.
HSM	Hardware Security Module — аппаратный модуль безопасности; устройство, предназначенное для защищенного выполнения криптографических операций и физически изолированного хранения мастер-ключей шифрования.
KMS	Key Management Service — система или сервис управления жизненным циклом криптографических ключей (генерация, хранение, ротация).
DLP	Data Loss Prevention — системы предотвращения утечек информации; программные средства, контролирующие передачу конфиденциальных данных за пределы защищенного контура.
OWASP	Open Web Application Security Project — международная организация, формирующая стандарты безопасности и перечни наиболее критических уязвимостей (OWASP Top 10).
Secure SDLC	Secure Software Development Life Cycle — безопасный жизненный цикл разработки ПО; методология, включающая контроль безопасности на каждом этапе создания продукта.
SAST	Static Application Security Testing — статическое тестирование безопасности; анализ исходного кода приложения на наличие уязвимостей без его запуска.
DAST	Dynamic Application Security Testing — динамическое тестирование безопасности; проверка работающего приложения на наличие уязвимостей путем имитации внешних атак.
Sonar Qube (Sonar)	Платформа для непрерывного контроля качества и безопасности программного кода, выполняющая его автоматический анализ.
Quality Gates	Набор пороговых критериев (процент тестов, отсутствие багов), выполнение которых необходимо для выпуска программного обеспечения.
Docker	Технология упаковки программного обеспечения в изолированные контейнеры, гарантирующая идентичность работы кода в разных средах.
Kubernetes	Открытая платформа для автоматизации развертывания, масштабирования и управления контейнеризированными

	приложениями (оркестрация)
Change Management	Процесс управления изменениями; регламентированная процедура внесения корректировок в систему с целью минимизации рисков для её стабильности.
Supply-chain risk	Риски цепочки поставок; угрозы безопасности, возникающие из-за использования сторонних компонентов, библиотек или сервисов внешних поставщиков.
IRP	Incident Response Plan — формализованный план действий технического персонала по обнаружению, локализации и ликвидации последствий инцидентов безопасности.

ОБЩИЕ СВЕДЕНИЯ

Настоящее Техническое задание на реализацию проекта «Разработка, внедрение и техническая поддержка мобильной банковской платформы «BRB» для физических лиц» разработано в соответствии с Государственным стандартом Республики Узбекистан O‘zDSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы».

1.1. Полное наименование МП и ее условное обозначение

Полное наименование проекта: «Разработка, внедрение и техническая поддержка мобильной банковской платформы «BRB».

Условное обозначение проекта: Мобильная платформа.

Краткое наименование системы, принятое в настоящем ТЗ: МП, Платформа, Система.

1.2. Наименование организации заказчика

Заказчик: Акционерный коммерческий банк «Банк развития бизнеса» (далее Заказчик). Адрес: 100011, г. Ташкент, Шайхантахурский р-н, ул. Навои, д. 18А.

Тел: +998 (78) 150-10-01

e-mail: headoffice@brb.uz

Web-site: https://brb.uz/

Исполнитель: «Исполнитель» разработки МП будет определен по результатам отбора наилучших предложений

Для выполнения отдельных работ Разработчик МП может привлекать другие организации в качестве соисполнителей, при обязательном согласовании с Заказчиком.

1.3. Перечень документов, на основании которых создается МП

Основанием для реализации Проекта являются следующие документы:

1. Постановление Президента Республики Узбекистан от 23.03.2018 г. №ПП-3620 "О дополнительных мерах по повышению доступности банковских услуг".
2. Решение Правления АКБ «Кишлок курилиш банк» №24 от 17 декабря 2019 года об утверждении «Дорожной карты по цифровизации услуг путём внедрения информационных технологий в системе АКБ «Кишлок курилиш банк»
3. Закон Республики Узбекистан от 01.11.2019 г. №ЗРУ-578 «О платежах и платежных системах» (Принят Законодательной палатой 19.09.2019 г., одобрен Сенатом 11.10.2019 г.);

4. Постановление Президента Республики Узбекистан №ПП-306 от 14.09.2023г.

«О мерах финансовой и институциональной поддержки развития малого бизнеса».

5. Постановление Президента Республики Узбекистан №ПП-3270 от 12.09.2017 г. «О мерах по дальнейшему развитию и повышению устойчивости банковской системы Республики Узбекистан»;
6. Постановление Президента Республики Узбекистан №ПП-3620 от 23.03.2018г. «О дополнительных мерах по повышению доступности банковских услуг»;
7. Постановление Президента Республики Узбекистан №ПП-2751 от 02.02.2017 г. «О мерах по созданию благоприятных условий для дальнейшего развития в республике системы безналичных расчетов на основе банковских пластиковых карточек»;
8. Постановление Президента Республики Узбекистан №ПП-4699 от 28.04.2020 года «О мерах по широкому внедрению цифровой экономики и электронного правительства»;
9. Указ Президента Республики Узбекистан №УП-5992 от 12.05.2020 года «О Стратегии реформирования банковской системы Республики Узбекистан на 2020 — 2025 годы»;
10. Постановление Правления Центрального Банка Республики Узбекистан «Об утверждении положения о защите информации в автоматизированных системах коммерческих банков Республики Узбекистан» (зарегистрировано Министерством юстиции Республики Узбекистан 10 марта 2020 г. Регистрационный №3224);
11. Решение Правления АКБ «Банк развития бизнеса» №-175 от 16.09.2024г.
12. Техническая документация на реализацию Проекта разрабатывается на основании: Постановления Президента Республики Узбекистан №ПП-4328 от 21.05.2019 года «О мерах по повышению качества разработки и реализации проектов в сфере информационно-коммуникационных технологий в рамках системы «Электронное правительство»

1.4. Плановые сроки начала и окончания работ по созданию МП

Реализация проекта должна осуществляться в несколько стадий:

1 стадия– проектирование;

2 стадия – разработка;

3 стадия – тестирование;

4 стадия – запуск в эксплуатацию.

Предварительные сроки начала и окончания работ должны быть согласованы с Разработчиком Системы на этапе согласования проекта и подготовки Договора на реализацию проекта. Окончательные сроки должны быть указаны в календарном плане работ в Договоре на реализацию проекта.

1.5. Порядок оформления и предъявления Заказчику результатов работ

Работы по внедрению Системы сдаются Разработчиком поэтапно в соответствии с календарным планом проекта. По окончании каждого из этапов работ Разработчик сдает Заказчику соответствующие отчетные документы этапа, состав которых определяется Договором в рамках реализации данного проекта. Приемка отдельных этапов работ должна производиться согласно этапам календарного плана работ, утвержденного Заказчиком и Разработчиком, и являющимся неотъемлемой частью Договора. По всем работам необходимо указать длительность выполнения работ, а также общую стоимость для каждой выполняемой работы.

В случае, если в процессе выполнения работ потребуется детализация и согласование Заказчиком и Разработчиком отдельных вопросов и решений, не отраженных (или отраженных недостаточно детально) в настоящем ТЗ, Заказчик может разработать и согласовать с Разработчиком следующие документы, которые будут являться частью данного документа:

частное ТЗ;

изменения к ТЗ;

дополнения к ТЗ.

Датой сдачи – приемки работ считают дату подписания акта Приемочной комиссией.

Оформление результатов работ должно соответствовать требованиям, изложенным в следующих нормативных документах:

1. O’z DST 1985:2018 Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем;

2. O’z DST 1986:2018 Информационная технология. Информационные системы. Стадии создания;

3. O’z DST 1987:2018 Информационная технология. Техническое задание на создание информационной системы

4. Постановление Правления Центрального банка Республики Узбекистан № 3030 от 02.07.2018 г. «Об утверждении Положения о минимальных требованиях к деятельности

коммерческих банков при осуществлении взаимоотношений с потребителями банковских услуг»

5. Постановление Правления Центрального банка Республики Узбекистан № 3759 от 21.01.2026 г. «Об утверждении Положения о минимальных требованиях по обеспечению информационной и кибербезопасности, а также предупреждению случаев фрода при оказании дистанционных финансовых услуг физическим лицам кредитными и платежными организациями, операторами платежных систем»

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

2.1. Назначение МП

Мобильная банковская платформа «BRB» для физических лиц предназначена для предоставления физическим лицам как клиентам АКБ «Банк развития бизнеса», таки и не-клиентам Банка комплексного, круглосуточного и безопасного доступа к полному спектру банковских, финансовых и сопутствующих нефинансовых услуг Банка через удаленные каналы обслуживания (смартфоны и планшеты).

Основное назначение МП заключается в следующем:

Для клиентов Банка (физических лиц): Предоставление комплексного, круглосуточного и безопасного доступа ко всем банковским продуктам (счета, карты, кредиты, депозиты) и дистанционному управлению финансами в режиме 24/7.

Для не-клиентов Банка (потенциальных пользователей): Привлечение новой аудитории через предоставление открытого нефинансового сервиса и базового платежного функционала (оплата коммунальных услуг, мобильной связи, переводы на карты других банков), с возможностью быстрой удаленной регистрации (онбординга) и открытия первого счета.

Для Банка: Создание ключевого, высокоэффективного канала продаж и обслуживания, способного масштабировать клиентскую базу и снижать операционную нагрузку на физическую сеть отделений.

Мобильное приложение для физических лиц является стратегическим инструментом для трансформации АКБ «Банк развития бизнеса» в ведущий цифровой банк Узбекистана.

2.2. Цели создания МП

Создание Мобильной банковской платформы «BRB» для физических лиц преследует следующие стратегические, бизнес- и операционные цели. Все цели являются измеримыми

и должны быть достигнуты в ходе реализации проекта. Основные измеримые цели при разработке данного приложения:

Рост клиентской базы и проникновение на рынок.

Привлечь новых пользователей, в том числе не-клиентов, предлагая удобные открытые сервисы, с последующим их переводом в статус активных клиентов Банка.

Увеличение ежемесячного числа активных пользователей (MAU) на ≥40% в первый год. Увеличение числа новых счетов, открытых через МП на ≥60%.

Увеличение цифровых продаж и кросс-продаж.

Установление мобильного приложения как основного канала для реализации банковских продуктов (кредитов, депозитов, карт), используя персонализированные предложения и механизмы скоринга. Доля цифровых продаж (оформленных через МП) должна достигнуть ≥50% от общего объема продаж физлицам. Рост среднего количества продуктов на 1 активного пользователя (PPU) на ≥0.5 единицы.

Оптимизация операционной эффективности.

Минимизировать транзакционные издержки и нагрузку на контакт-центр и физические отделения за счет полной автоматизации стандартных запросов и операций.

Снижение операционных расходов на обслуживание 1 клиента в месяц на ≥20% в течение 18 месяцев. Снижение числа запросов в контакт-центр, связанных с проверкой баланса/статуса платежа, на ≥70%.

Соответствие регуляторным требованиям.

Обеспечить полное соответствие системы законодательству Республики Узбекистан в области ИТ-безопасности, защиты персональных данных и удаленной идентификации (KYC/AML). Отсутствие критических замечаний при аудите со стороны регулятора в первый год эксплуатации. Обеспечение 100% прохождения верификации через систему биометрической идентификации.

Полная адаптация функционала и архитектуры системы к требованиям информационной и кибербезопасности, установленным Постановлением ЦБ РУз № 3759, что включает внедрение методов защиты от несанкционированного доступа и предотвращения фрод-операций.

Реализация инструментов «клиентского добровольного запрета» на кредитование и гибкого управления лимитами, что позволяет пользователю выступать активным участником обеспечения безопасности своих средств.

Создание интеллектуального мониторинга транзакций, которое поможет в режиме реального времени выявлять нетипичное поведение системы и предотвращать вывод средств на сторонние счета при признаках компрометации устройства.

Создание удобного и эффективного пользовательского опыта (UX).

Разработать высокопроизводительное, надежное и интуитивно понятное приложение, обеспечивающее высокую скорость транзакций и стабильность работы в соответствии с мировыми стандартами. Достижение среднего рейтинга МП в App Store и Google Play на уровне ≥4.7 балла. Снижение времени на выполнение ключевой операции (P2P-перевод) до ≤5 секунд.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Объектом информатизации является АКБ «Банк развития бизнеса» и его существующая информационная инфраструктура, бизнес-процессы и клиентская база физических лиц, которые будут охвачены и трансформированы в результате внедрения Мобильного приложения для физических лиц.

Акционерный коммерческий банк «Банк развития бизнеса» начал свою деятельность в соответствии с Постановлением Кабинета Министров Республики Узбекистан № 311 от 20.06.1994 года как Республиканский специализированный акционерно-коммерческий «Галлабанк», а со 2 августа 1994 года Центральный Банк Республики Узбекистан выдал Генеральную лицензию №45 на оказание банковских услуг.

Согласно решению Президента Республики Узбекистан № ПП-1083 от 30 марта 2009 года на базе Галлабанка был преобразован в АКБ «Кишлок курилиш банк».

Постановлением Президента Республики Узбекистан №292 от 04.09.2023г. АКБ «Кишлок курилиш банк» преобразован в Акционерный коммерческий банк «Банк развития бизнеса».

Юридический адрес банка: индекс 100011, г.Ташкент, Шайхонтохурский район, улица А.Навои, дом 18А.

Основные направления деятельности банка направлены на финансирование проектов субъектов малого предпринимательства и оказание им комплексных услуг.

Кроме того, населению предоставляются все виды розничных банковских услуг. В частности, через 40 сервисных офисов, расположенных по всей республике, предоставляются такие услуги, как автокредитование, ипотека, микрозайм, обмен валюты, банковские карты, кассовая практика, международные денежные переводы.

Основными задачами Банка являются:

кредитно-банковское обслуживание населения и юридических лиц;

услуги по кредитованию и лизингу специализированных подрядных организаций, занимающихся строительством и ремонтом многоквартирных домов, производственной и социальной инфраструктуры;

кредитование и оказание комплексных банковских услуг предприятиям всех форм собственности, производящих новые современные строительные материалы и конструкции, внедряющих промышленные и сборные технологии для строительства объектов на территории по утвержденным типовым проектам;

В соответствии с действующим законодательством Банк осуществляет следующие операции:

привлечение средств во вклады;

осуществление платежей, в том числе без открытия банковских счетов;

открытие и ведение банковских счетов физических и юридических лиц, в том числе корреспондентских счетов банков;

операции с иностранной валютой в наличной и безналичной формах;

инкассо и кассовое обслуживание;

выдают гарантии и принимают другие обязательства от имени третьих лиц, обеспечивая выполнение ими своих обязательств;

получение права требовать от третьих лиц исполнения денежных обязательств (факторинг);

выпуск, покупка, продажа ценных бумаг, их учет и хранение, управление ценными бумагами по договору с клиентом, совершение иных операций с ними;

купля-продажа аффинированных драгоценных металлов, в том числе ведение счетов хранения металлов и приватизированных (нефизических) счетов металлов;

купля-продажа монет из драгоценных металлов;

осуществление операций с производными финансовыми инструментами (деривативами);

аренда специальных помещений для хранения документов или ценностей или сейфов внутри них;

лизинг;

кредитование в формах, предусмотренных законодательством;

оказание консультационных услуг по финансовым операциям;

управление активами (портфелем);

выпуск, использование и оплата электронных денег;

выпуск и процессинг банковских карт, обслуживание банковских карт в сотрудничестве с другими организациями, в том числе с другими финансовыми учреждениями.

Существующие информационные системы Банка

На сегодняшний день в Банке используются следующие информационные системы:

№	НАЗВАНИЕ СИСТЕМЫ	ОПИСАНИЕ
Внутренние системы		
1.	IABS	Автоматизированная банковская система Заказчика
2.	Центр сертификации	Система управления сертификатами безопасности при обмене с расчетно-кассовыми центрами
3.	Корпоративный интернет банкинг	Онлайн-банк для юридических лиц
4.	Процессинг центр Card suite	Процессинг центр карт VISA

Внешние системы (в составе IABS)		
5.	НИББД	Национальная информационная база банковских депозиторов
6.	Система НИКИ	Система Национального Института Кредитной Информации
7.	АСОКИ	Автоматизированная система обмена кредитной историей. База кредитного бюро
8.	Залоговый реестр	Система ГУП Залоговый реестр РУз
9.	ЕЭИСВО	Единая электронная информационная система внешнеторговых операций

Мобильная платформа будет автоматизировать и цифровизировать следующие группы процессов, которые в настоящее время могут выполняться через отделения или менее удобные цифровые каналы:

Процессы онбординга: Удаленная идентификация (через систему биометрической идентификации), открытие счетов и выпуск виртуальных карт (полностью в МП).

Операционные процессы: P2P-переводы, оплата услуг, управление картами (блокировка, PIN-код), обмен валют (согласно Модулю «Переводы P2P»).

Кредитно-депозитные процессы: Подача онлайн-заявок на кредиты и депозиты, мониторинг их статуса.

Взаимодействие с государственными сервисами: Обеспечение доступа к ключевым государственным услугам и платежам (через интеграцию с «MyGov»).

