



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

**«31» октябрь 2025 г.
№ 284**

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на разработку мобильного приложения
для физических лиц
на 71 листах
действует с «___» _____ 2025 г.

Ташкент – 2025 г.

Оглавление

ОБЩИЕ СВЕДЕНИЯ	5
1.1. Полное наименование МП и ее условное обозначение.....	5
1.2. Наименование организации заказчика	5
1.3. Перечень документов, на основании которых создается МП	5
1.4. Плановые сроки начала и окончания работ по созданию МП.....	6
1.5. Порядок оформления и предъявления Заказчику результатов работ	6
2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ	7
2.1. Назначение МП.....	7
2.2. Цели создания МП	8
3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	9
4 ТРЕБОВАНИЯ К МОБИЛЬНОМУ ПРИЛОЖЕНИЮ	12
4.1 Требования к МП в целом.....	12
4.1.1 Требования к структуре и функционированию МП.....	12
4.1.1.1 Перечень подсистем, их назначение и основные характеристики	15
4.1.1.2 Перечень сторонних ИС, с которыми должно быть обеспечено взаимодействие.....	17
4.1.1.3 Требования к режимам функционирования приложения, определяющим функционирование системы мобильного приложения в нормальном и аварийном режиме.....	19
4.1.1.4 Перечень и описание сценариев использования	21
4.1.1.5 Требования по диагностированию	32
4.1.1.6 Перспективы развития, модернизации МП	33
4.1.2 Требования к взаимодействию со сторонними информационными системами.....	33
4.1.3 Требования к численности и квалификации пользователей	34
4.1.4 Показатели назначения	35
4.1.5 Требования к надежности.....	37
4.1.6 Требования безопасности	40
Требования к обеспечению ИБ при проектировании и разработке.....	40
4.1.7 Требования к эргономике и технической эстетике.....	46
4.1.8 Требования к транспортабельности для подвижных ИС*	49
4.1.9 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы	49
4.1.10 Требования к патентной и лицензионной чистоте.....	51
4.1.11 Требования по стандартизации и унификации	51
4.1.12 Дополнительные требования*	52
4.2 Требования к функциям (задачам), выполняемым системой приложения	53
4.2.1. Модуль «Регистрация пользователей»	53
4.2.2. Модуль «Персональный кабинет и профиль пользователя».....	54
4.2.3. Модуль «Управление картами»	55

4.2.4.	Модуль «СМС служба».....	55
4.2.5.	Модуль «Переводы P2P»	56
4.2.6.	Модуль «Платежи и история платежей»	57
4.2.7.	Модуль «Администрирование»	57
4.2.8.	Модуль «Интеграции»	58
4.2.9.	Модуль «Депозиты».....	59
4.2.10.	Модуль «Кредиты»	60
4.2.11.	Модуль «Валютные операции».....	60
4.3	Требования к видам обеспечения	61
4.3.1	Требования к математическому обеспечению*	61
4.3.2	Требования к информационному обеспечению	61
4.3.3	Требования к лингвистическому обеспечению	62
4.3.4	Требования к программному обеспечению	62
4.3.5	Требования к техническому обеспечению	63
4.3.6	Требования к метрологическому обеспечению*	64
4.3.7	Требования к организационному обеспечению	64
4.3.8	Требования к методическому обеспечению	64
5.	СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ.....	65
6.	ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ	66
7.	ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ДЕЙСТВИЕ	67
7.1.	Технические мероприятия.....	67
7.2.	Обучение персонала.....	68
8.	ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ	69

Сокращения и определения

НИББД	Национальная информационная база банковских депозиторов
МП	Мобильное приложение — программное изделие, разновидность прикладного программного обеспечения, предназначенная для работы на смартфонах, планшетах и других мобильных устройствах. Обеспечивает без привязки к компьютеру, необходимые пользователю взаимодействия с интернетом
O'z DST	Государственный стандарт Республики Узбекистан
АКБ «БРБ»	Акционерный коммерческий банк «Банк развития бизнеса»
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
Администратор	Учетная запись пользователя, которая имеет полный доступ к системе и позволяет вносить изменения, влияющие на других пользователей.
Модератор	Следит за соблюдением правил на общественных сетевых ресурсах. Имеет более узкие права, чем администратор, но более широкие, чем обычные пользователи
USB-Token	Устройство-носитель ключевой информации, позволяющее упростить и обезопасить процедуру идентификации и аутентификации пользователя
API	Программный интерфейс приложения
HUMO, UzCARD	Межбанковские платежные системы
Интеграция	Любое взаимодействие между системами с помощью общих для них форматов данных или форматов вызовов
ПИНФЛ	Персональный идентификационный номер физического лица
Финансовые технологии	Отрасль, включающая в себя различные компании, использующие IT технологии для предложения финансовых продуктов и услуг