Внедрение МП потребует тесной интеграции со следующими ключевыми элементами существующей ИТ-инфраструктуры Банка:

Автоматизированная Банковская Система (IABS): Основной источник информации о счетах, остатках и клиентских данных. Все финансовые транзакции, инициированные в МП, должны быть финализированы в АБС.

Процессинговый центр: Системы, управляющие эмиссией, авторизацией и обработкой транзакций по картам HUMO, Uzcard и Visa/Mastercard.

Системы безопасности (Бэкэнд): Серверы авторизации, шифрования и хранения персональных данных.

Модуль «Интеграции» (API-шлюзы): Специализированные API для взаимодействия с внешними системами: Paynet, OFD, SMS провайдерами и др.

4 ТРЕБОВАНИЯ К МОБИЛЬНОЙ ПЛАТФОРМЕ

4.1 Требования к МП в целом

4.1.1 Требования к структуре и функционированию МП

Архитектура

Вся информационная система мобильной платформы для физических лиц, включая ключевые API-шлюзы и сервисы бизнес-логики построена на микросервисной архитектуре. Данное решение является очень важным для обеспечения высокой масштабируемости системы под растущую базу пользователей и транзакционную нагрузку. Оно гарантирует отказоустойчивость (изоляцию сбоев) и позволяет проводить независимое развертывание и обновление отдельных компонентов, минимизируя простои и риски.

Стек разработки Backend:

Основной стек разработки всех backend-компонентов (микросервисы бизнес-логики) должен быть реализован с использованием последних, актуальных и производительных фреймворков.

DevOps и Инфраструктура:

Архитектура должна быть модульной, слабо связанной и предусматривать возможность дальнейшего расширения приложения. Это означает, что добавление новых независимых микросервисов (например, для запуска новых продуктов, модулей или B2B-сервисов) должно происходить без необходимости внесения изменений в базовое ядро системы.

Приложение должно быть разработано и поддерживать обе основные на сегодняшний день мобильные платформы: iOS (начиная с версии 15) и Android (начиная с версии 7).

Для достижения максимальной производительности, безопасности и нативного пользовательского опыта предпочтение отдается нативным языкам разработки

(Swift/Kotlin) или высокопроизводительным кроссплатформенным решениям, обеспечивающим компиляцию в нативный код.

Производительность и Отклик (User Experience):

Время выполнения ключевых операций, таких как P2P-перевод, вход в систему и загрузка истории транзакций, не должно превышать 3 секунд при стабильном интернет-соединении. Это обеспечивает высокий уровень удовлетворенности пользователя.

Система должна быть спроектирована с учетом обработки пиковых нагрузок и обеспечивать стабильную работу при заданном количестве одновременных активных пользователей, согласно утвержденной технической спецификации.

Базы данных и Хранение Данных:

Для операций, требующих высокой целостности и надежности (счета, балансы, транзакции), должна использоваться реляционная СУБД (например, PostgreSQL или аналогичные).

Для некритических данных, требующих высокой скорости чтения/записи (логи, кэш, сессии, динамические настройки), должны быть использованы высокоскоростные NoSQL-решения (например, Redis).

Конфиденциальные данные (токены, ключи, биометрия) должны храниться исключительно в защищенных хранилищах мобильных операционных систем (KeyChain для iOS, Keystore для Android).

Система должна иметь возможности развития и модернизации по следующим направлениям:

Увеличение количества пользователей;

Увеличение объёма сохраняемых данных;

Расширение функциональных возможностей для обеспечения потребностей пользователей Системы, включая доработки силами Заказчика;

Изменение (дополнение и расширение) форматов и протоколов обмена данными;

Адаптация к изменениям норм законодательства и, соответственно, автоматизируемых процессов.

API и Стандарты Взаимодействия:

Все внутренние и внешние API должны строго соответствовать принципам RESTful API и использовать формат передачи данных JSON.

В качестве транспортного протокола для всех транзакционных вызовов должен использоваться протокол HTTPS с актуальной версией TLS 1.3 для обеспечения шифрования данных.

Пользовательские интерфейсы Системы должны быть разработаны с учетом фирменного стиля АКБ «Банк развития бизнеса» и требований эргономики для обеспечения интуитивно понятного клиентского пути.

Пользовательский интерфейс Системы должен быть реализован на узбекском, русском, английском и китайском языках. Переводы должны быть согласованы с представителями АКБ «Банк развития бизнеса».

Порядок проведения тестирования мобильного приложения

Тестовая среда и покрытие: Тестирование проводится на реальных устройствах, используемых пользователями. Обязательно покрытие операционных систем iOS (начиная с версии 15.0) и Android (начиная с версии 7.0 и выше).

Нормативное соответствие: Методика испытаний и Программа и методика испытаний (ПМИ) должны быть разработаны в соответствии с требованиями O‘zDSt 1985:2018 (требования к документации).

Тестирование интеграций: Особенное внимание должно быть уделено тестированию интеграций с национальными платежными системами Uzcard и Humo, а также с ИАБС и Центром обработки данных Банка.

Пентестинг: Обязательным является проведение независимого Penetration Testing (пентеста) со стороны сертифицированной организации, что подтверждает соответствие требованиям информационной безопасности, предъявляемым к финансовым учреждениям РУз.

Мобильная платформа для физических лиц должно поддерживать механизм автоматического обновления через официальные магазины приложений. Бэкэнд-система должна включать централизованную систему мониторинга (доступную через Модуль 7 «Администрирование») для отслеживания ошибок, производительности и анализа нагрузки в режиме реального времени.

Также будет проведено тестирование системы на разных типах устройств: смартфоны и планшеты. Тестирование будет включать проверку интерфейса на операционных системах Android и iOS, а также на устройствах с различными разрешениями экрана. Это необходимо для обеспечения того, чтобы интерфейс оставался удобным и функциональным вне зависимости от используемого устройства.

В целях улучшения пользовательского опыта, в рамках тестирования будет проведена проверка стабильности работы интерфейса при переходах между различными устройствами, а также кроссплатформенная совместимость на уровне всех поддерживаемых платформ. Это гарантирует, что интерфейс будет стабильным и отзывчивым, соответствуя ожиданиям пользователей при работе с системой на разных

устройствах и в различных условиях.

Меры защиты на уровне кода

Для предотвращения атак на уровне API и приложения применяются следующие меры:

Угроза	Механизм защиты и предотвращения
Rate Limit	Внедрение контроля частоты запросов на уровне API Gateway для всех конечных точек (endpoints), особенно для запросов на вход/регистрацию и отправку OTP
LFI/Path Traversal	Строгая валидация и очистка всех входных данных, поступающих от пользователя. Использование "белых списков" (whitelisting) допустимых символов и отключение прямого доступа к файловой системе через входные параметры.
XXE/Big XML (Billion Laughs)	Если используется XML, необходимо отключить обработку внешних сущностей (external entities) и ограничить лимит размера XML-документа, передаваемого в запросе. Предпочтительно использовать JSON.
RCE/Template/Expression	Использование безопасных шаблонизаторов и строгая изоляция среды выполнения. Отказ от использования функций, позволяющих выполнение произвольного кода, на основе пользовательского ввода.
Аутентификация API	Все API-запросы защищены токенами (JWT) с проверкой их валидности, срока действия и подписи.
SQL-инъекции	Использование параметризованных запросов (Prepared Statements) во всех взаимодействиях с базой данных.

Интеграция с SIEM, FIM и DAM

Для обеспечения всеобъемлющего контроля, проактивного выявления угроз и соблюдения регуляторных требований Республики Узбекистан в области информационной безопасности финансового сектора, предусматривается обязательная интеграция разработанной ИС со следующими корпоративными системами безопасности и мониторинга:

SIEM (Security Information and Event Management) — Управление событиями безопасности

Назначение: Система SIEM предназначена для централизованного сбора, корреляции, анализа и хранения всех событий, генерируемых приложением и его инфраструктурой. Это ключевой инструмент для проактивного обнаружения инцидентов и реагирования на них в режиме реального времени.

Требования к интеграции:

Критические события: Все события, имеющие отношение к безопасности и финансовым операциям, должны быть стандартизированы и переданы в SIEM-систему Банка. К ним относятся:

Все успешные и неуспешные попытки аутентификации.

Срабатывания механизмов Rate Limit и других средств защиты.

Инициация, успешное выполнение и отмена всех финансовых транзакций.

Изменения в настройках безопасности клиента (например, смена пароля или привязка устройства).

Механизм передачи: Логи передаются в режиме реального времени по защищенному протоколу (например, Syslog over TLS) для обеспечения конфиденциальности и целостности данных аудита.

FIM (File Integrity Monitoring) — Мониторинг целостности файлов

Назначение: FIM-система обеспечивает непрерывный контроль за целостностью критически важных файлов на серверах Бэкенда. Это необходимо для обнаружения несанкционированных модификаций или внедрения вредоносного кода.

Требования к контролю:

Объекты мониторинга: Под постоянным мониторингом должны находиться:

Исполняемые файлы (бинарники) приложения.

Ключевые конфигурационные файлы (включая настройки подключения к АБС и платежным системам).

Системные библиотеки, используемые Бэкендом.

Реагирование: При обнаружении любых изменений (добавление, удаление, изменение атрибутов или хэш-сумм файлов) FIM должен немедленно оповещать службу ИБ, что позволяет оперативно реагировать на потенциальный взлом или саботаж.

DAM (Database Activity Monitoring) — Мониторинг активности базы данных

Назначение: DAM-система необходима для независимого и гранулярного аудита всех действий, происходящих непосредственно на уровне базы данных, особенно тех, которые совершаются, минуя прикладную логику ИС (например, прямые запросы администраторов БД).

Требования к аудиту и соответствию нормам:

Контроль привилегированных пользователей: Обязательному логированию подлежат все запросы, выполненные администраторами БД и разработчиками, имеющими привилегированный доступ.

Мониторинг чувствительных данных: В режиме аудита фиксируются все операции SELECT, INSERT, UPDATE, DELETE, затрагивающие таблицы, содержащие

персональные данные клиентов (ПИНФЛ, паспортные данные) и финансовую информацию.

Соблюдение законодательства РУз: Внедрение DAM является критически важным для исполнения внутренних политик Банка и соблюдения требований законодательства о банковской тайне и защите персональных данных граждан Республики Узбекистан, обеспечивая неотвратимость аудита доступа к конфиденциальной информации.

4.1.1.1 Перечень подсистем, их назначение и основные характеристики

Структура Мобильной платформы «BRB» для физических лиц представляет собой совокупность взаимосвязанных функциональных модулей, каждый из которых отвечает за определенный блок банковских и нефинансовых услуг.

Основная структура мобильной платформы «BRB» для физических лиц должна включать в себя следующие подсистемы и модули:

1. Подсистема «Мой профиль»
2. Подсистема «Услуги»
3. Подсистема «Оплата»
4. Модуль «Переводы»
5. Модуль «Мониторинг»

1. Подсистема «Мой профиль».

Назначение подсистемы: предоставление пользователю платформы инструментов для управления личным кабинетом, настройки параметров безопасности и доступа к информационным сервисам Банка.

Основные характеристики:

индивидуальная настройка профиля и актуализация персональных данных;

управление механизмами защиты: смена кодов доступа и биометрическая идентификация. В рамках модернизации подсистемы предусмотрено внедрение обязательной защиты от несанкционированного копирования данных экрана (FLAG_SECURE);

оперативное информирование через модуль «Уведомления», архитектура которого будет переработана для исключения любых уязвимостей типа SQL-инъекций;

информационная поддержка: актуальные курсы валют, данные фондового рынка, поиск ближайших филиалов и банкоматов на карте;

клиентская поддержка через встроенный AI-чат и доступ к нормативным документам (оферта, сведения о приложении).

2. Подсистема «Услуги»

Назначение подсистемы: дистанционное предоставление банковских продуктов и интеграция с государственными цифровыми платформами.

Основные характеристики:

полноценный цикл управления кредитами и депозитами: от открытия и конверсии валют до мониторинга кредитной безопасности через КАТМ;

выпуск и обслуживание широкой линейки карт: виртуальных, зарплатных, международных и карт моментальной выдачи;

современные способы расчетов, включая QR-оплату и бесконтактные технологии;

интеграция с порталом My.gov.uz и сервисами для автовладельцев.

техническое сопровождение подсистемы гарантирует «атомарность» всех операций: финансовые транзакции будут защищены от сбоев, что исключит риск частичного списания или потери данных.

3. Подсистема «Оплата»

Назначение подсистемы: организация удобного интерфейса для проведения мгновенных платежей в пользу поставщиков различных услуг и государственных органов.

Основные характеристики:

поддержка широкого спектра оплат: от мобильной связи и коммунальных платежей до образовательных услуг и страхования;

специализированные разделы для оплаты штрафов ГАИ, государственных пошлин и услуг через электронные кошельки;

возможность погашения кредитов и пополнения счетов онлайн-сервисов;

4. Модуль «Переводы»

Назначение модуля: обеспечение быстрых и безопасных денежных переводов между собственными счетами пользователя и в адрес других получателей.

Основные характеристики:

внутрибанковские и межбанковские переводы с сохранением истории недавних операций для упрощения повторных транзакций;

функционал запроса денежных средств у сторонних пользователей;

для повышения надежности вводится обязательный контроль корректности вводимых номеров карт по международным стандартам и проверка срока действия карт.

5. Модуль «Мониторинг»

Назначение подсистемы: анализ финансовой активности пользователя и прозрачный

контроль за движением денежных средств.

Основные характеристики:

детализированная история всех совершенных операций с возможностью фильтрации по категориям;

наглядная аналитика расходов, помогающая пользователю контролировать свой бюджет;

подсистема включает системы внутренней диагностики приложения, чтобы технические службы Банка могли мгновенно получать информацию о программных ошибках и устранять их до того, как они затронут клиента.

4.1.1.2 Перечень сторонних ИС, с которыми должно быть обеспечено взаимодействие.

Для реализации полного функционала мобильного приложения для физических лиц, включая платежи, переводы, идентификацию и обслуживание карт, требуется обязательная интеграция со следующими внешними информационными системами (ИС) и сервисами.

1. *Платежные системы HUMO и Uzcard.*

Назначение взаимодействия: Обеспечение процессинга транзакций по картам этих систем, включая переводы P2P (по номеру карты/телефона), оплату услуг, проверку баланса и управление картами (блокировка, разблокировка) и подключение дополнительных сервисов систем как TEZ QR, Humo Pay и Uzcard Pay.

Тип взаимодействия: Прямое взаимодействие через API-интерфейсы процессингового центра Банка или Национального межбанковского процессингового центра.

2. *Платежный агрегатор «Paynet».*

Назначение взаимодействия: Предоставление клиентам доступа к широкому спектру мерчант-платежей (мобильная связь, интернет, коммунальные услуги, штрафы), которые агрегируются через систему «Paynet».

Тип взаимодействия: Интеграция по протоколу API для проведения моментальных платежей и получения статуса их исполнения.

3. *Сервис удаленной биометрической идентификации.*

Назначение взаимодействия: Выполнение обязательной удаленной биометрической идентификации клиентов (KYC) для их регистрации в приложении и открытия счетов в соответствии с требованиями регулятора.

Тип взаимодействия: Защищенное взаимодействие через шлюзы государственных сервисов для передачи и проверки персональных данных.

4. *КАТМ («КРЕДИТНО-ИНФОРМАЦИОННЫЙ АНАЛИТИЧЕСКИЙ ЦЕНТР»).*

Назначение взаимодействия: Получение актуальной кредитной истории и кредитного рейтинга физических лиц. Эта информация критически важна для реализации функций онлайн-скоринга и принятия Банком предварительных решений по заявкам на кредиты и лимиты в режиме реального времени.

Тип взаимодействия: Защищенное API-взаимодействие для получения кредитных отчетов.

5. *Портал государственных услуг «MyGov».*

Назначение взаимодействия: Интеграция с сервисами «MyGov» для обеспечения оплаты государственных пошлин, налогов и получения определенного набора государственных услуг непосредственно через приложение.

Тип взаимодействия: Интеграция через API для платежей и получения данных.

6. *Оператор Фискальных Данных (ОФД / OFD).*

Назначение взаимодействия: Обеспечение фискализации платежей и транзакций, подлежащих обязательной регистрации в соответствии с законодательством Республики Узбекистан (согласно Модулю «Платежи»).

Тип взаимодействия: Передача информации о платеже в ОФД для формирования фискального чека.

7. *Провайдеры СМС-услуг*

Назначение взаимодействия: Обеспечение надежного и резервированного канала доставки служебных сообщений, включая критически важные OTP-коды для аутентификации и подтверждения транзакций.

Тип взаимодействия: Прямое подключение к API обоих провайдеров для реализации механизма автоматического переключения в случае сбоя.

8. *Интегрированная Автоматизированная Банковская Система (АБС / IABS).*

Назначение взаимодействия: АБС является master-системой Банка. Интеграция обеспечивает выполнение всех финансовых операций (движение по счетам, кредиты, депозиты) и является источником актуальных остатков и клиентских данных.

Тип взаимодействия: Высокоскоростное защищенное API-взаимодействие (внутренний контур) для транзакционных запросов в режиме реального времени.