ОБЩИЕ СВЕДЕНИЯ

Настоящее Техническое задание на реализацию проекта «Разработка мобильного приложения для физических лиц разработано в соответствии с Государственным стандартом Республики Узбекистан О‘zDSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы».

1.1. Полное наименование МП и ее условное обозначение

Полное наименование проекта: Разработка мобильного приложения для физических лиц.

Условное обозначение проекта: Мобильное приложение.

Краткое наименование системы, принятое в настоящем ТЗ: МП, Приложение, 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 №ПП-306 от 14.09.2023г. «О мерах финансовой и институциональной поддержки развития малого бизнеса».
2. Решение Правления АКБ «Банк развития бизнеса» №-175 от 16.09.2024г.
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 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);

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. Указ Президента Республики Узбекистан №УП-5992 от 12.05.2020 года «О Стратегии реформирования банковской системы Республики Узбекистан на 2020 — 2025 годы»;
9. Постановление Президента Республики Узбекистан №ПП-4699 от 28.04.2020 года «О мерах по широкому внедрению цифровой экономики и электронного правительства»;
10. 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

Плановые сроки начала и окончания работы по созданию мобильного приложения

Начало работ – 02.10.2025 г.

Окончание работ – 02.06.2026 г.

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

С целью принятия результатов работ по проекту Заказчик имеет право создать в установленном порядке Приемочную комиссию. 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. О'z DST 1985:2018 Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем;
2. О'z DST 1986:2018 Информационная технология. Информационные системы. Стадии создания;
3. О'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»

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

2.1. Назначение МП

Мобильное приложение предназначено для предоставления физическим лицам как клиентам АКБ «Банк развития бизнеса», так 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 Мобильного Приложения 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 $\geq 40\%$ в первый год. Увеличение числа новых счетов, открытых через МП на $\geq 60\%$.

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 $\geq 50\%$ 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 $\geq 20\%$ в течение 18 месяцев. Снижение числа запросов в контакт-центр, связанных с проверкой баланса/статуса платежа, на $\geq 70\%$.

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 MyID

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.	Мобильное приложение для физических лиц	Предназначенное для оказания удаленных банковских услуг физическим лицам
5.	Процессинг центр Card suite	Процессинг центр карт VISA

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

Мобильное приложение 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 MyID), 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, EastTelecom, OFD и др.

4 ТРЕБОВАНИЯ К МОБИЛЬНОМУ ПРИЛОЖЕНИЮ

4.1 Требования к МП в целом

4.1.1 Требования к структуре и функционированию МП

Архитектура

Вся информационная система мобильного приложения 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 (изоляция 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 на языке программирования Java с использованием актуальных и производительных фреймворков. Выбор Java обусловлен его надежностью, высокой скоростью обработки данных и широкой экосистемой, что критично для финансовых систем.

DevOps и Инфраструктура:

Развертывание должно осуществляться с применением технологий контейнеризации (Docker) и оркестрации (Kubernetes). Это обеспечит автоматизированное управление жизненным циклом сервисов, эффективную балансировку нагрузки и, как следствие, высокую доступность системы в режиме 24/7.

Расширяемость:

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 5).

Для достижения максимальной производительности, безопасности и нативного пользовательского опыта предпочтение отдается нативным языкам разработки (Swift/Kotlin) или

высокопроизводительным кросс-платформенным 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 актуальными версиями TLS 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 и английском языках. Переводы должны быть согласованы с представителями АКБ «Банк развития бизнеса».