Требования к форматам данных, протоколам и режиму взаимодействия Системы с внешними информационными системами должны быть определены на этапе Технического проектирования и описаны в рамках документа «Частное техническое задание».

Разработка интеграций должна вестись Исполнителем по принципам сервисно-ориентированной архитектуры с возможностью дальнейшего переиспользования на стороне Заказчика.

4.1.1.3 Требования к режимам функционирования приложения, определяющим функционирование системы мобильного приложения в нормальном и аварийном режиме.

Система должна обеспечивать стабильную работу в трех основных режимах: штатном, аварийном и техническом. Переход между режимами должен происходить с максимальным сохранением целостности данных и информированием пользователей.

1. Нормальный (Штатный) режим

В этом режиме система работает в полном объеме, обеспечивая взаимодействие со всеми внутренними и внешними сервисами (ИАБС, процессинг, платежные шлюзы).

Доступность: сервисы доступны в круглосуточном режиме (24/7).

Производительность: время отклика системы на приоритетные запросы (авторизация, быстрые переводы P2P) не должно превышать 2 секунд.

Синхронизация и эффективность: обработка данных должна быть оптимизирована для исключения избыточной нагрузки на серверы. Статусы исполнения финансовых операций отражаются в приложении в режиме реального времени.

Многоканальность: обеспечивается одновременная и независимая работа пользователей с различных мобильных устройств без потери качества связи.

2. Аварийный режим

Активируется при частичной или полной недоступности компонентов (сбои ИАБС, каналов связи, SMS-провайдеров или внешних API).

Обеспечение транзакционности: это критическое требование. Любая незавершенная операция должна быть либо корректно доведена до конца после восстановления связи, либо полностью отменена с возвратом средств. «Зависание» транзакций в промежуточном состоянии недопустимо.

Автоматическое резервирование: при отказе основного канала (например, поставщика SMS-уведомлений) система обязана мгновенно переключаться на резервный шлюз без прерывания текущей сессии клиента.

Сохранение ключевого функционала: в случае сбоя второстепенных внешних сервисов (госуслуги, скоринг) приложение должно оставаться работоспособным. При этом недоступные функции автоматически скрываются или сопровождаются поясняющим сообщением.

Кэширование данных: для повышения удобства приложение должно сохранять во внутренней памяти устройства базовую информацию (шаблоны, историю последних операций), позволяя просматривать её даже при кратковременной потере интернета.

Информирование: пользователи получают оперативные push-уведомления о характере проблемы и примерных сроках её устранения. Режим считается завершенным только после автоматической сверки накопленных данных и восстановления всех интеграций.

3. Технический режим

Вводится для проведения плановых обновлений, настройки безопасности или профилактики серверного оборудования.

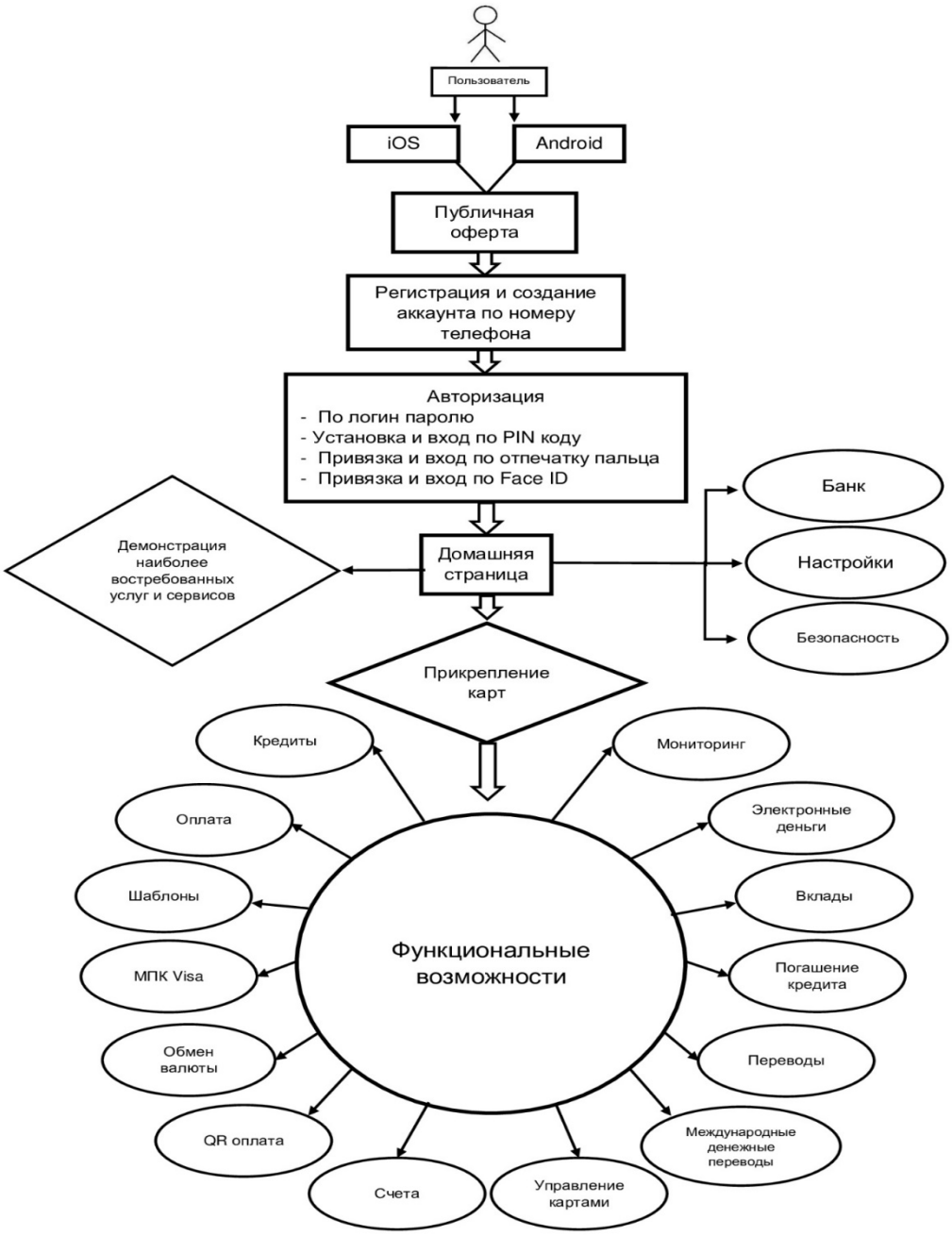
Планирование: регламентные работы проводятся в часы минимальной активности пользователей (преимущественно в ночное время).

Предварительное оповещение: банк заранее уведомляет клиентов о предстоящем ограничении доступа через новостную ленту приложения или push-сообщения.

Управление обновлениями: обновление клиентской части в официальных магазинах (Google Play, App Store) должно проходить бесшовно, с сохранением всех персональных настроек и авторизационных данных пользователя.

Администрирование: Технический персонал должен иметь исключительный доступ к управлению релизами и инструментам мониторинга, обеспечивая быстрый возврат системы в штатный режим после завершения работ.

4.1.1.4 Перечень и описание сценариев использования



Общая модель сценариев использования

Описание ролей пользователей мобильной платформы «BRB» для физических лиц

Администратор:

Основные функции:

Создание, редактирование и удаление пользователей.

Назначение ролей и прав доступа.

Конфигурирование системы: настройка модулей, интеграций, отчетов.

Управление данными: загрузка, экспорт, резервное копирование.

Мониторинг системы: отслеживание работоспособности, выявление и устранение ошибок.

Управление доступом к системе: создание и управление группами пользователей, настройка политик безопасности.

Анализ данных и генерация отчетов.

Права доступа /см. матрица доступа/:

Полный доступ ко всем функциям системы.

Возможность изменять настройки системы.

Доступ ко всем данным системы.

Модератор

Основные функции:

Проверка и утверждение создаваемого пользователями контента.

Мониторинг активности пользователей.

Ответы на вопросы пользователей.

Поддержка пользователей.

Права доступа:

Ограниченный доступ к функциям администрирования.

Доступ к инструментам модерации.

Возможность изменять свой профиль и настройки.

Доступ к статистике и аналитике.

Пользователь

Основные функции:

Доступ к функционалу системы в соответствии с назначенной ролью.

Создание и редактирование собственного профиля.

Взаимодействие с другими пользователями.

Использование сервисов Системы.

Получение уведомлений о событиях в системе.

Права доступа:

Ограниченный доступ к функциям системы.

Возможность изменять только свой профиль и связанные с ним данные.

Доступ к информации, соответствующей его роли.

Матрица доступа				
Роль	Создание пользователей	Изменение настроек	Просмотр всех данных	Модерация контента
Администратор	Да	Да	Да	Да
Модератор	Нет	Нет	Частично	Да
Пользователь	Нет	Нет	Нет	Нет

Перечень сценариев использования мобильного приложения представлен в таблице1.

Идентификационный Номер	**Наименование сценария Использования**	**Действующие лица**	**Тип сценарий**
A1	Управление конфигурациями, доступом и безопасностью	Администратор	Основной
M1	Мониторинг и контроль целостности операций	Модератор	Основной
U1	Проведение финансовых транзакций и использование сервисов	Пользователь	Основной

Сценарий использования A1. Управление конфигурациями, доступом и безопасностью.

Условия запуска: Администратор выполняет плановую настройку или реагирует на запрос по изменению прав доступа.

Основное действующее лицо: Администратор системы.

Порядок выполнения сценариев: Администратор — уполномоченное лицо, имеющее право управлять системой и ее внутренними ролями:

проводит многофакторную авторизацию в Модуле «Администрирование»;

проверяет и актуализирует конфигурацию информационной системы (в том числе перенос секретов и паролей в защищенное хранилище .env);

регистрирует модераторов в системе на основе официального запроса;

создает безопасные учетные данные (логин/пароль) согласно корпоративным стандартам безопасности;

определяет роли и разрешения (доступ к мониторингу транзакций или управлению лимитами), исключая избыточные привилегии.

Временной регламент выполнения сценария: Зависит от объема настроек и регламента безопасности Банка.

Входные данные: Данные сотрудника, запрашиваемая роль, параметры системных конфигураций.

Выходные данные: Настроенные роли и уровни доступа, обновленные параметры безопасности системы.

Сценарий использования М1. Мониторинг и контроль целостности операций.

Условия запуска: Модератор осуществляет плановый контроль или реагирует на уведомление системы о сбое в фоновых процессах.

Основное действующее лицо: Модератор системы.

Порядок выполнения сценариев:

проходит авторизацию в панели мониторинга с соответствующими правами контроля;

проверяет статусы исполнения транзакций в подсистемах «Оплата», «Переводы» и «Услуги»;

при обнаружении зависших или прерванных анализирует логи на предмет рассинхронизации данных;

инициирует процедуру завершения транзакции или полного отката (Rollback) для сохранения финансовой точности;

взаимодействует с пользователями через чат или систему уведомлений для информирования о статусе решения проблемы.

Временной регламент выполнения сценария: Время получения статуса по транзакции — не более 3 секунд.

Входные данные: ID операции, системные логи, данные из ИАБС.

Выходные данные: Актуальный статус транзакции, подтверждение целостности базы данных.

Сценарий использования U1. Проведение финансовых транзакций и использование сервисов.

Условия запуска: Пользователь инициирует операцию через интерфейс мобильного приложения.

Основное действующее лицо: Пользователь (Клиент банка).

Порядок выполнения сценариев:

походит аутентификацию в приложении (PIN/биометрия), при этом система активирует режим защиты экрана (FLAG_SECURE);

выбирает необходимую услугу или тип перевода и вводит реквизиты;

система проводит автоматическую валидацию данных (проверка номера карты, проверка достаточности средств);

пользователь подтверждает операцию одноразовым кодом (в случае сбоя SMS-шлюза система незаметно для пользователя переключается на резервный канал);

приложение отображает результат операции и предоставляет электронный чек.

Временной регламент выполнения сценария: Время отклика на критические операции — до 2 секунд.

Входные данные: Реквизиты платежа, сумма, код подтверждения.

Выходные данные: Исполненная операция, обновленный баланс счета, уведомление в истории мониторинга.

4.1.1.5 Требования по диагностированию

Мобильное приложение для физических лиц должно предоставлять инструменты диагностирования основных процессов, удобный интерфейс для возможности просмотра диагностических событий, мониторинг процесса выполнения программ.

Для обеспечения высокой надежности функционирования как системы в целом, так и её отдельных компонентов должно обеспечиваться выполнение требований по диагностированию ее состояния.

Диагностика программных и технических средств должна осуществляться с помощью стандартных режимов системных операционных систем, операционных систем отдельных рабочих станций и системы управления БД.

При возникновении аварийных ситуаций, либо ошибок в программном обеспечении, диагностические инструменты должны позволять сохранять полный набор информации, необходимой разработчику для идентификации проблемы (журнал процессов, содержащий сведения о текущем состоянии памяти и текущем состоянии файловой системы).

Необходимо реализовать систему диагностирования с возможностью отслеживания текущего состояния в режиме реального времени. Разработать графические дашборды для визуализации ключевых показателей и параметров работы системы в целом, а также каждой из её компонентов по отдельности. Дашборды должны содержать информацию о загрузке серверов, использовании ресурсов, времени отклика, сетевом трафике, статусе баз данных и других критических компонентов.

Внедрить механизм оповещений для моментального уведомления об обнаруженных проблемах, предоставив возможность пользовательской настройки приоритетов оповещений. Разработать план действий для оперативного реагирования на проблемы, включая автоматизированные процессы восстановления и масштабирования.

Обеспечить периодическую отчетность о состоянии системы, включая обобщенную статистику и анализ работы. Гарантировать конфиденциальность данных, передаваемых и хранимых в процессе мониторинга, и обеспечить контроль доступа к графическим дашбордам только для авторизованных пользователей.

В процессе эксплуатации тестирование и диагностика программно-технических комплексов должны осуществляться системным администратором в автоматическом режиме при ее запуске.

Для всех технических компонентов необходимо обеспечить регулярный и постоянный контроль состояния и техническое обслуживание.

4.1.1.6 Перспективы развития, модернизации МП

Мобильная платформа «BRB» для физических лиц создается как масштабируемая платформа, рассчитанная на долгосрочное развитие, внедрение новых финансовых и нефинансовых сервисов, а также адаптацию к меняющимся регуляторным и рыночным условиям.

При разработке платформы должны быть предусмотрены возможности ее последующей модернизации и развития в ходе появления новых модулей и подсистем, функций и задач при минимальных временных и финансовых затратах по следующим направлениям:

- изменение (дополнение и расширение) форматов и протоколов обмена данными;
- расширение списка автоматизируемых функций;
- адаптация к изменениям норм законодательства и, соответственно, автоматизируемых процессов;
- расширение состава интерфейсов ввода и предоставления информации;

− применение новых узлов системы, новых участников взаимодействия и, соответственно, новых процессов;

− техническое переоснащение системы.

Модернизация системы должна проводиться на основе:

− адаптации стандартов системы к новым законодательным и нормативным документам;

− разработки новых стандартов электронных документов.

Интегрированная система должна обеспечивать возможность модернизации при развитии интеграционных процессов. В ходе модернизации интегрированной системы должна быть обеспечена возможность сохранения и дальнейшего использования всех данных, хранящихся в этой системе.

4.1.1.7 Подсистема гибкого интерфейса

Данная подсистема (виджеты) предназначена для обеспечения индивидуальной настройки рабочего пространства пользователя на главном экране приложения. Подсистема должна функционировать на основе гибкой модульной сетки и включать следующие функциональные и технические возможности:

Механизмы управления контентом:

Переход в режим настройки должен осуществляться через длительное нажатие на виджет или через кнопку «Настроить экран» в нижней части списка. В данном режиме пользователю доступны функции добавления, удаления и перемещения блоков.

Реализация поддержки жеста Drag-and-drop для свободного перемещения виджетов по вертикали. Позиция каждого виджета должна сохраняться в профиле пользователя и быть идентичной при входе с разных мобильных устройств под одной учетной записью.

Наличие отдельного меню (Store/Gallery), содержащего все доступные информационные блоки, не выведенные на главный экран.

Параметры настройки виджетов:

Поддержка различных размеров виджетов (S — малый квадрат, M — средний прямоугольник, L — полноэкранный блок по ширине) в зависимости от объема выводимой информации.

Возможность временного скрытия балансов на виджетах («режим инкогнито») по нажатию на иконку «глаз».

Должна быть доступна настройка количества отображаемых строк.

Технические требования к подсистеме:

Данные в виджетах должны загружаться асинхронно. При отсутствии стабильного интернет-соединения виджет должен отображать последнее актуальное состояние с визуальной пометкой о времени обновления.

Система должна гарантировать, что критически важные системные уведомления (блокировка учетной записи или технические работы) отображаются выше пользовательских виджетов вне зависимости от их настроек.

Скорость рендеринга главного экрана при наличии более 5 активных виджетов не должна превышать 1.5 секунды на устройствах среднего ценового сегмента.

4.1.2 Требования к взаимодействию со сторонними информационными системами

Взаимодействие мобильной платформы «BRB» для физических лиц со сторонними информационными системами (ИС) должно быть реализовано через специализированный Модуль «Интеграции» (API-шлюз), обеспечивающий унификацию протоколов, безопасность и надежность обмена данными.

Взаимодействие Системы со сторонними информационными системами должно быть обеспечено согласно установленным организационным и техническим требованиям государственных стандартов O`zDSt 2590:2012 «Информационная технология, а также требованиям к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы» и O`zDSt 2864:2014 «Информационная технология. Межведомственная интеграционная платформа. Общие технические условия».

Взаимодействие со сторонними информационными системами должно достигаться путем использования сервис-ориентированной архитектуры, представляющей собой совокупность веб-сервисов, построенных по общепринятым стандартам, а также путем использования единых технологических решений и стандартов, единых классификаторов и описаний структур данных.

Программными средствами веб-сервиса должны протоколироваться факты приема и отправки каждого информационного сообщения в рамках системы взаимодействия с указанием уникального в рамках электронного сервиса идентификатора сообщения, направления (вида) сообщения (прием или отправка), даты, времени, адресата и контрольной суммы сообщения.

Связь с системами должна происходить по утвержденному протоколу и через сеть МСПД системы «Электронного правительства».

Результаты выполнения операций импорта и экспорта данных должны регистрироваться в специальном журнале событий и предоставляться по запросу администратора/пользователя.

Информационное взаимодействие системы со БД и информационными системами сторонних организаций должно осуществляться на основе веб-сервисов с использованием протокола SOAP (протокол обмена структурированными сообщениями в распределённой вычислительной среде). Обмен должен осуществляться путем экспорта-импорта XML-документов, веб-сервисов, API (интерфейс прикладного программирования), структурированных текстовых файлов исходной информации (текстовых макетов) и документов пакета Microsoft Office 2003/2007/2010 и последующих версий, OpenOffice, iWork в соответствии с регламентами и форматами обмена информацией, разработанными на основании договоров и соглашений с организациями- владельцами информационных систем (баз данных).

4.1.3 Требования к численности и квалификации пользователей

Мобильная платформа предназначена для использования среди широкого круга пользователей, поэтому максимальное количество конечных пользователей, одновременно имеющих доступ лимитируется только техническими ограничениями серверной части Системы.

Мобильная платформа «BRB» для физических лиц должно быть спроектировано для пользователя с базовым уровнем владения современным смартфоном и минимальными навыками работы с мобильными приложениями (интуитивный интерфейс).

Специальная подготовка конечных пользователей не требуется. Должно быть обеспечено наличие интерактивных подсказок (туториалов) и справочного раздела (FAQ) непосредственно в приложении.

Решение должно обеспечить возможность оперативного и одновременного доступа большого числа пользователей к базе данных приложения для предоставления услуг, изменения и анализа необходимой информации, обработки запросов в реальном режиме времени.

Обслуживающий персонал — это сотрудники АКБ «Банк развития бизнеса», использующие Модуль «Администрирование» для управления, мониторинга и поддержки системы.

Требуется средний и высокий уровень квалификации в области информационных систем, банковских продуктов и информационной безопасности.

Для персонала, работающего с Модулем «Администрирование», требуется обязательное прохождение специализированного обучения по утвержденному Банком Руководству Администратора с получением сертификата о допуске к работе с системой.

Обслуживающий персонал должен быть обеспечен рабочими местами, оснащенными персональными компьютерами с доступом к внутренней корпоративной сети Банка и Модулю «Администрирование» через защищенные каналы.

В состав персонала, необходимого для обеспечения эксплуатации мобильного приложения, необходимо выделение следующих ответственных лиц:

Администратор системы: (1-2 сотрудника) для управления конфигурациями и ролями (сценарий А1).

Оператор Кол-центра/Модератор: (10+ сотрудников) для мониторинга транзакций, обработки обращений и управления службами (Модуль «Администрирование»).

Специалист ИТ-поддержки: (1-2 сотрудника) для мониторинга логов, производительности и взаимодействия с разработчиками.

4.1.4 Показатели назначения

Степень приспособляемости системы к изменению процессов и методов управления, к отклонениям параметров объекта управления

Мобильная платформа «BRB» для физических лиц должна адаптироваться к увеличению нагрузочной способности при изменении количества пользователей и изменению реквизитного состава без изменения структуры системы.

Система должна адаптироваться к изменяющимся требованиям безопасности.

Система должна быть открытой для подключения любого количества пользователей, т.е. изменение количества пользователей зависит от технических характеристик сервера базы данных.

Вероятностно-временные характеристики, при которых сохраняется целевое назначение системы

Целевое назначение системы должно сохраняться на протяжении всего срока эксплуатации. Срок эксплуатации приложения определяется сроком устойчивой работы аппаратных средств вычислительных комплексов и технических средств, своевременным проведением работ по замене (обновлению) аппаратных и технических средств, по сопровождению программного обеспечения и его модернизации. При условии постоянного выполнения этих работ целевое назначение системы должно сохраняться неограниченно долго.

Работоспособность системы не должна нарушаться при превышении номинальной нагрузки, при этом допускается пропорциональное увеличение времени реакции или отказ в обслуживании отдельных запросов.

Приложение должно стабильно функционировать при определенной проектной нагрузке, которая составляет не менее 100 000 одновременных пользователей и до 10 млн зарегистрированных учетных записей.

Для обеспечения функциональности системы при максимальной нагрузке (300,000 одновременных пользователей) необходимо провести нагрузочное тестирование с использованием сценариев стресс-тестирования:

Критерии для проведения тестирования:

Производительность базы данных, пропускная способность сети, время отклика для пользователей, время выполнения критически важных операций.

Сценарии нагрузочного тестирования:

Тестирование на разных уровнях нагрузки (10,000 – 100,000 пользователей) для моделирования реальных условий эксплуатации.

Проверка системы на резкие всплески нагрузки с одновременным выполнением критических операций (например, аутентификация пользователей, транзакции).

Стресс-тестирование:

Определение пределов производительности системы для оценки, сколько пользователей система способна поддерживать до возникновения задержек или сбоев.

Проведение тестов с использованием инструментов (Apache JMeter, LoadRunner и т.д.).

Для контроля над критически важными функциями системы допустимы следующие пороги:

Время авторизации пользователя: не более 2 секунд при максимальной нагрузке.

Время выполнения транзакций: не более 5 секунд для 99% запросов.

В случае превышения проектной нагрузки, допускается временное увеличение времени реакции системы. Время отклика при этом может увеличиться пропорционально росту нагрузки, но система не должна полностью прекращать функционировать.

После снижения нагрузки до номинального уровня система должна автоматически восстанавливать своё время реакции до начальных показателей.

Система должна предусматривать механизмы автоматического восстановления после сбоев и аварий. Включаются следующие меры:

Регулярное резервное копирование данных (как минимум раз в сутки) для обеспечения возможности восстановления данных.

Максимально допустимое время восстановления системы после сбоя не должно превышать 2 часов.

Использование резервных серверов позволит автоматически переключаться на резервные мощности в случае сбоя основных серверов.

Для поддержания системы в рабочем состоянии и сохранения её целевого назначения предусмотрены регулярные обновления и мониторинг системы. Это включает:

Использование инструментов для постоянного мониторинга производительности и безопасности системы.

Платформа должна поддерживать регулярные обновления программных компонентов
и базы данных с минимальным временем простоя.

4.1.5 Требования к надежности

Надежность системы обеспечивается за счет распределения нагрузки и многократного дублирования всех критических узлов.

Обеспечение сохранности данных: В системе должна быть внедрена технология потоковой репликации СУБД. Это означает, что каждая запись в базе данных мгновенно дублируется на резервный сервер. В дополнение к этому настраивается автоматизированная архивация, которая создает «снимки» системы для долгосрочного хранения. Это позволяет восстановить данные на любой момент времени в прошлом, если произойдет масштабный программный сбой.

Архитектурное сегментирование: Виртуальная инфраструктура должна строиться по принципу «эшелонированной защиты». Все серверы разделяются на три логических слоя: внешний (DMZ), внутренний прикладной и слой баз данных. Прямое соединение между внешним слоем и базой данных запрещено; все запросы должны проходить через цепочку проверок.

Конфигурация мощностей: Для стабильной работы приложения в промышленной среде Исполнитель разворачивает не менее 6 специализированных виртуальных машин. Такая структура позволяет выделить отдельные мощности под балансировку трафика, обработку запросов пользователей и мониторинг, исключая их взаимное влияние.

Защита от перегрузок: для каждого элемента системы (контейнера) устанавливаются жесткие границы потребления памяти и ресурсов процессора. Это гарантирует, что система останется стабильной даже при резком увеличении пользователей.

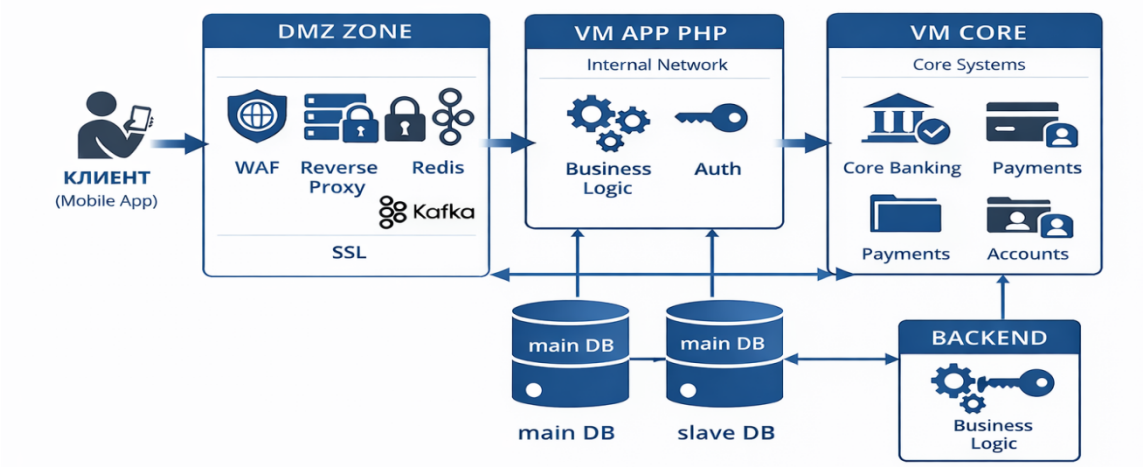


Рис. Архитектура взаимодействия виртуальных машин

Ответственность за бесперебойную работу технических средств, и комплексов инженерных средств несет заказчик проекта.

Ответственность за бесперебойную работу приложения несет Исполнитель проекта.

Информационная система проектируется как высокодоступное решение, функционирующее в режиме 24/7. Архитектура должна полностью исключать наличие единых точек отказа, обеспечивая показатель доступности не менее 99.9% в год. В случае возникновения критических сбоев оборудования или системного ПО, время восстановления работоспособности всех бизнес-функций (RTO) не должно превышать 30 минут, при этом за счет использования синхронной репликации баз данных и механизмов мгновенного зеркалирования транзакционных логов гарантируется полное отсутствие потери данных (RPO = 0).

Для обеспечения прозрачности эксплуатации и оперативного выявления инцидентов должна быть реализована глубокая интеграция с централизованной системой мониторинга и анализа событий безопасности (SIEM). Процесс журналирования должен охватывать все уровни системы: от действий администраторов до каждой финансовой транзакции. Журналы должны быть защищены от несанкционированного изменения и храниться в защищенном контуре: не менее 1 года (366 дней) в оперативном доступе и до 3 лет в архиве. Среднее время отклика серверной части не должно превышать 200 мс для 95% запросов при нагрузке до 5000 активных сессий. Система должна автоматически масштабироваться в кластере Kubernetes, наращивая ресурсы при достижении порога нагрузки в 70%. Исполнитель обязан предоставить формализованный план реагирования на инциденты (IRP) с регламентированными сроками устранения угроз по SLA.

Требования к методам оценки и контроля показателей надежности на разных стадиях создания системы в соответствии с действующими нормативно-техническими документами

Система должна разрабатываться на основании действующих нормативных правовых актов и организационно-распорядительных документов.

Должны быть разработаны и утверждены в установленном порядке методики и инструкции выполнения пользователями операций в Системе.

В состав методического обеспечения входит:

• нормативные правовые документы;

• должностные инструкции персонала, выполняющего работы с использованием Системы.

Состав методического обеспечения может уточняться в процессе технорабочего проектирования и согласовывается с заказчиком.

Нормативно-техническая документация должна соответствовать требованиям нормативных правовых актов и разрабатываться согласно следующим стандартам:

• O‘zDSt 1985:2018 Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем;

• O‘zDSt 1986:2018 Информационная технология. Информационные системы. Стадии создания;

• O‘zDSt 1987:2018 Информационная технология. Техническое задание на создание информационной системы.

• Постановление Правления Центрального банка Республики Узбекистан № 3030 от 02.07.2018 г. «Об утверждении Положения о минимальных требованиях к деятельности коммерческих банков при осуществлении взаимоотношений с потребителями банковских услуг»

• Постановление Правления Центрального банка Республики Узбекистан № 3759 от 21.01.2026 г. «Об утверждении Положения о минимальных требованиях по обеспечению информационной и кибербезопасности, а также предупреждению случаев фрода при оказании дистанционных финансовых услуг физическим лицам кредитными и платежными организациями, операторами платежных систем»

4.1.6 Требования безопасности

Защита персональных данных пользователей обеспечивается многоуровневой системой безопасности, спроектированной с учетом актуальных киберугроз и требований регулятора.

Вход в систему и инициация любых финансовых транзакций защищены механизмом усиленной многофакторной аутентификации (2FA). Система использует динамические одноразовые коды (OTP), передаваемые по защищенным каналам. Параметры OTP строго

регламентированы: длина кода составляет не менее 6 буквенно-цифровых символов, а период его актуальности ограничен 60 секундами. Для нейтрализации угроз подбора идентификаторов внедрена логика временной блокировки учетной записи (не менее 15 минут) после трех последовательных неудачных попыток ввода пароля или OTP. Каждая сессия пользователя имеет ограниченный период активности (тайм-аут не превышает 5 минут при бездействии), по истечении которого требуется повторная авторизация.

Реализована технология «аппаратного профилирования» (Device Binding), фиксирующая уникальный цифровой отпечаток устройства пользователя. Доступ к учетной записи с нового устройства возможен только после прохождения процедуры доверенной верификации. Мобильное приложение осуществляет непрерывный мониторинг целостности операционной системы (контроль Root/Jailbreak) и блокирует доступ к финансовым функциям в случае обнаружения активных инструментов удаленного управления (AnyDesk, TeamViewer и аналогичные) или признаков дублирования интерфейса («экранных наложений»).

Все критические события, включая действия администраторов, системные ошибки и попытки несанкционированного доступа, подлежат детальному логированию. В соответствии с требованиями Постановления ЦБ РУз. № 3759, срок хранения журналов в оперативном доступе составляет не менее 12 месяцев. Хранение паролей пользователей реализуется исключительно в хешированном виде с использованием стойких алгоритмов (уровня Argon2id). Передача данных между клиентом и сервером защищается протоколами TLS версии не ниже 1.3 с использованием доверенных сертификатов.

При обработке данных платежных карт применяется маскирование (PAN Masking) и токенизация. Управление ключами шифрования должно соответствовать ISO 27001 A.10 с использованием аппаратных модулей безопасности (HSM) или защищенных внутренних сервисов управления ключами; хранение секретов в программном коде запрещено. Для защиты конфиденциальных данных должна быть реализована их классификация и интеграция с системами предотвращения утечек (DLP). Исполнитель гарантирует отсутствие в коде уязвимостей из списка OWASP Top 10.

Интеграция с антифрод-системой Банка для анализа контекста операций. Система автоматически выделяет транзакцию как подозрительную, если фиксируется резкая смена паттерна (крупный перевод сразу после смены SIM-карты или устройства), и инициирует дополнительную проверку.

Требования к серверной операционной среде

В качестве фундамента для всех серверных компонентов должны использоваться операционные системы корпоративного класса — Oracle Linux (версии 8 / 9.9) или Alma

Linux. Выбор данных систем обусловлен их высокой стабильностью и гарантированным циклом поддержки обновлений.

Все серверы должны быть настроены на автоматическое получение и установку критических обновлений безопасности. Это минимизирует время, в течение которого система может быть уязвима для новых киберугроз.

Процесс обновления должен сопровождаться системой оповещений. В случае, если автоматический патч не смог установиться или вызвал конфликт в системе, ответственный персонал должен немедленно получить уведомление для ручного вмешательства.

Требования к защите конфиденциальных данных

Безопасность учетных записей пользователей строится на принципе «невозможности восстановления».

Система никогда не хранит пароли в их исходном виде. Каждый пароль преобразуется в уникальный зашифрованный след (хеш) с использованием алгоритма Argon2id.

К каждому паролю перед шифрованием добавляется уникальный набор случайных символов (salt). Это делает бесполезными заранее заготовленные базы данных для взлома (радужные таблицы) и гарантирует, что даже два одинаковых пароля разных пользователей будут выглядеть в базе данных совершенно по-разному.