В рамках разработки мобильного приложения для физических лиц будет проведено тестирование совместимости системы с самыми распространенными на сегодняшний день мобильными браузерами, включая Chrome, Safari, Edge, Samsung internet, Firefox и т.д. Это тестирование будет охватывать как настольные, так и мобильные версии браузеров. Процесс тестирования будет направлен на проверку корректности отображения всех интерфейсных элементов, их функциональности, адаптивности страниц и общей производительности на каждом из поддерживаемых браузеров.

Мобильное приложение 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: компьютеры, ноутбуки, смартфоны и планшеты. Тестирование будет включать проверку интерфейса на операционных системах Windows, macOS, 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 кроссбраузерная 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.

Основная структура мобильного приложения для физических лиц должна включать в себя следующие модули:

1. Модуль «Регистрация пользователей»;
2. Модуль «Персональный кабинет и профиль пользователя»
3. Модуль «Управление картами»;
4. Модуль «СМС служба»;
5. Модуль «Платежи и история платежей»;
6. Модуль «Переводы P2P»
7. Модуль «Администрирование»
8. Модуль «Интеграции»

9. Модуль «Депозиты»
10. Модуль «Кредиты»
11. Модуль «Валютные операции»

4.1.1.1 Перечень подсистем, их назначение и основные характеристики

Структура Мобильного приложения для физических лиц представляет собой совокупность взаимосвязанных функциональных модулей, каждый из которых отвечает за определенный блок банковских и нефинансовых услуг.

1. Модуль «Регистрация пользователей».

Назначение: Обеспечение безопасной первичной регистрации, удаленной идентификации клиента и всех последующих процессов аутентификации для доступа к сервисам.

Основные характеристики: включает интеграцию с государственным сервисом «MyID» для удаленной идентификации и поддержку OTP-кодов для верификации.

2. Модуль «Персональный кабинет и профиль пользователя».

Назначение: Предоставление клиенту доступа к персонализированным данным, настройкам безопасности и сервисной информации Банка.

Основные характеристики: включает управление безопасностью (смена PIN-кода/пароля), просмотр персональных данных, а также отображение Филиалов и банкоматов на карте.

3. Модуль «Управление картами».

Назначение: Предоставление клиенту полного онлайн-контроля над его банковскими картами, включая их эмиссию (виртуальные карты) и управление безопасностью.

Основные характеристики: позволяет добавлять, удалять, блокировать карты, устанавливать PIN-коды и дистанционно получать карты по ПИНФЛ.

4. Модуль «СМС служба».

Назначение: Обеспечение надежного, резервированного и защищенного от мошенничества канала доставки служебных сообщений, OTP-кодов и Push-уведомлений.

Основные характеристики:

Предусматривает автоматическую смену провайдера (например, между «Playmobile» и «EastTelecom») для обеспечения максимальной отказоустойчивости доставки.

Включает интеграцию с системой Telecom Antifraud для защиты от:

SMS-бомбинга (OTP Flooding): Ограничение частоты запросов и доставки OTP-кодов на один номер.

SMS-спуфинга/смишинга (Smishing): Фильтрация сообщений по подозрительным ключевым словам, URL-ссылкам и паттернам для защиты клиента от мошенничества.

Контроль доставки: Мониторинг и анализ трафика для выявления аномалий и предотвращения финансовых потерь, связанных с несанкционированными рассылками.

5. Модуль «Платежи и история платежей».

Назначение: Обеспечение всех видов регулярных платежей за услуги, их автоматизация (авто платежи) и предоставление детализированной истории расходов.

Основные характеристики: Интегрирован с платежными агрегаторами («Paynet») и включает функции автоматического формирования диаграмм и графиков для анализа прихода-расхода, с возможностью просмотра баланса доходов и трат за период. Включает функции мониторинга по категориям (продукты, транспорт, услуги) с автоматической категоризацией операций и сравнением трат с предыдущими отчетными периодами. мониторинга по категориям и диаграммам для анализа прихода-расхода.

6. Модуль «Переводы P2P».

Назначение: Обеспечение быстрых и безопасных переводов денежных средств между физическими лицами (по номеру карты или телефона), а также между собственными счетами клиента.

Основные характеристики: поддерживает QR – Оплату и функции Обмена валют по курсу Банка.

7. Модуль «Администрирование» (доступен только для администратора системы).

Назначение: Обеспечение контроля, безопасности, мониторинга и управления всеми процессами и пользователями в бэкэнд-части. Доступен только авторизованным сотрудникам Банка.

Основные характеристики: содержит инструменты для управления ролями и разрешениями, P2P мониторинга и администрирования транзакций, а также функции колл-центра.

8. Модуль «Интеграции» (доступен только для администратора системы)

Назначение: Техническая подсистема, обеспечивающая надежную и безопасную связность МП с внешними платежными системами, государственными и банковскими сервисами.

Основные характеристики: включает все необходимые API-интерфейсы для взаимодействия с «Humo», «Uzcard», основной АБС Банка («IABS»), процессинговым центром Банка (ТИЕТО), государственными порталами («MyGov») и платежными агрегаторами.

Дополнительно включает API для взаимодействия с системами защиты мобильной связи (Telecom Antifraud, Session Antifraud) на стороне SMS-агрегатора, а также платежным агрегатором «Paynet» и системой Центрального Банка Республики Узбекистан Munis (Munis QR).

9. Модуль «Депозиты»

Назначение: Предоставление клиенту возможности дистанционного открытия, управления и закрытия срочных, досрочных и сберегательных вкладов, а также доступа к полной информации по существующим депозитным счетам. Работа с сумовыми и валютными

депозитами.

Основные характеристики: включает онлайн-калькулятор для расчета доходности, функции пополнения и частичного снятия средств, просмотр истории начисления процентов и возможность автопродлонгации/закрытия вклада.

10. Модуль «Кредиты»

Назначение: Обеспечение функциональности для подачи онлайн-заявки на кредит, мониторинга текущего состояния кредитного портфеля клиента и удобного погашения задолженности.

Основные характеристики: предоставляет график платежей, информацию о размере основного долга и начисленных процентах, возможность срочного и досрочного погашения, а также функцию автоматического списания ежемесячного платежа со счета клиента.

11. Модуль «Валютные операции»

Назначение: Предоставление клиенту сервисов для проведения операций по обмену валюты (конверсия, конвертация), управления валютными счетами, включая просмотр актуальных курсов.

Основные характеристики: включает онлайн-обмен валюты по курсу Банка между своими счетами (конверсия и конвертация), отображение актуальных курсов валют, возможность открытия новых валютных счетов.

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).

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. Государственный сервис удаленной идентификации «MyID».

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 («playmobile» и «EastTelecom»).

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.

Мобильное приложение для физических лиц должно функционировать в трех основных режимах: нормальный (штатный), аварийный (отказоустойчивый) и технический (обслуживание).

1. Нормальный (Штатный) Режим Функционирования

Система функционирует в штатном режиме, когда все внутренние и внешние компоненты (ИАБС, процессинг, интеграционные шлюзы) доступны и работают согласно установленным нормативам производительности и надежности.

Доступность: доступно пользователям в режиме 24 часа в сутки, 7 дней в неделю (24/7).

Производительность: Время отклика на критически важные операции (авторизация, P2P-перевод) не превышает 2 секунды.

Синхронность: Все финансовые операции, инициированные в МП, должны синхронно отражаться в ИАБС Банка, а статусы исполнения должны поступать в МП в режиме близком к реальному времени.

Многоканальность: поддерживается одновременный и независимый доступ пользователей с различных устройств (смартфоны, планшеты).

2. Аварийный (Отказоустойчивый) Режим Функционирования

Система переходит в аварийный режим в случае возникновения сбоев в работе отдельных внутренних или внешних компонентов (например, недоступность ИАБС, сбой у платежного провайдера, сбой в работе провайдера СМС).

Критическая отказоустойчивость: В случае недоступности одного из провайдеров (например, СМС-службы), система должна автоматически переключаться на резервный канал (согласно Модулю «СМС служба») без прерывания сессии пользователя.

Частичный функционал: при недоступности некритических внешних сервисов (например, КАТМ для скоринга или MyGov), должно продолжать обеспечивать доступ к основному функционалу (проверка баланса, P2P-переводы внутри Банка), при этом недоступные функции

должны быть корректно скрыты или помечены соответствующим информационным сообщением.