Каждое подключение пользователя имеет строго ограниченное время жизни. При обнаружении подозрительной активности или долгом бездействии система автоматически прерывает сеанс.

Требования к обеспечению ИБ при проектировании и разработке

Архитектура:

Запрет прямого обращения в бэковую часть и базы данных со стороны публичных сетей (Интернет).

Если ПО создается для массового сегмента и предполагает взаимодействие, то интерфейс для взаимодействия с мобильным приложением должен быть выделен в отдельный фронтовый модуль и расположен в сегменте DMZ.

Жизненный цикл:

Все компоненты, используемые Системой, должны иметь длительный срок поддержки со стороны их разработчиков.

Для эксплуатации Системы приложения необходимо предусмотреть ее полный жизненный цикл, включая выпуск обновлений и патчей, замена устаревших версий и компонентов (поддержка приложения).

Система приложения проходит регулярный аудит безопасности.

Система приложения должна пройти нагрузочное тестирование на нагрузку, заявленную в ТЗ с имитацией действий пользователей, в том числе на предмет не корректных пользовательских запросов.

По мере готовности приложения Банк оставляет за собой право провести тестирование Системы на проникновение и потребовать устранения выявленных недочетов.

ИС должна соответствовать требованиям национальных стандартов:

O'z DSt 1987:2010 «Техническое задание на создание информационной системы»

O'z DSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения»;

O‘z DSt ISO/IEC 27001:2018 «Информационные технологии. Методы обеспечения безопасности системы управления информационной безопасностью. Требования»;

O‘z DSt ISO/IEC 27002:2018 «Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью».

Программное обеспечение должно соответствовать по надёжности международным стандартам, стандартам и техническим регламентам Республики Узбекистан, которые относятся к данной отрасли.

Программное обеспечение системы должно обеспечивать обработку информации, согласно установленной категории.

Мониторинг, аудит и обработка инцидентов:

Для обеспечения безопасности данных и предотвращения попыток несанкционированного доступа система будет оснащена следующими механизмами мониторинга и аудита:

будут применяться технологии обнаружения вторжений (IDS — Intrusion Detection Systems) и предотвращения вторжений (IPS — Intrusion Prevention Systems), которые будут активно сканировать потоки данных и сообщать о попытках несанкционированного доступа или необычных паттернах активности;

все важные операции (входы в систему, изменения прав доступа, попытки доступа к защищённой информации, неудачные попытки аутентификации) будут записываться в журналы событий с указанием времени и данных о пользователях. Эти журналы будут доступны для анализа с целью выявления потенциальных угроз и попыток вторжений;

будут проводиться периодические проверки логов и системных данных для выявления возможных уязвимостей или инцидентов безопасности. Аудиты будут

включать анализ логов на предмет аномальных действий, проверку соответствия политике безопасности и анализ слабых мест в системе;

встроенная система оповещений будет автоматически уведомлять администраторов системы и группы реагирования на инциденты о подозрительной активности, что позволит оперативно реагировать на угрозы.

Для обеспечения своевременного реагирования на инциденты безопасности в системе будет разработан и внедрен план реагирования, включающий следующие этапы:

в случае обнаружения угрозы или аномальной активности система безопасности должна немедленно определить тип инцидента (например, попытка взлома, утечка данных, внутренняя угроза);

после идентификации инцидента предпринимаются меры для ограничения его последствий. Это может включать изоляцию уязвимого узла, ограничение доступа, блокирование подозрительных IP-адресов или учетных записей пользователей;

после ограничения угрозы проводится устранение последствий инцидента, например, восстановление системы из резервных копий, пересмотр прав доступа или обновление программного обеспечения для устранения уязвимости;

каждый инцидент должен быть детально задокументирован. Отчет будет включать описание угрозы, ее воздействие на систему, принятые меры и дальнейшие рекомендации по предотвращению повторения инцидента;

в случае серьёзных инцидентов (например, утечка данных) о ситуации уведомляются соответствующие регулирующие органы и пользователи, чьи данные могли быть затронуты;

впоследствии проводится анализ причин инцидента, чтобы в будущем избежать подобных ситуаций. По результатам инцидента сотрудники проходят дополнительное обучение, и в систему могут быть внесены изменения (например, усиление политики доступа или обновление программного обеспечения).

Требования безопасности технических средств

Требования по обеспечению безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств системы, по допустимым уровням освещённости, вибрационных и шумовых нагрузок к системе приложения в соответствии с требованиями производителя оборудования и транспортного средства.

Необходимый уровень безопасности должен обеспечиваться путем строгого соблюдения правил эксплуатации и технического обслуживания оборудования, рекомендованных разработчиками средств информатизации.

Работы по монтажу и наладке Системы, а также последующее ее техническое обслуживание не должны быть сопряжены с воздействием на персонал опасных значений электрического тока, электромагнитных полей, акустических шумов, вибраций и т.д.

Конструкция технических средств, в случае их наличия, должна обеспечивать защиту обслуживающего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003-75 и ГОСТ 12.2.007.0-75.

Конструкция технических средств должна обеспечивать свободный доступ к отдельным узлам и элементам для их технического обслуживания и ремонта, удобное подключение силовых кабелей.

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в целях нагрузки, а также аварийное ручное отключение; система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в целях нагрузки, а также аварийное ручное отключение.

Должна быть обеспечена безопасность кабелей, входящих в состав Системы по следующим принципам:

кабели электропитания и линии связи, идущие к информационным системам, должны быть проведены (по возможности) под землей или защищены надлежащим образом;

для защиты сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, используются экраны или кабели прокладываются так, чтобы они не проходили через общедоступные места;

кабели электропитания должны быть отделены от кабелей телекоммуникаций, чтобы исключить помехи;

незадействованные разъемы информационных кабелей, предназначенные для подключения PC, должны быть опечатаны или заклеены специальной маркой для исключения возможного несанкционированного подключения нештатных технических средств обработки информации.

Помещения и здание, где будет размещен аппаратно-программный комплекс создаваемой информационной системы, должны соответствовать требованиям стандарта O'z DSt 2875:2014 «Информационная технология. Требования к дата центрам. Инфраструктура и обеспечение информационной безопасности» и руководящего документа RH 45-201:2011 «Технические требования к зданиям и сооружения для установки средств вычислительной техники».

Все оборудование, входящее в состав Системы, должно быть серийным и иметь соответствующие сертификаты соответствия. Все ПО, входящее в состав Системы, должно быть лицензионным и являться продуктом мировых производителей.

Требования по разграничению доступа к частям МП

ПО должна обеспечивать возможность управления доступом к документам. Уровень детализации правил разграничения доступа должен позволять определить права доступа для каждого конкретного пользователя.

Возможность определения авторства каждой операции в системе приложения и отсутствие неавторизованных операций на основе уникальных персонифицированных идентификаторов каждого пользователя, процедуры аутентификации и протоколирования действий пользователей в журналах аудита.

Наличие развитой системы управления аутентификационной информацией пользователей (паролями, ключами) и механизмов контроля за ее качеством и использованием, обладающие следующими характеристиками:

- длина пароля не менее восьми символов;

- периодическая принудительная смена паролей не реже, чем раз в месяц;

- возможность самостоятельного изменения пользователями своего пароля в любое время;

- предоставление доступа к информации при первом входе пользователя в Приложение;

- перехваченная передаваемая по каналу связи аутентифицирующая информация не должна позволять осуществлять вход в Приложение через прикладную систему.

Требования к защите информации от несанкционированного доступа

Распределение ролей и управление учётными записями пользователей мобильного приложения должно осуществляться назначенным администратором системы. Организационные меры должны быть обеспечены ответственными лицами и должны исключать неконтролируемый доступ посторонних к техническим средствам.

Система безопасности приложения должна обеспечивать:

- конфиденциальность информации при передаче по открытым сетям;

- защиту от несанкционированного доступа к системе и информации в системе;

- целостность информации;

- идентификация/аутентификация и авторизацию пользователей системы разделение прав и доступов с привязкой к штатному расписанию компании, интеграция со штатным расписанием.

Система неизменимого логирования действий пользователей и администраторов.

Защита данных от несанкционированной модификации (изменения), доказательство авторства передаваемых сообщений, идентификация/аутентификация и авторизация пользователей при доступе к информационным ресурсам производятся с использованием логина и пароля).

Для предотвращения несанкционированных операций и выявления признаков мошенничества, мобильное приложение должно поддерживать интеграцию с системой антифрод-мониторинга сессий:

Мониторинг параметров сессии (скорость ввода, типичные маршруты навигации, способы взаимодействия с экраном).

Проверка устройства на наличие признаков Root/Jailbreak, работы эмуляторов, активных сессий удаленного управления и использования VPN/Proxy.

Каждой сессии должен присваиваться уровень риска. При выявлении аномалий система должна запрашивать дополнительную аутентификацию (Liveness Check или ввод ПИН-кода) либо блокировать выполнение финансовой операции.

В Системе предусмотрены программные модули, дающие возможность контроля и ограничения прав пользователей приложения.

Доступ к системе приложения обеспечен только для зарегистрированных пользователей, прошедших процедуры идентификации/аутентификации.

Полномочия на доступ к системе приложения должны реализовываться и контролироваться администраторами через функции администрирования Системы.

Идентификация/аутентификация пользователей в системе производится (через систему биометрической идентификации).

Система должна автоматически блокировать сессии пользователей по заранее заданным временам отсутствия активности со стороны пользователей и приложений.

Все действия пользователей должны записываться в соответствующих журналах.

Доступ к журналам действий пользователей должен иметь только администратор. Никто (даже администратор) не должен иметь права на изменение/удаление записей журналов.

При вводе данных в системе должен осуществляться контроль входной информации по типу данных и диапазону допустимых значений. В данной ситуации Система должна обеспечивать корректную обработку ситуаций, связанных неверными

действиями пользователей и недопустимыми значениями входных данных. В указанных случаях пользователю должна выдаваться соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных».

Загрузка файлов в формате кроме установленных в системе - должен быть исключен и максимальный размер загружаемых в систему файлов должен быть ограничен.

Требования по сохранности информации при авариях

Требования по сохранности информации при авариях и расчетные типы отказов и сбойно-аварийных ситуаций должны определяться общими техническими требованиями к АСУ. При этом специализированные программные средства администратора базы данных должны обеспечивать:

- возможность полного или частичного восстановления данных в результате возникновения сбойных ситуаций;

- наличие системы дублирования на резервные устройства хранения с последующим восстановлением данных.

Для обеспечения сохранности информации в системе должны быть включены следующие функции:

- резервное копирование баз данных системы, должно быть предусмотрено удаленное хранение резервных копий баз данных, обеспечивающее сохранность информации на случай пожара и стихийных бедствий;

- восстановление данных в непротиворечивое состояние при программно-аппаратных сбоях (отключение электрического питания, сбоях операционной системы и других) вычислительно-операционной среды функционирования;

- восстановление данных в непротиворечивое состояние при сбоях в работе сетевого программного и аппаратного обеспечения.

Требования к защите от влияния внешних воздействий

Компьютеры, на которых должны быть установлены компоненты системы, должны находиться в специально оборудованных помещениях, в отдалении от отопительных приборов и электрических кабелей.

Система должна сохранять работоспособность при нормальных климатических условиях эксплуатации:

- температура окружающей среды от 10 до 50ºС , 5 ºС;

- повышенная запыленность;

- относительная влажность 60%, 15%;

- атмосферное давление от 84 до 107 кПа (от 630 до 800 мм рт. ст.).

Сервера системы должны быть снабжены ИБП для предохранения от перепадов напряжения и непредвиденного отключения электричества.

4.1.7 Требования к эргономике и технической эстетике

Интерфейс должен быть интуитивно понятен пользователю, с четко структурированной информацией и логически построенными навигационными элементами. Для этого необходимо минимизировать количество действий, необходимых для выполнения основных операций (например, регистрация, отправка документов или осуществление финансовых операций).

Проектирование интерфейса мобильного приложения должно происходить с учетом современных требований к UX/UI и обеспечивать высокий уровень персонализации для конечного пользователя:

Система должна поддерживать механизм динамической смены тем оформления. Пользователю должна быть предоставлена возможность выбора между светлой, темной и системной темами, а также возможность изменения акцентных цветов интерфейса в рамках палитры, утвержденной Банком.

Визуальное оформление элементов управления (кнопок, переключателей) должно адаптироваться под выбранную тему, обеспечивая соблюдение контрастности и читабельности текста в соответствии с международными стандартами доступности.

Управление шрифтами: Возможность изменения размера экранных шрифтов в рамках настроек приложения для повышения удобства использования лицами с ограниченными возможностями зрения.

В интерфейсе мобильного приложения должен быть реализован функционал «Guest Mode» (гостевой режим), предоставляющий Пользователю возможность ознакомления с приложением без прохождения биометрической или иной формы аутентификации.

В рамках гостевого режима должны быть реализованы следующие ограничения и возможности:

Пользователь получает доступ к навигации по основным экранам приложения, демонстрационным разделам и информационному контенту.

Все функции, связанные с оплатой, переводами, оформлением продуктов, получением услуг и изменением персональных данных, должны быть полностью отключены.

Финансовые данные (балансы, лимиты, история операций, статусы продуктов) не отображаются либо заменяются на демонстрационные (заглушечные) значения.

При попытке выполнения ограниченного действия (оплата, заказ услуги, перевод средств и т.п.) Пользователю должно отображаться уведомление с предложением пройти идентификацию и авторизацию.

Переход из гостевого режима в полноценный режим использования приложения должен быть доступен через кнопку «Войти» / «Пройти идентификацию» с последующим выполнением стандартного сценария аутентификации.

Также в мобильном приложении должен быть реализован функционал «Picture-in-Picture» (картинка в картинке), позволяющий Пользователю одновременно работать с несколькими экранами приложения без необходимости закрытия или повторного открытия текущего экрана.

Функциональные требования:

Пользователь должен иметь возможность свернуть текущий активный экран приложения в минимизированное плавающее окно.

Минимизированное окно отображается поверх других экранов приложения и сохраняет текущее состояние (данные, введённые значения, шаг сценария).

Пользователь может свободно перемещать плавающее окно по экрану устройства.

Из плавающего окна должна быть доступна возможность:

- возврата к полноэкранному режиму;
- закрытия плавающего окна.

Основной интерфейс приложения при этом остаётся доступным для навигации и выполнения других действий, не связанных с активным сценарием в плавающем окне.

Закрытие или сворачивание плавающего окна не должно приводить к потере данных или сбросу текущего пользовательского сценария.

Функционал предназначен для повышения удобства пользовательского взаимодействия и многозадачности внутри приложения.

Мобильная платформа “BRB” для физических лиц должно корректно отображаться на различных устройствах (мобильные телефоны, планшеты) и подстраиваться под разрешение экрана. Важно обеспечить удобство работы как в настольной, так и в мобильной версии.

Пользователи не должны сталкиваться с излишне сложными интерфейсами. Важная информация должна быть представлена в простом и понятном виде, с возможностью получения более детальной информации при необходимости (например, в формате всплывающих окон или инструкций).

Приложение должно быть адаптировано для пользователей в Узбекистане с учетом языковых предпочтений.

Интерфейс не должен быть перегружен сложными визуальными эффектами, которые замедляют его работу. Важно обеспечить быстрый отклик системы на действия пользователя, особенно при работе с медленным интернетом.

Цветовая палитра не должна вызывать дискомфорта при длительном использовании платформы. Рекомендуется использование корпоративных цветов, ассоциирующихся с платформой и поддерживающих идентификацию бренда. При формировании информативно-текстовых элементов должны быть использованы “фирменные” шрифты и общая стилистика АКБ “Банк развития бизнеса”, но не должен быть продублирован полностью.

Шрифты должны быть четкими и удобочитаемыми на любом устройстве. Рекомендуется использование шрифтов без засечек, обеспечивающих хорошую читаемость при малом размере. Цвет текста должен контрастировать с фоном, чтобы обеспечить максимальную видимость.

Графические элементы (иконки, кнопки, диаграммы) должны быть унифицированы и подчинены единому стилю. Необходимо использовать современные иконки с понятной визуальной метафорой для всех категорий пользователей.

Все элементы интерфейса (меню, кнопки, ссылки) должны быть сгруппированы по логическим признакам. Важные разделы, такие как "Личный кабинет", "Документооборот", "Финансовые услуги", должны быть легко доступны с главного экрана.

Переходы между разделами должны быть интуитивными и быстрыми, а пользователю должно быть понятно, где он находится на платформе в любой момент времени.

Для повышения удобства и предотвращения ошибок пользователю должны предоставляться визуальные и текстовые подсказки. Важные события (например, успешная отправка документов или выполнение транзакции) должны сопровождаться уведомлениями.

В случае возникновения ошибок, они должны быть четко описаны и сопровождаться инструкциями по их исправлению. Ошибки должны быть визуально выделены, но не перегружать пользователя ненужной информацией.

Все элементы интерфейса должны быть выполнены в едином стиле и иметь согласованное оформление. Это касается шрифтов, кнопок, полей ввода, графики и т.д.

Дизайн должен отражать фирменный стиль электронной платформы, что способствует повышению узнаваемости бренда.