Целостность данных: Все незавершенные транзакции, инициированные до сбоя, должны быть либо отменены с возвратом средств и информированием клиента, либо поставлены в очередь для гарантированного исполнения после восстановления работоспособности (с уведомлением пользователя).

Автономная работа: МП должно иметь механизмы кэширования некритических данных (например, история операций, шаблоны), позволяющие отображать эту информацию даже при временной потере связи с сервером.

При активации аварийного режима пользователи должны быть немедленно уведомлены о проблеме через push-уведомления, а также через уведомление внутри приложения.

В уведомлениях пользователям должна быть представлена информация о текущем состоянии системы, ожидаемом времени восстановления и действиях, которые они могут предпринять в аварийном режиме.

Аварийный режим считается завершенным, и система возвращается в нормальный режим при выполнении следующих условий:

- восстановлено устойчивое соединение с основными серверами и обеспечен нормальный доступ к базе данных;
- подтверждена нормальная работа всех внешних интеграций, включая банковские системы, API сторонних сервисов и государственные реестры;
- проведена автоматическая синхронизация всех данных, накопленных в аварийном режиме, с сервером, и получено подтверждение их целостности;
- все пользователи уведомлены о завершении аварийного режима и восстановлении нормального режима работы приложения.

3. Технический (Обслуживание) Режим Функционирования

Система переходит в технический режим для проведения плановых работ, обновления или профилактики.

Плановое обслуживание: Должна быть предусмотрена возможность перевода бэкэнд-системы в режим планового обслуживания с минимальным влиянием на пользователей. Плановые работы должны проводиться в периоды минимальной нагрузки (ночное время).

Уведомление: Клиенты должны быть предварительно оповещены о запланированных технических работах через Push-уведомления и сообщения на экране входа.

Ограниченный доступ: В режиме технического обслуживания вход в может быть временно ограничен, либо может быть доступен только ограниченный функционал (например, просмотр баланса).

Обновление МП: Обновление клиентской части приложения осуществляется через официальные магазины приложений (App Store и Google Play) с обязательным сохранением пользовательских настроек и данных.

4.1.1.4 Перечень и описание сценариев использования

Роли пользователей



Администратор - управляет ролями всех пользователей системы



Модератор - имеет доступ, чтобы добавлять, редактировать и удалять базовый функционал системы



Пользователь - проходит авторизацию и имеет возможность добавлять, редактировать собственные данные

Описание ролей пользователей мобильного приложения 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.



Рис. Организация прав доступа

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	Изменение	Просмотр всех	Модерация

	пользователей	настроек	данных	контента
Администратор	Да	Да	Да	Да
Модератор	Нет	Нет	Частично	Да
Пользователь	Нет	Нет	Нет	Нет

Перечень сценариев использования мобильного приложения представлен в таблице 1.

Идентификационный Номер	Наименование сценария Использования	Действующие лица	Тип сценарий
A1	Управление конфигурациями и правами всех ролей в системе	Администратор	Основной
U1	Удаленная регистрация нового клиента (Онбординг)	Пользователь, ИС «MyID»	Основной
U2	P2P-перевод с карты на карту	Пользователь	Основной
U3	Оплата коммунальных услуг	Пользователь	Основной
U4	Блокировка утерянной карты	Пользователь	Основной
U5	Открытие виртуальной карты (Visa/Humo/Uzcard)	Пользователь	Основной
U6	Оформление кредита	Пользователь, ИС «КАТМ»	Основной
U7	Погашение кредита	Пользователь	Основной
U8	Оформление депозита	Пользователь	Основной

U9	Проведение конверсии (Обмен между своими счетами/картами в разных валютах)	Пользователь	Основной
U10	Проведение конвертации (Обмен между собственными счетами)	Пользователь	Основной
U11	Авторизация с использованием биометрии	Пользователь	Основной

Сценарий использования A1. Управление конфигурациями и правами всех ролей в системе.

Условия запуска: Администратор выполняет задачи по настройке, контролю и поддержке работоспособности системы через Модуль «Администрирование».

Основное действующее лицо: Администратор системы.

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

- проводит авторизацию и аутентификацию в Модуле «Администрирование»;
- проверяет конфигурацию информационной системы на основе запроса или регламента;
- проводит регистрацию модераторов в информационной системе на основе запроса;
- проверяет наличие подобных записей ранее;
- создает логин и пароль для входа модераторов в систему на основе правил информационной безопасности;
- определяет роль и разрешения модераторов в системе (например, права на P2P мониторинг или управление транзакциями).

Временной регламент выполнения сценария: Время выполнения данного сценария не регламентируется системой, зависит от действий администратора.

Входные данные: Персональные данные модератора, запрашиваемая роль (права), конфигурационные параметры.

Выходные данные: Установленные конфигурационные параметры системы, Доступ в систему (логин и пароль) для модераторов системы, настроенные роли и разрешения.

Сценарий использования U1. Удаленная регистрация нового клиента (Онбординг).

Условия запуска: Пользователь впервые устанавливает и не является зарегистрированным клиентом Банка. Требуется удаленная идентификация для открытия счета.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев: Пользователь выполняет пошаговую процедуру регистрации:

- Пользователь вводит номер мобильного телефона.
- Система проверяет наличие номера в клиентской базе и отправляет ОТП-код через СМС (Модуль «СМС служба»).
- Пользователь вводит ОТП-код.
- Система запрашивает персональные данные (ПИНФЛ, серию/номер паспорта).
- Пользователь подтверждает данные и инициирует сессию интеграции с сервисом «MyID».
- Система через Модуль «Интеграции» проводит биометрическую идентификацию пользователя.
- В случае успешной идентификации, система предлагает создать логин/пароль и открыть первый базовый счет в Банке.

Временной регламент выполнения сценария: Время выполнения полного цикла сценария (от ввода номера до открытия счета) должно составлять не более 5 минут.

Входные данные: Номер мобильного телефона, ПИНФЛ, паспортные данные, биометрические данные, ОТП-код.

Выходные данные: Успешно зарегистрированный профиль Пользователя, логин и пароль для входа, новый открытый счет в АБС Банка.

Сценарий использования U2. P2P-перевод с карты на карту.

Условия запуска: Пользователь авторизован в системе, имеет активную карту с достаточным балансом и знает реквизиты получателя.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь выбирает в Модуле «Переводы P2P» функцию «Перевод на карту».
- Пользователь выбирает карту списания, вводит номер карты получателя и сумму.
- Система проверяет достаточность средств, лимиты и рассчитывает комиссию.
- Пользователь подтверждает операцию (например, по биометрии или PIN-коду).
- Система отправляет транзакцию на исполнение через процессинговый центр и АБС.
- Транзакция успешно исполнена, система отправляет Push-уведомление клиенту.

Временной регламент выполнения сценария: Время исполнения транзакции не должно превышать 5 секунд.

Входные данные: Номер карты списания, номер карты получателя, сумма, подтверждение (биометрия/PIN).

Выходные данные: Успешный перевод, обновление баланса, запись в истории платежей.

Сценарий использования U3. Оплата коммунальных услуг.

Условия запуска: Пользователь авторизован и имеет задолженность по лицевому счету у мерчанта (поставщика услуг).

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь выбирает в Модуле «Платежи» категорию «Коммунальные услуги» и поставщика.
- Пользователь вводит абонентский номер (лицевой счет).
- Система через интеграцию с «Paynet» запрашивает информацию о задолженности.
- Пользователь выбирает карту списания и подтверждает сумму оплаты.
- Система отправляет запрос на оплату, одновременно регистрирует операцию через ОФД.
- Платеж успешно проведен, система формирует электронную квитанцию.

Временной регламент выполнения сценария: Время проведения оплаты с момента подтверждения — не более 10 секунд.

Входные данные: Абонентский номер, сумма, карта списания.

Выходные данные: Успешная оплата, электронная квитанция, запись в истории платежей с фискальной информацией.

Сценарий использования U4. Блокировка утерянной карты.

Условия запуска: Пользователь обнаружил утерю/кражу карты и авторизован в МП.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь переходит в Модуль «Управление картами» и выбирает нужную карту.
- Пользователь выбирает функцию «Блокировка карты».
- Система запрашивает подтверждение действия (например, с помощью OTP или PIN-кода) для предотвращения ошибочной блокировки.
- Пользователь подтверждает блокировку.
- Система отправляет команду на немедленную блокировку карты в процессинговый центр и ИАБС.
- Блокировка подтверждена, система отправляет СМС-уведомление.