Интерфейс Мобильного приложения, а также все системные уведомления, шаблоны документов и ответы чат-бота должны поддерживать полноценную локализацию.

Перечень поддерживаемых языков:

Узбекский — основной государственный язык (поддержка латиницы).

Русский язык.

Английский — для международного использования.

Китайский — для обеспечения удобства работы с клиентами из КНР.

Техническая реализация:

Приложение должно автоматически определять язык системы устройства при первом запуске.

Пользователь должен иметь возможность вручную сменить язык в разделе «Настройки» без перезагрузки приложения.

Все текстовые константы должны храниться в отдельных ресурсных файлах (i18n), исключая наличие «жестко закодированного» (hardcoded) текста в коде.

Поддержка динамической подгрузки языковых пакетов с сервера (Server-Driven Localization).

Разработка удобного и понятного интерфейса, который соответствует требованиям O‘z DSt 1987:2018, обеспечит легкость и комфорт работы пользователей с системой, а также повысит эффективность использования платформы.

4.1.8 Требования к подсистеме сбора и анализа поведенческих метрик (Трекинг)

Подсистема мониторинга клиентских путей предназначена для обеспечения непрерывного сбора, регистрации и анализа взаимодействия Пользователя с интерфейсом мобильного приложения. Данные, собираемые подсистемой, являются основой для формирования аналитической отчетности о качестве клиентского опыта (UX) и стабильности функционала.

Объект мониторинга и событийная модель

Подсистема должна автоматически регистрировать следующие типы событий:

Фиксация каждого факта перехода между экранными формами (Activity для Android, ViewController для iOS). Лог должен содержать уникальный технический идентификатор экрана, наименование класса и временную метку события (с точностью до миллисекунд).

Регистрация событий пользовательской активности (onClick, onLongClick, onSwipe, onScroll) для всех компонентов графического интерфейса. Каждая запись должна содержать:

Идентификатор элемента (Element ID);

Тип действия;

Текстовое значение элемента;

Координаты нажатия.

Мониторинг последовательности действий в рамках ключевых бизнес-процессов («Авторизация», «P2P-перевод», «Оплата услуг», «Открытие вклада»). Система должна фиксировать точку и причину прерывания сценария Пользователем.

Метрики времени и производительности интерфейса

Для оценки эффективности интерфейса подсистема должна рассчитывать следующие показатели:

Активное время (Time on Screen): Суммарная длительность нахождения экранной формы в состоянии Foreground. Время нахождения приложения в фоновом режиме не должно учитываться.

Задержка взаимодействия (Interaction Delay): Интервал времени между полной отрисовкой контента на экране и первым целенаправленным действием (нажатием) Пользователя.

Длительность ввода (Input Duration): Время, затрачиваемое на заполнение экранных форм и полей ввода. Данная метрика используется для выявления избыточных или сложных для заполнения данных.

Время отклика системы: Фиксация времени между нажатием на кнопку выполнения операции и получением визуального результата (ответа от Backend-системы).

Технические требования и ограничения

Процесс сбора и передачи данных должен соответствовать следующим регламентам:

Безопасность и конфиденциальность: категорически запрещается сбор и передача в подсистему аналитики персональных данных, сведений о балансах счетов, полных номеров карт, ПИН-кодов и иной информации, составляющей банковскую тайну. Перед отправкой данные должны проходить процедуру анонимизации на стороне мобильного приложения.

Режим накопления (Буфферизация): для оптимизации энергопотребления устройства и экономии сетевого трафика события должны накапливаться в локальном защищенном хранилище приложения. Пакетная отправка данных на сервер должна осуществляться строго при наступлении одного из условий:

Достижение лимита в 50 накопленных событий;

Завершение сеанса работы Пользователя (переход приложения в Background или закрытие);

Переход на критически важный этап бизнес-сценария.

Обеспечение целостности данных (Offline-mode): при отсутствии подключения к сети интернет-данные трекинга должны сохраняться в энергонезависимой памяти устройства. Синхронизация накопленного архива с сервером должна производиться автоматически при восстановлении соединения в фоновом режиме.

Влияние на производительность: Работа подсистемы трекинга не должна приводить к задержкам в отрисовке интерфейса (UI Lag). Все операции по записи логов и их отправке должны выполняться в низкоприоритетных асинхронных потоках.

4.1.9 Требования к транспортабельности для подвижных ИС*

Требования к транспортабельности не предъявляются.

4.1.10 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Проведение сложного обслуживания и ремонта должно осуществляться силами сервисных служб поставщика технических средств и определяется соответствующим договором на техническое обслуживание.

Ремонт технических средств должен производиться в специализированных сервисных центрах квалифицированным персоналом.

1) Условия эксплуатации и регламент эксплуатации.

Условия и регламент (режим) эксплуатации, а также виды и периодичность обслуживания технических средств должны соответствовать требованиям по эксплуатации, техническому обслуживанию, ремонту и хранению, изложенным в документации производителя. Условия эксплуатации Системы должны обеспечивать выполнение требований обеспечения надежности Системы.

Для нормальной эксплуатации разрабатываемой системы должно быть обеспечено бесперебойное питание. Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации изготовителей, но не реже одного раза в год.

Периодическое техническое обслуживание и тестирование технических средств должны включать в себя обслуживание и тестирование всех используемых средств, включая рабочие станции, серверы, кабельные системы и сетевое оборудование, устройства бесперебойного питания.

В процессе проведения периодического технического обслуживания должны проводиться внешний и внутренний осмотр и чистка технических средств, проверка

контактных соединений, проверка параметров настроек работоспособности технических средств и тестирование их взаимодействия.

Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

2) Предварительные требования к допустимым площадям для размещения персонала и технических средств системы, к параметрам сетей энергоснабжения.

Технические средства и персонал должны размещаться в существующих помещениях Заказчика, или в специально арендованных помещениях, которые по климатическим условиям должны соответствовать требованиям стандартов, установленным в Республике Узбекистан. Размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях документов с конфиденциальной информацией и технических средств.

Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

К надежности электроснабжения предъявляются следующие требования:

- с целью повышения отказоустойчивости системы в целом необходима обязательная комплектация серверов и клиентских компьютеров источником бесперебойного питания с возможностью автономной работы системы не менее 15 минут;

- обеспечение бесперебойного питания активного сетевого оборудования.

Параметры сетей энергоснабжения должен соответствовать межгосударственному стандарту «ГОСТ 32144-2013 Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения».

3) Требования к количеству, квалификации обслуживающего персонала и режиму его работы

Техническое обслуживание Системы должно осуществляться эксплуатационным персоналом Заказчика. Численность, квалификация, режим работы и функции эксплуатационного персонала, а также регламент технического обслуживания будет определяться на стадии «Ввод в эксплуатацию».

4) Требования к составу, размещению и условиям хранения комплекта запасных изделий и приборов

Система является стационарной и устанавливается на серверы Заказчика. Для функционирования системы дополнительных комплектов запасных изделий и приборов не требуется. В связи с этим, требования к составу, размещению и условиям хранения комплекта запасных изделий и приборов не предъявляется.

5) Требования к регламенту обслуживания

Обслуживание Системы должно производиться специализированным подразделением - службой эксплуатации Заказчика в соответствии с требованиями эксплуатационной документации на систему.

Специалисты, отвечающие за эксплуатацию Системы, должны обеспечивать работоспособность системных и программно-технических средств системы, их конфигурирование и настройку, осуществлять анализ функционирования программно-технических средств, отвечать на запросы пользователей системы в рамках своей компетенции.

Специалисты должны обладать достаточными знаниями в области используемых в системе информационных технологий, в рамках используемых программно-технических средств на уровне технической и эксплуатационной документации, технологии производственных процессов на уровне технологических инструкций и описания технологического процесса обработки данных, организации эксплуатации комплекса технических средств и перечня используемых ресурсов для своевременного реагирования на внештатные и аварийные ситуации при функционировании ресурсов системы, анализа и разрешения возникающих проблем.

6) Требования к санитарным нормам электромагнитного воздействия

Показатели вредных воздействий электромагнитных излучений на здоровье персонала, не должны превышать действующих норм «Санитарные нормы допустимых уровней электромагнитных полей радиочастот» (СанПиН № 0064-96). «Санитарные нормы уровней электростатических полей на рабочих местах (СанПиН №0121-01).

4.1.11 Требования к патентной и лицензионной чистоте

Проектные решения по лицензированию ПО, а также созданию Системы мобильного приложения должны отвечать требованиям по патентной чистоте согласно действующему законодательству Республики Узбекистан.

Авторские и имущественные права на предоставляемое программное обеспечение определяются в соответствии с законодательством Республики Узбекистан.

Лицензия на использование без ограничения по времени, а также без ограничения на количество пользователей.

При использовании в Системе приложения программ (программных комплексов или модулей), разработанных третьими лицами, условия, на которых передается право на использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию Системы по ее прямому назначению.

4.1.12 Требования по стандартизации и унификации

Для исключения избыточности технологических процедур при выполнении функций системы следует единообразно реализовать общие для всех функций процедуры.

Проектные решения при выполнении различных функций система должна обеспечивать:

- соблюдение единых правил организации интерфейса с пользователем;
- единообразную реакцию системы на неверные действия пользователей;
- единообразие заполнения классифицируемых реквизитов с использованием справочников;
- использование фиксированного перечня терминов и определений системы при организации диалога и формировании экранов;
- типовой подход к разграничению доступа пользователей к информации системы;
- максимальное использование средств, имеющихся в инструментальных средствах разработки системы (базовые библиотеки процедур и функций, DLL, элементы интерфейса и т. п.).

Программное обеспечение системы должно использовать объектно-ориентированный и модульный принцип построения программной системы с использованием типовых программных компонент, реализующих одни и те же функции (фрагменты функций) системы.

Одним из условий эффективного функционирования системы должно быть использование стандартных комплексов технических и программных средств, унифицированных форм документов, единых международных, отраслевых классификаторов, единых международных стандартов.

Система должна обеспечиваться унификация проектных решений, что должно обеспечиваться единообразным подходом к решению однотипных задач, унификацией технического, информационного, лингвистического, математического, информационного и организационного обеспечения Единообразный подход к решению однотипных задач должен достигаться:

- унификацией функциональной структуры в части реализации автоматизированных функций и информационных связей между ними;

- одинаковым программно-техническим способом реализации подобных функций системы и единым интерфейсом с пользователем, соответствующим международным стандартам.

Унификация технических средств системы должна достигаться за счет:

- применения серийных технических средств, соответствующих международным стандартам;

- использования типовых автоматизированных рабочих мест, компонентов и комплексов.

4.1.13 Дополнительные требования*

Дополнительные требования не предъявляются.

4.2 Требования к функциям (задачам), выполняемым системой приложения

Для каждой функциональной области системы будут внедрены процедуры регулярного обновления модулей с целью поддержания их актуальности и соответствия требованиям пользователей. Обновления будут выпущены в формате регулярных релизов (ежеквартально или по мере необходимости в случае выявления критических уязвимостей).

Для критически важных исправлений, таких как уязвимости безопасности или серьезные ошибки, будет разработан процесс экстренного патчирования, который позволит оперативно внедрять изменения без длительного тестирования, но с последующим пост-патч мониторингом производительности и стабильности системы.

Все обновления и патчи будут сопровождаться подробной документацией, включая описание внесённых изменений, инструкций по их использованию, а также возможные последствия для других модулей системы. Пользователи будут своевременно уведомляться об изменениях через автоматизированные уведомления.

В случае возникновения проблем в процессе обновления, будет разработан план действий по быстрому восстановлению работы системы, который включает откат изменений и восстановление системы из резервной копии.

4.2.1. Подсистема «Мой профиль»

Подсистема «Мой профиль» является центральным узлом управления личными данными пользователя, параметрами безопасности приложения, а также содержит

информационно-справочные сервисы Банка. Подсистема «Мой профиль» состоит из следующих модулей и подмодулей:

1. Модуль «Персональный кабинет»

Назначение модуля: Обеспечение единой точки входа для визуализации статуса пользователя и быстрого перехода к ключевым сервисам.

Основные функциональные возможности:

Отображение краткой сводки по активным продуктам и персональным уведомлениям.

Наличие прямой функциональной ссылки для перехода в расширенную веб-версию кабинета по адресу: http://new-cabinet.brb.uz/.

Быстрый доступ к редактированию профиля и настройкам приватности.

2. Модуль «Персональные данные»

Назначение модуля: Хранение и актуализация идентификационных данных клиента.

Основные функциональные возможности:

Автоматическое формирование анкеты (ФИО, ПИНФЛ, паспортные данные) на основе интеграции с ИАБС Банка и данных биометрической идентификации (Liveness Check).

Возможность инициирования обновлений персональной информации.

Обязательное биометрическое подтверждение в режиме реального времени при попытке изменения любого критически важного поля данных.

3. Модуль «AI Chat»

Назначение модуля: Автоматизированная интеллектуальная поддержка пользователей.

Основные функциональные возможности:

Предоставление мгновенных ответов на типовые вопросы с помощью искусственного интеллекта.

Поддержка мультимедийных вложений (скриншоты ошибок, фотодокументов) для детального разбора обращений.

Бесшовная передача диалога живому оператору (Модератору) при запросе сложной финансовой консультации.

4. Модуль «Контакты»

Назначение модуля: Обеспечение связи пользователя с подразделениями Банка.

Основные функциональные возможности:

Предоставление актуальных номеров контакт-центра с возможностью совершения звонка в один клик.

Интеграция со ссылками на официальные мессенджеры и социальные сети Банка.

5. Модуль «Филиалы и банкоматы»

Назначение модуля: Поиск и навигация к точкам обслуживания Банка.

Основные функциональные возможности:

Отображение объектов на интерактивной карте с использованием геолокации.

Гранулярная фильтрация объектов по типу услуг (прием наличных, валютный обмен, работа с юридическими лицами).

Отображение статуса работы объекта («открыто», «перерыв», «закрыто») в реальном времени.

6. Модуль «Курсы валют»

Назначение модуля: Информирование о котировках валют.

Основные функциональные возможности:

Отображение курсов покупки/продажи валют Банка и официального курса ЦБ.

Инструментарий калькулятора валют для предварительного расчета операций конверсии.

7. Модуль «Фондовый рынок»

Назначение модуля: Мониторинг финансовых индикаторов.

Основные функциональные возможности:

Визуализация актуальных котировок ценных бумаг и ключевых индексов рынка.

Предоставление базовой аналитической информации для клиентов-инвесторов.

8. Модуль «Реферальный код сделавшего предложение»

Назначение модуля: Управление участием в программах лояльности.

Основные функциональные возможности:

Ввод реферальных кодов для активации бонусных предложений.

Просмотр истории начислений и статусов приглашенных участников.

9. Модуль «Безопасность»

Назначение модуля: Комплексная защита доступа к приложению и управление лимитами.

Основные функциональные возможности:

Управление методами аутентификации (смена PIN-кода, включение/выключение FaceID/TouchID).

Настройка индивидуальных лимитов на транзакции (дневные/месячные), где повышение лимита требует биометрического подтверждения.

Программная активация защиты FLAG_SECURE, исключающая возможность создания скриншотов или записи видео экрана в защищенных разделах.

10. Модуль «Уведомление»

Назначение модуля: Управление системой оповещений.

Основные функциональные возможности:

Настройка пороговых сумм для получения уведомлений о списаниях.

Выбор каналов доставки сообщений (Push/SMS).

Техническое требование: Реализация модуля на базе параметризованных запросов, полностью исключающая риск проведения SQL-инъекций.

11. Модуль «Язык»

Назначение модуля: Локализация интерфейса.

Основные функциональные возможности:

Мгновенная смена языка (UZ, RU, EN) всех элементов интерфейса без необходимости повторной авторизации или перезапуска приложения.

12. Подмодуль «О приложении»

Назначение подмодуля: Идентификация программного продукта.

Основные функциональные возможности:

Отображение номера версии сборки, информации о правообладателе и ссылки на политику конфиденциальности.

13. Модуль «Оферта»

Назначение модуля: Предоставление юридической базы обслуживания.

Основные функциональные возможности:

Хранение и отображение актуальных редакций публичных договоров и условий банковского обслуживания.

Возможность экспорта документов в формат PDF для сохранения на устройстве пользователя.

4.2.2. Подсистема «Услуги»

Подсистема «Услуги» является функциональным блоком приложения, объединяющим сложные финансовые продукты, инструменты управления картами и

интеграции с государственными цифровыми платформами. Подсистема обеспечивает полный цикл дистанционного обслуживания клиента и состоит из следующих модулей:

1. Модуль «Онлайн кредиты»

Назначение модуля: Дистанционное предоставление кредитных продуктов и микрозаймов без посещения офиса Банка.

Основные функциональные возможности:

Подача электронных заявок и автоматизированный скоринг на основе данных КАТМ и ИАБС.

Обеспечение строгой атомарности транзакций: финансовый цикл открытия кредита защищен от системных сбоев (автоматический откат при ошибке).

Автоматическое зачисление кредитных средств на выбранную карту или счет пользователя.

2. Модуль «Онлайн конверсия»

Назначение модуля: Мгновенный обмен валют между счетами пользователя в режиме реального времени.