Временной регламент выполнения сценария: Время между подтверждением блокировки и фактической блокировкой карты должно составлять не более 1 секунды (режим реального времени).

Входные данные: Выбор карты, подтверждение действия.

Выходные данные: Смена статуса карты на «Заблокирована» во всех системах Банка.

Сценарий использования U5. Открытие виртуальной карты (Visa/Humo/Uzcard).

Условия запуска: Клиент Банка авторизован и желает открыть новую виртуальную карту для интернет-платежей или P2P.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь переходит в Модуль «Управление картами» и выбирает «Открыть виртуальную карту».
- Пользователь выбирает тип карты (Visa или Humo) и подтверждает условия.
- Система проверяет лимиты на открытие карт и инициирует процесс эмиссии в процессинговом центре.
- После успешной эмиссии система автоматически привязывает карту к профилю пользователя.
- МП отображает реквизиты новой карты (номер, CVV) и устанавливает ее в активный статус.

Временной регламент выполнения сценария: Время с момента выбора типа карты до ее активации — не более 60 секунд.

Входные данные: Выбор типа карты, согласие с условиями.

Выходные данные: Активная виртуальная карта, отображение реквизитов, запись об эмиссии в ИАБС.

Сценарий использования U6. Оформление кредита.

Условия запуска: Пользователь авторизован в системе, прошел удаленную идентификацию, соответствует базовым кредитным требованиям Банка. Обязательным условием является оформление страховки через партнера Банка.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь выбирает в Модуле «Кредиты» функцию «Оформить новый кредит».
- Пользователь выбирает тип кредита, указывает желаемую сумму и срок. - Система через Модуль «Интеграции» (с ИАБС, Бюро кредитных историй) проводит скоринг и формирует индивидуальные условия (процентная ставка, график платежей).

- Система предлагает клиенту выбрать страховую программу от компании-партнера и рассчитывает стоимость страховки (через Модуль «Интеграции» с системой страховой компании).
- Пользователь ознакомливается с условиями кредита и страховки, проверяет сформированный график и подтверждает согласие на прохождение биометрической идентификации.
- Система генерирует кредитный и страховой договоры в электронном виде и предлагает пользователю подписать их (прохождение биометрической идентификации с помощью OneID).
- После прохождения биометрической идентификации, система автоматически удерживает сумму страховки и зачисляет оставшуюся сумму кредита на указанный счет или карту клиента (исполнение транзакции через Модуль «Интеграции» с ИАБС).
- Система отправляет Push-уведомление об успешном зачислении средств через Модуль «СМС служба».

Временной регламент выполнения сценария: Время от подтверждения договора до зачисления средств — не более 30 секунд.

Входные данные: Тип кредита, сумма, срок, выбор страховой программы, электронная подпись договора.

Выходные данные: Открытый кредитный счет, списанная премия по страховке, зачисленные средства на карту/счет, запись в истории кредитов.

Сценарий использования U7. Погашение кредита.

Условия запуска: Пользователь авторизован в системе, имеет активный кредит и достаточный баланс на карте/счете для погашения.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь переходит в Модуль «Кредиты», выбирает активный кредит.
- Пользователь выбирает функцию «Внести платеж» или «Досрочное погашение».
- Система отображает сумму текущего планового платежа или рассчитывает сумму для досрочного погашения.
- Пользователь выбирает карту/счет списания и подтверждает операцию.
- Система отправляет транзакцию на списание средств через Модуль «Интеграции» (процессинг) и обновление состояния кредитного счета в ИАБС.
- Платеж успешно проведен, система обновляет график платежей и отправляет Push-уведомление через Модуль «СМС служба».

Временной регламент выполнения сценария: Время проведения транзакции погашения — не более 5 секунд.

Входные данные: Выбор кредита, сумма погашения, карта/счет списания, подтверждение.

Выходные данные: Обновленный остаток основного долга, обновленный график платежей, запись в истории транзакций.

Сценарий использования U8. Оформление депозита.