Основные функциональные возможности:

Покупка и продажа иностранной валюты по внутреннему курсу Банка в режиме 24/7.

Использование инструментария калькулятора для предварительного расчета суммы операции перед подтверждением.

3. Модуль «Онлайн депозиты»

Назначение модуля: Дистанционное управление сбережениями и открытие вкладов.

Основные функциональные возможности:

Открытие, пополнение и частичное снятие средств с депозитных счетов согласно условиям выбранного продукта.

Визуализация накопленных процентов и управление пролонгацией договоров.

4. Модуль «Кредитная безопасность»

Назначение модуля: Защита пользователя от мошеннических действий и контроль доступа к кредитным продуктам (КАТМ).

Основные функциональные возможности:

Установка добровольного запрета на получение кредитов через интеграцию с государственными системами.

Обязательное биометрическое подтверждение в режиме реального времени при попытке изменения статуса запрета.

5. Модуль «QR-оплата»

Назначение модуля: Обеспечение быстрых бесконтактных расчетов за товары и услуги.

Основные функциональные возможности:

Сканирование QR-кодов для мгновенной оплаты в торговых точках и сервисах.

Генерация персональных кодов для проведения транзакций между пользователями.

6. Модуль «Погашение кредита»

Назначение модуля: Инструментарий для своевременного исполнения долговых обязательств.

Основные функциональные возможности:

Просмотр актуального графика платежей и остатка задолженности.

Погашение кредитов, оформленных как в текущем Банке, так и в сторонних финансовых организациях.

7. Модуль «Управление картами»

Назначение модуля: Комплексное администрирование активных карточных продуктов пользователя.

Основные функциональные возможности:

Установка и изменение лимитов на операции, смена ПИН-кода и временная блокировка карты.

Отображение реквизитов карты с использованием защиты от копирования экрана (FLAG_SECURE).

8. Модуль «Visa direct»

Назначение модуля: Мгновенные международные переводы на карты платежной системы Visa.

Основные функциональные возможности:

Отправка денежных средств по номеру карты получателя в любую страну мира, поддерживающую технологию.

9. Модуль «Снять наличные»

Назначение модуля: Обеспечение доступа к наличности без использования физического носителя.

Основные функциональные возможности:

Генерация разовых цифровых кодов для снятия средств в банкоматах Банка.

10. Модуль «Заказать карту»

Назначение модуля: Дистанционная подача заявки на выпуск физического платежного инструмента.

Основные функциональные возможности:

Выбор типа карты и точки доставки или самовывоза.

Отслеживание статуса изготовления и готовности карты.

11. Модуль «Зарплатная карта»

Назначение модуля: Специализированное обслуживание участников зарплатных проектов.

Основные функциональные возможности:

Управление специфическими лимитами и доступ к льготным продуктам, привязанным к зарплатному счету.

12. Модуль «Карта Momentum»

Назначение модуля: Работа с картами мгновенной выдачи.

Основные функциональные возможности:

Быстрая активация и привязка неименных карт к профилю пользователя.

13. Модуль «Виртуальная карта»

Назначение модуля: Мгновенная эмиссия цифровых карт для безопасных расчетов в сети Интернет.

Основные функциональные возможности:

Выпуск карты без физического носителя в течение нескольких секунд.

Полное управление балансом и реквизитами из приложения.

14. Модуль «Международные переводы»

Назначение модуля: Трансграничные перемещения средств через различные системы денежных переводов.

Основные функциональные возможности:

Отправка и получение средств с автоматической конвертацией и проверкой по требованиям валютного контроля.

15. Модуль «My.gov.uz услуги»

Назначение модуля: Интеграция с Единым порталом интерактивных государственных услуг.

Основные функциональные возможности:

Получение справок, выписок и государственных услуг напрямую через банковское приложение.

16. Модуль «Моя машина»

Назначение модуля: Управление данными и платежами, связанными с автотранспортом.

Основные функциональные возможности:

Проверка и оплата штрафов ГАИ, мониторинг данных страховых полисов и доверенностей.

4.2.3. Подсистема «Оплата»

Подсистема «Оплата» предназначена для обеспечения удобного и безопасного интерфейса проведения платежей в пользу поставщиков услуг, государственных органов и коммерческих организаций. Она минимизирует необходимость посещения касс и использования сторонних сервисов, объединяя все финансовые обязательства пользователя в едином интерфейсе. Подсистема «Оплата» состоит из следующих модулей:

1. Модуль связи и IT-инфраструктуры

(Мобильные операторы, Интернет-провайдеры, Телефония, Хостинг-провайдеры)

Назначение модуля: Обеспечение бесперебойной оплаты услуг связи, доступа в сеть и ИТ-ресурсов.

Основные функциональные возможности:

Мгновенное пополнение баланса по номеру телефона или лицевому счету.

Интеграция с API провайдеров для проверки задолженности в реальном времени.

Поддержка оплаты международных операторов связи.

2. Модуль коммунальных услуг и медиа

(Коммунальные услуги, Телевидение и онлайн-вещание, Онлайн-сервисы)

Назначение модуля: Регулярная оплата бытовых нужд и доступа к развлекательному

контенту.

Основные функциональные возможности:

Получение актуальных счетов за электроэнергию, газ, воду и вывоз мусора по ПИНФЛ или кадастровому номеру.

Подписка на уведомления о выставленных счетах и автоплатежи.

Оплата подписок на онлайн-кинотеатры и стриминговые платформы.

3. Модуль государственных и бюджетных платежей

(Гос. услуги и штрафы ГАИ, Реквизитные и бюджетные платежи, Юридические услуги)

Назначение модуля: Исполнение обязательств перед государственным бюджетом и оплата правовых услуг.

Основные функциональные возможности:

Поиск и оплата штрафов ГУБДД (ГАИ) по номеру техпаспорта или протокола.

Оплата государственных пошлин и услуг через интеграцию с платежными системами электронного правительства.

Проведение платежей по произвольным банковским реквизитам.

4. Модуль финансовых и страховых услуг

(Погашение кредитов и рассрочек, Электронные кошельки, Страхование)

Назначение модуля: Управление внешними долгами, пополнение платежных инструментов и покупка страховых продуктов.

Основные функциональные возможности:

Перевод средств на счета сторонних микрокредитных организаций и маркетплейсов для закрытия рассрочек.

Прямое пополнение популярных электронных кошельков.

Дистанционное оформление и продление страховых полисов (ОСАГО и др.).

5. Модуль коммерции, транспорта и туризма

(Интернет-магазины, Объявления и реклама, Транспорт, Авиа и ж.-д. билеты, Отели и туризм, Зарядные станции)

Назначение модуля: Оплата покупок, бронирование билетов и логистические расходы.

Основные функциональные возможности:

Прямая оплата заказов в маркетплейсах и сервисах объявлений (продвижение, реклама).

Бронирование и выкуп авиационных и железнодорожных билетов с получением

квитанции в приложении.

Оплата услуг зарядки электромобилей и пополнение транспортных карт.

6. Модули образования, досуга и благотворительности

(Обучение, Благотворительность, Игры и соц. сети)

Назначение модуля: Оплата образовательных контрактов, досуга и социальных инициатив.

Основные функциональные возможности:

Оплата контрактов ВУЗов, школ и детских садов по идентификатору учащегося.

Перечисление пожертвований в проверенные благотворительные фонды.

Пополнение игровых аккаунтов и покупка виртуальных товаров в социальных сетях.

Технические требования для модулей подсистемы «Оплата»:

Надежность: Обеспечение атомарности платежа — исключение ситуаций, когда списание произошло, а зачисление у провайдера не подтверждено (автоматический откат/Rollback).

Безопасность: Использование параметризованных запросов для исключения SQL-инъекций и обязательное подтверждение биометрией платежей свыше установленного лимита.

Документирование: Формирование электронного фискального чека в PDF по каждой операции.

4.2.4. Модуль «Переводы»

Модуль «Переводы» предназначен для обеспечения быстрых и защищенных перемещений денежных средств как между собственными счетами пользователя, так и в адрес сторонних получателей. Модуль минимизирует время на проведение типовых операций и гарантирует точность взаиморасчетов. Модуль «Переводы» состоит из следующих подмодулей:

1. Подмодуль «Перевод на мою карту»

Назначение подмодуля: Оперативное распределение денежных средств между собственными картами и счетами пользователя (включая карты Humo, Uzcard и виртуальные карты).

Основные функциональные возможности:

Визуализация доступных остатков на всех привязанных картах в режиме реального времени.

Выбор карты списания и карты зачисления в едином интерфейсе с мгновенным

исполнением операции.

Техническое требование: Обеспечение синхронного отражения балансов в ИАБС сразу после завершения транзакции.

2. Подмодуль «Недавние получатели»

Назначение подмодуля: Сокращение времени на проведение повторных транзакций за счет хранения истории контрагентов.

Основные функциональные возможности:

Автоматическое сохранение реквизитов (номер карты, ФИО получателя, маскированный номер телефона) после первого успешного перевода.

Интеллектуальная сортировка списка получателей по частоте использования и дате последней операции.

Возможность удаления или редактирования данных получателя в списке быстрого доступа.

3. Подмодуль «Запросить деньги»

Назначение подмодуля: Формирование запросов на получение денежных средств от других клиентов Банка или через внешние каналы связи.

Основные функциональные возможности:

Генерация счета-запроса с указанием конкретной суммы и назначения платежа.

Отправка запроса через внутренние Push-уведомления (для клиентов Банка) или в виде платежной ссылки/QR-кода для внешних мессенджеров.

Отслеживание статуса запроса (ожидание, оплачено, отклонено) в истории операций.

Технические требования для подсистемы «Переводы»:

Интеллектуальная валидация: Обязательная проверка номера карты получателя на стороне мобильного клиента до отправки запроса на сервер.

Безопасность данных: Использование программного механизма FLAG_SECURE для защиты экранов ввода реквизитов от копирования или трансляции.

Гарантия транзакционности: Техническая поддержка обязана гарантировать «атомарность» переводов. В случае обрыва связи в момент обработки, система должна автоматически завершить операцию либо осуществить возврат средств (Rollback), исключая их «зависание» на промежуточных счетах.

Логирование: Исправление системы обработки исключений (замена пустых блоков catch на содержательные логи) для возможности восстановления деталей перевода при возникновении технических инцидентов.

4.2.5. Модуль «Мониторинг»

Модуль «Мониторинг» предназначен для обеспечения прозрачности финансовых потоков пользователя, предоставления инструментов аналитики и контроля за исполнением банковских операций. Модуль служит инструментом финансового планирования и верификации всех действий, совершенных в приложении. Модуль «Мониторинг» состоит из следующих подмодулей:

1. Подмодуль «История транзакций»

Назначение подмодуля: Формирование и отображение единого реестра всех финансовых событий пользователя (списания, зачисления, переводы, оплаты).

Основные функциональные возможности:

Детализированный просмотр каждой операции: дата, время, MCC-код, сумма комиссии и итоговый статус.

Многокритериальный поиск и фильтрация операций по типу продукта (карты, счета), категориям услуг и временным интервалам.

Повтор любого успешного платежа или перевода напрямую из экранной формы истории.

Формирование и выгрузка электронных квитанций и выписок по выбранным операциям.

2. Подмодуль «Аналитика расходов»

Назначение подмодуля: Визуализация структуры трат пользователя для эффективного управления личным или семейным бюджетом.

Основные функциональные возможности:

Графическое отображение распределения расходов по категориям («Транспорт», «Коммунальные платежи» и т.д.).

Сравнение динамики трат за различные отчетные периоды (месяц к месяцу, год к году).

Установка бюджетных лимитов на определенные категории с уведомлением пользователя при их достижении.

3. Подмодуль «Статус исполнения услуг»

Назначение подмодуля: Отслеживание прохождения сложных многоэтапных процессов, требующих взаимодействия с внешними системами (кредиты, госуслуги).

Основные функциональные возможности:

Мониторинг этапов обработки заявок на кредиты, депозиты или выпуск карт.

Отображение статусов взаимодействия с государственными шлюзами (My.gov.uz) и внешними провайдерами.

Оповещение пользователя о необходимости совершения дополнительных действий для успешного завершения процесса.

Технические требования для модуля «Мониторинг»:

Интеграция с системой логирования: Каждое событие в мониторинге должно быть связано с системным логом.

Синхронность данных: Обеспечение обновления статусов в режиме «близком к реальному времени» (Near Real-Time) за счет оптимизации кэширования и запросов к ИАБС.

Безопасность (Privacy): В интерфейсе мониторинга должна быть реализована возможность временного скрытия балансов и сумм операций (режим «Инкогнито») для защиты конфиденциальности в общественных местах.

Архитектурная чистота: Использование оптимизированных индексов в базе данных для мгновенной подгрузки истории, исключая задержки при наличии большого количества транзакций (устранение проблем производительности

4.3 Требования к видам обеспечения

4.3.1 Требования к математическому обеспечению*

Специальных требования к математическому обеспечению не предъявляются. При разработке необходимо использование наиболее оптимальных стандартных математических методов и моделей, типовых алгоритмов.

4.3.2 Требования к информационному обеспечению

Система должна соответствовать требованиям информационной безопасности согласно законодательству РУз, Постановлению ЦБ №3224, а также стандартам O'z DSt ISO/IEC 27001:2018 и O'z DSt 2875:2014.

Для корректного отображения всех языковых групп, включая китайские иероглифы, вся система (БД, API, мобильные клиенты) должна поддерживать кодировку UTF-8. Использование иных кодировок, ограничивающих набор символов, не допускается.

Основные характеристики и требования:

Управление секретами: Пароли, API-ключи, токены и реквизиты доступа к базам данных (DB credentials) должны храниться исключительно в специализированных защищенных хранилищах (Vault/KMS). Прямое хранение в коде запрещено.

Контроль среды исполнения: Внедрение механизмов проверки целостности среды (Root/Jailbreak detection). Установлен строгий запрет на работу приложения на рутованных устройствах, эмуляторах и при использовании инструментов отладки (debuggers).

Защита от перебора: Реализация мер против Brute-force и Password Spraying. Внедрение ограничений на количество попыток, временных задержек и механизмов блокировки IP-адресов.

Анти-бот и анти-фрод: Защита от Credential stuffing и автоматизированных ботнетов через анализ аномалий, проверку репутации IP и применение Step-up аутентификации.

Контроль сессий: Наличие механизмов немедленного отзыва токена (Token revoke / Force logout) при смене пароля, устройства или выявлении угрозы.

Административная безопасность: Внедрение модели доступа RBAC. Доступ к панели администратора должен быть закрыт из внешних сетей, защищен через MFA и ограничен списком разрешенных IP (Allowlist).

Логирование и аудит: Полный запрет на удаление системных логов. Обеспечение их непрерывной передачи в системы мониторинга (SIEM).

Маскирование данных: Все конфиденциальные данные (номера карт, ПИН-коды, OTP, персональные данные) в логах и базах данных должны быть маскированы.

Состав, структура и способы организации данных в Системе должны быть определены на этапе рабочего проектирования. Информационный обмен данными в системе должен осуществляться с помощью разработанного коммуникационного протокола передачи данных.

Состав данных профиля клиента Банка

Информационная модель профиля клиента должна включать следующие обязательные атрибуты, получаемые через интеграцию с Государственными ИС и ИАБС Банка:

ИНН/ПИНФЛ.

Фамилия, Имя, Отчество.

Дата, место и страна рождения.

Пол, гражданство.

Тип документа, серия и номер паспорта, дата выдачи и срок окончания действия.

Страна проживания, область, район, полный адрес проживания.

Основной телефон, мобильный телефон.

Семейное положение

Код филиала Банка

Данные в ИС должны храниться в резервной базе данных под управлением современной реляционной системы управления базами данных. Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД. База данных должна быть структурирована согласно правилам нормализации и иметь следующие основные разделы:

– раздел данных, обеспечивающий возможность централизованного хранения, наполнения и представления данных по показателям;

– раздел служебных данных, формируемый администраторами системы и обеспечивающий работу программного обеспечения

– раздел данных, позволяющий вести мониторинг действий пользователей и ход исполнения функций системы (журналы мониторинга работы системы, действий пользователей и т.д.).

Организация базы данных должна соответствовать требованиям O'zDSt 1135:2007.

Информационное обеспечение системы мобильного приложения должно быть достаточным для выполнения всех автоматизированных функций Системы.

Информационное обеспечение мобильного приложения должно быть совместимо с информационным обеспечением систем, взаимодействующих с ней, по содержанию, системе кодирования, методам адресации, форматам данных и форме представления информации, получаемой и выдаваемой системой.

Перечень баз данных для работы системы должны быть определены в процессе разработки системы.

При разработке системы приложения должны использоваться стандартные, принятые и зарегистрированные классификаторы, унифицированные формы документов и справочных данных.

Система мобильного приложения должна иметь возможность подключения к базам данных «Электронного правительства» (БД физических лиц и БД юридических лиц) и Единому регистру справочников и классификаторов.

В процессе разработки системы будет учтен тот момент, что все модули системы должны взаимодействовать друг с другом.

Информация в базе данных системы должна сохраняться при возникновении аварийных ситуаций.

Резервное копирование данных должно осуществляться на регулярной основе, в объёмах, достаточных для восстановления информации в подсистеме хранения данных.

В рамках реализации проекта предусматривается использование персональных данных клиентов Банка, ранее зарегистрированных в текущем мобильном приложении для

физических лиц.

Источником персональных данных действующих пользователей является база данных существующего мобильного приложения Банка, а также связанные с ней внутренние информационные системы (включая IABS и процессинговые системы).

В рамках запуска нового мобильного приложения должны быть обеспечены:

– корректная миграция (или синхронизация) персональных данных пользователей;

– сохранение идентификаторов клиентов (Client ID, ПИНФЛ, номера телефонов и иных уникальных ключей);

– обеспечение целостности, актуальности и непротиворечивости данных;

– исключение дублирования клиентских записей;

– сохранение истории операций и связки с банковскими продуктами клиента.

Передача и обработка персональных данных должны осуществляться с соблюдением:

– законодательства Республики Узбекистан о защите персональных данных;

– внутренних политик информационной безопасности Банка;

– требований PCI DSS (при обработке карточных данных);

– регламентов по защите банковской тайны.

4.3.3 Требования к лингвистическому обеспечению

Приложение должно предусматривать языковую поддержку интерфейсов пользователей, в зависимости от настроечных данных. Должны поддерживаться следующие языки: узбекский (шрифт – латиница), русский (шрифт – кириллица), английский и китайский. Информация в базе должна храниться на том языке, на котором она была введена.

4.3.4 Требования к программному обеспечению

Программное обеспечение Системы должно быть лицензионным (или Open Source без ограничений на коммерческое использование) и строиться на базе микросервисной архитектуры, обеспечивающей независимое масштабирование модулей и доступность в режиме 24/7. Реализация интерфейса мобильного приложения должна базироваться на поэтапной стратегии: на первом этапе обеспечивается строго нативная разработка для iOS (Swift не ниже 5.x, Clean Swift/MVVM) и Android (Kotlin не ниже 1.9.x, Jetpack, MVVM/MVI) для реализации критического функционала, включая биометрию (FaceID/TouchID), криптографию и SDK Uzcard/Humo. На втором этапе внедряется гибридная архитектура с использованием веб-контейнеров и фреймворков (React или

Vue.js) для динамического обновления разделов (акции, справочники, маркетплейс) без переопубликации в App Store и Google Play, включая поддержку JSON-структур для управления интерфейсом с сервера.

Серверная часть системы должна реализовываться на языке Java (последней актуальной версии) с использованием фреймворков Spring Boot / Spring Cloud, транзакционной БД PostgreSQL и кэширования в Redis. Асинхронное взаимодействие микросервисов должно обеспечиваться брокерами сообщений Apache Kafka или RabbitMQ, а высокоскоростной внутренний обмен данными — протоколом gRPC. Для обеспечения отказоустойчивости и автоматического восстановления («самолечения») сервисов развертывание всех компонентов должно осуществляться исключительно с применением технологий контейнеризации Docker и оркестрации Kubernetes (K8s). Безопасность серверной части должна гарантироваться внедрением API Gateway для авторизации и защиты от DoS/DDoS атак, а также шифрованием данных (Data-at-rest и Data-in-transit) с использованием протокола TLS 1.3.

Требования к безопасной разработке и контейнеризации

«Программное обеспечение поставляется в виде автономных защищенных модулей (Docker-контейнеров). Они собраны по строгим стандартам безопасности и содержат внутри всё необходимое для стабильной работы, что исключает ошибки при установке».

Использование технологии Multi-stage build гарантирует, что внутри контейнера останется только сама программа. Все вспомогательные инструменты сборки удаляются на этапе производства. В качестве основы используется защищенная система Alpine Linux.

Внутри контейнеров запрещено использование прав администратора (root). Приложение запускается от имени пользователя с минимальными полномочиями, достаточными только для выполнения конкретной задачи.

Каждый этап сборки приложения контролируется сканерами уязвимостей Trivy или Snyk. Если в используемых библиотеках обнаруживается брешь в безопасности, процесс сборки блокируется до тех пор, пока разработчик не исправит уязвимость.

Процесс разработки обязан соответствовать стандарту ISO/IEC 12207 и включать автоматизированные конвейеры CI/CD с обязательной интеграцией инструмента статического анализа Sonar Qube (Sonar). Без успешного прохождения порогов качества (Quality Gates) деплой запрещен; установлены следующие критерии: полное отсутствие критических багов и уязвимостей, покрытие кода Unit-тестами не менее 80%, уровень дублирования кода не более 5% и обязательная проверка всех Security Hotspots. Система должна поддерживать RESTful API с документированием в Swagger/OpenAPI и обеспечивать полноценную локализацию на узбекском, русском, английском и китайском

языках (UTF-8). Исполнитель гарантирует лицензионную чистоту кода, отсутствие недекларированных возможностей и ведение детальных журналов системных сообщений для аудита безопасности.

4.3.5 Требования к техническому обеспечению

Используемые технические средства должны обладать достаточными количественными и качественными показателями для обеспечения высокой доступности и производительности системы мобильного приложения в режиме реального времени.

Для стабильной работы микросервисной архитектуры и соблюдения целевого времени отклика системы (Response Time) аппаратная конфигурация должна учитывать затраты ресурсов на фоновые процессы безопасности (мониторинг, логирование и шифрование трафика).

К техническим средствам системы мобильного приложения относятся:

Серверы баз данных (СУБД);

Серверы приложений Системы (API Gateway, Backend-сервисы).

Минимальные требования к аппаратному обеспечению для роли «Сервер базы данных»:

Процессор (CPU): Не менее 16 ядер, работающих на тактовой частоте не ниже 3,0 ГГц. Увеличение количества ядер необходимо для эффективного выполнения процедур репликации и архивации данных без ущерба для скорости обработки основных транзакций.

Оперативная память (RAM): Не менее 128 ГБ. Объем памяти должен обеспечивать эффективное кэширование данных СУБД для минимизации задержек при операциях чтения/записи.

Жесткий диск: Не менее 2000 ГБ. Рекомендуется использование SSD/NVMe дисков корпоративного класса с высоким показателем IOPS для поддержки интенсивных операций обмена данными.

Сетевой интерфейс: Выделенный сетевой адаптер для обеспечения бесперебойной работы между серверами и выполнения задач репликации данных.

Минимальные требования к аппаратному обеспечению для роли «Сервер приложений системы»:

Процессор (CPU): Не менее 16 ядер, работающих на тактовой частоте не ниже 3,0 ГГц. Дополнительные ядра позволяют распределять нагрузку между изолированными Docker-контейнерами и выполнять автоматическое сканирование безопасности без замедления работы приложения.

Оперативная память (RAM): Не менее 128 ГБ. Данный объем важен для нормального функционирования среды оркестрации контейнеров и поддержания стабильной работы всех микросервисов в оперативной памяти.

Жесткий диск: Не менее 2000 ГБ.

Сетевой интерфейс: Высокоскоростной сетевой интерфейс для обеспечения связи между фронтенд-частью, бэкенд-сервисами и базами данных внутри защищенного периметра.

4.3.6 Требования к метрологическому обеспечению*

Требования не предъявляются.

4.3.7 Требования к организационному обеспечению

Организационное обеспечение мобильного приложения должно быть достаточным для эффективного выполнения персоналом возложенных на него обязанностей при осуществлении автоматизированных и связанных с ними неавтоматизированных функций системы.

Должны быть определены должностные лица, ответственные за:

- обработку информации;
- администрирование;
- обеспечение безопасности информации;
- управление работой персонала по обслуживанию.

К работе с системой мобильного приложения должны допускаться работники, имеющие навыки работы на персональном компьютере и мобильных устройствах, ознакомленные с правилами эксплуатации и техники безопасности.

Необходимы обязательные инструктажи пользователей, в том числе по технике безопасности.

4.3.8 Требования к методическому обеспечению

Мобильная платформа «BRB» для физических лиц должна разрабатываться на основании действующих нормативных правовых актов и организационно-распорядительных документов заказчика. Следовательно, в рамках разработки, данного мобильного приложения, должны быть учтены соответствующие административные регламенты заказчика, в которых должны быть определены процессы деятельности и функции подразделений, а также сотрудников объектов заказчика, их права, обязанности и ответственности по использованию данной системы. Также, должны быть утверждены в

установленном порядке инструкции выполнения пользователями операций в работе с Системой приложения. Состав методического обеспечения будет уточняться в процессе разработки ПО и согласовывается с Заказчиком. Методическое обеспечение предоставляется по требованию Разработчика и состоит из:

- нормативных правовые документы;
- инструкции пользователей ПО;
- должностные инструкции персонала, выполняющего работы с использованием Системы и ее компонентов.

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Контроль, испытания и приемка ИС должны осуществляться на основании ГОСТ 34.603-92, согласно которому устанавливаются следующие основные виды испытаний:

1) предварительные;

2) опытная эксплуатация;

3) приемочные (промышленная).

Предварительные испытания следует выполнять после проведения разработчиком отладки и тестирования поставляемого программного решения и представления им соответствующих документов об их готовности к испытаниям, а также после ознакомления персонала с ее эксплуатационной документацией.

Опытную эксплуатацию проводят с целью определения соответствия функции приложения к предъявляемым требованиям.

Приемочные испытания проводят для определения ее соответствия техническому заданию, оценки качества опытной эксплуатации и решения вопроса о возможности приемки ее в постоянную эксплуатацию.

При испытаниях проверяют:

1) качество выполнения комплексом программных и технических средств автоматических функций во всех режимах функционирования Приложения, согласно Техническому заданию;

2) знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования, согласно Техническому заданию;

3) полноту содержащихся в эксплуатационной документации указаний персоналу по выполнению им функций во всех режимах функционирования системы, согласно Техническому заданию;

4) количественные и (или) качественные характеристики выполнения автоматических и автоматизированных функций системы приложения в соответствии с Техническим заданием;

5) другие свойства приложения, которым она должна соответствовать по Техническому заданию.

Прием проводимых работ и ввод в эксплуатацию Приложения должны осуществляться специальной Комиссией Заказчика с обязательным участием Исполнителя.

Приемочные испытания проводят для определения соответствия мобильного приложения настоящему ТЗ.

Тестовые испытания мобильного приложения производятся на объекте Исполнителя.

По результатам своей работы Комиссия оформляет Акт приемки работ, который подписывается всеми членами Комиссии и представляется на утверждение Заказчику, иначе должны быть составлены протоколы проведения испытаний с указанием замечаний и сроков их устранения.

Возникшие в процессе испытаний и опытной эксплуатации дополнительные требования Заказчика, не предусмотренные в настоящем ТЗ, не будут являться основанием для отрицательной оценки и могут быть удовлетворены по дополнительному соглашению в согласованные сроки.

7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ДЕЙСТВИЕ

7.1. Технические мероприятия

В ходе выполнения проекта на объекте автоматизации требуется выполнить работы по подготовке к вводу Мобильной платформы «BRB» в действие. При подготовке к вводу в эксплуатацию должно быть обеспечено выполнение следующих работ:

- определить подразделение и ответственных должностных лиц, ответственных за внедрение и проведение опытной эксплуатации;

- обеспечить присутствие пользователей для обучения работе с системой мобильного приложения, проводимым Исполнителем;

- обеспечить соответствие помещений и рабочих мест пользователей приложения в соответствии с требованиями;

- обеспечить выполнение требований, предъявляемых к программно-техническим средствам, на которых должна быть развернута информационная система;

- совместно с Исполнителем подготовить план развертывания системы мобильного приложения на технических средствах Заказчика;

- провести опытную эксплуатацию.

Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу мобильного приложения в действие, включая перечень основных мероприятий и их исполнителей должны быть, уточнены на стадии подготовки рабочей документации и по результатам опытной эксплуатации.

7.2. Обучение персонала

До передачи мобильной платформы в использование, Разработчик должен подготовить Руководство пользователя, Руководство Администратора и провести тренинг-обучение персонала Заказчика по использованию Системы и ее техническому сопровождению, основываясь на данной документации.

Программа обучения пользования системой будет разбита на категории/модули в зависимости от уровней сложности и профиля пользователей. Например, для базовых пользователей (нетехнический персонал) будут разработаны отдельные модули по использованию основных функций системы, для администраторов и технического персонала — углубленные модули по настройке и поддержке системы.

Будет предусмотрено проведение очных и онлайн семинаров с периодичностью раз в месяц, в ходе которых пользователи смогут ознакомиться с основными и продвинутыми функциями системы. Практическое обучение будет включать работу в тестовой среде системы для отработки навыков в реальных сценариях.

По завершении обучения для всех категорий пользователей будет проводиться тестирование с целью оценки уровня усвоения материала.

Для обеспечения доступности информации будут разработаны подробные текстовые и видео-руководства по работе с системой. Эти материалы будут доступны через внутренний портал системы и будут охватывать как базовые, так и расширенные функции. Особое внимание будет уделено обучению пользователей с разным уровнем технической подготовки.

Также будет разработан раздел FAQ, который будет регулярно обновляться на основе запросов пользователей. Также будет интегрирован чат-бот, способный предоставлять пользователям оперативные консультации и перенаправлять к соответствующим учебным материалам.

В течение первых шести месяцев после внедрения системы будет обеспечена пост-выводная поддержка с дежурными консультантами, которые смогут оперативно решать вопросы и предоставлять помощь по работе с системой.

После ввода системы в эксплуатацию будет действовать программа пост-выводной поддержки, которая будет включать индивидуальные консультации для пользователей, оперативное решение возникающих проблем и корректировки учебных материалов на основании реальной эксплуатации.

На регулярной основе будет собираться обратная связь от пользователей для оценки эффективности обучения. На основе этой информации будет проводиться корректировка обучающих материалов, добавление новых инструкций и рекомендаций, что обеспечит актуальность программы обучения.

Эти меры должны обеспечить качественное обучение всех категорий пользователей и помогут минимизировать риски, связанные с недостаточной подготовкой сотрудников.

7.3 Требования к эксплуатации

Процессы сопровождения системы должны соответствовать стандарту ISO/IEC 20000. Исполнитель внедряет инструменты визуализации состояния (Prometheus, Grafana) и централизованный сбор логов. Любое изменение в программной или аппаратной конфигурации в продуктивной среде должно проходить через процедуру управления изменениями (Change Management) с обязательным согласованием комитетом по изменениям (CAB).

Обновления внедряются по технологии «бесшовного» развертывания (Rolling Update). К каждому релизу Исполнитель прикладывает верифицированный план отката (Rollback plan), гарантирующий возврат к стабильной версии в течение 10 минут. В рамках управления рисками цепочки поставок (Supply-chain risk) Исполнитель ежеквартально проводит аудит сторонних библиотек (Open Source), обеспечивая их обновление до безопасных версий. Эксплуатационный цикл включает обучение технического персонала Заказчика и предоставление полной документации по администрированию инфраструктуры.

Любое вмешательство в работающую систему должно быть прозрачным и предсказуемым.

Каждое обновление системы — от маленького исправления до новой версии — фиксируется в системе учета заявок (тикетов). Это позволяет отследить, кто, когда и зачем внес изменения.

Перед внедрением любого обновления Исполнитель обязан подготовить сценарий быстрого возврата (Rollback plan). Если после обновления мониторинг зафиксирует сбои или ошибки, система должна иметь возможность в течение нескольких минут вернуться к предыдущему стабильному состоянию.

Инфраструктура должна быть оснащена системой мгновенных уведомлений, которая информирует службу поддержки о любых отклонениях от нормальной работы еще до того, как проблему заметят пользователи.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Перечень документов технического и рабочего проектирования должен соответствовать номенклатуре, приведенной в O‘zDSt 1985:2018. Исполнитель по результатам выполненных работ должен предоставить полный комплект документов, необходимых для эксплуатации Информационной системы и отражающих текущее состояние при его сдаче в промышленную эксплуатацию.

Комплект документов технического проекта Передаваемая в (Заказчику) представляется в 2-ух экземплярах печатном виде, а также дополнительно в электронном виде (на компакт-дисках, флэш-накопителе).

Проектная документация должна согласовываться и утверждаться Заказчиком.

Ниже приведён перечень документации, которая должна быть передана Заказчику на этапах тестирования мобильного приложения и при подписании Акта о вводе в опытную эксплуатацию.

В состав документов должны быть включены все необходимые документы, включая следующие:

- Общее описание разработанного мобильного приложения;
- Программа и методика испытаний разработанного приложения;
- Руководство пользователя разработанного мобильного приложения»;
- Руководство Администратора разработанного мобильного приложения».

Ответственные за разработку технического задания:

Директор Департамента Цифрового
Бизнеса АКБ «Банк развития бизнеса» _____ Г. Мавланов
(подпись)

Проектный менеджер _____
(подпись)

Бизнес аналитик _____
(подпись)

согласные: Ғ.Мавланов, Б. Шамсиев, З.Орифхўжаев

https://hujjat.brb.uz/?pin=aT25bR41&id=09b56d2c-46e4-48ff-bf84-e443f5ae47c4