Условия запуска: Пользователь авторизован в системе, имеет активный счет/карту для пополнения депозита.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь выбирает в Модуле «Депозиты» функцию «Открыть новый вклад».
- Пользователь выбирает тип вклада (срочный/сберегательный), срок и начальную сумму.
- Система отображает предварительный расчет доходности и условия вклада.
- Пользователь выбирает счет/карту списания, с которой будет списана начальная сумма.
- Пользователь подтверждает согласие с условиями и подписывает электронный депозитный договор (с помощью OTP, доставленного через Модуль «СМС служба»).
- Система отправляет команду в ИАБС (Модуль «Интеграции») для открытия нового депозитного счета и списания средств.
- Депозит успешно открыт и пополнен, система отправляет электронный документ и Push-уведомление через Модуль «СМС служба».

Временной регламент выполнения сценария: Время от подтверждения договора до открытия счета — не более 15 секунд.

Входные данные: Тип вклада, срок, сумма, счет списания, электронная подпись договора (биометрическая идентификация с помощью OneID).

Выходные данные: Открытый депозитный счет, запись в истории вкладов, электронный договор.

Сценарий использования U9. Проведение конверсии (Обмен между своими счетами/картами в разных валютах).

Условия запуска: Пользователь авторизован, имеет счета или карты в разных валютах, необходимую сумму для обмена.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь выбирает в Модуле «Валютные операции» функцию «Обмен валюты».
- Пользователь выбирает счет/карту списания и счет/карту зачисления.
- Пользователь вводит сумму, которую хочет обменять.
- Система автоматически отображает актуальный курс Банка и рассчитывает сумму зачисления в другой валюте.
- Пользователь подтверждает операцию.
- Система отправляет транзакцию на исполнение в ИАБС (Модуль «Интеграции») с учетом текущего обменного курса.
- Транзакция успешно исполнена, средства списаны и зачислены, система отправляет Push-уведомление через Модуль «СМС служба».

Временной регламент выполнения сценария: Время исполнения транзакции не должно превышать 3 секунд.

Входные данные: Счет списания, счет зачисления, сумма конверсии, подтверждение.

Выходные данные: Успешный обмен валюты, обновление балансов по счетам, запись в истории операций.

Сценарий использования U10. Проведение конвертации (Обмен между собственными счетами).

Условия запуска: Пользователь авторизован, имеет счета в разных валютах, необходима операция обмена.

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь переходит в Модуль «Валютные операции».
- Пользователь инициирует перевод/обмен между своими валютными счетами.
- Пользователь указывает сумму для конвертации.
- Система производит расчет по курсу Банка и показывает итоговую сумму зачисления.
- Пользователь подтверждает действие (по биометрии).
- Операция обрабатывается через ИАБС (Модуль «Интеграции»).
- Балансы счетов обновляются, клиенту поступает уведомление через Модуль «СМС служба».

Временной регламент выполнения сценария: Время проведения операции — не более 3 секунд.

Входные данные: Счета для обмена, сумма, подтверждение.

Выходные данные: Успешная конвертация, обновление балансов, запись в истории.

Сценарий использования U11. Авторизация с использованием биометрии.

Условия запуска: Пользователь уже зарегистрирован и ранее активировал биометрическую аутентификацию (Touch ID/Face ID).

Основное действующее лицо: Пользователь.

Порядок выполнения сценариев:

- Пользователь запускает Мобильное приложение.
- МП распознает наличие биометрических данных и инициирует запрос к ОС устройства.
- Пользователь проходит идентификацию (сканирование отпечатка пальца/лица).
- ОС устройства подтверждает подлинность.
- Система предоставляет немедленный доступ к личному кабинету.

Временной регламент выполнения сценария: Время входа в систему по биометрии — не более 1 секунды.

Входные данные: Биометрические данные пользователя.

Выходные данные: Успешный вход в МП, запуск пользовательской сессии.

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

Мобильное приложение 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 приложения 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.

4.1.2 Требования к взаимодействию со сторонними информационными системами

Взаимодействие мобильного приложения 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 О`zDSt 2590:2012 «Информационная технология, а также требованиям к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы» и О`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

Мобильное приложение предназначено для использования среди широкого круга пользователей, поэтому максимальное количество конечных пользователей, одновременно имеющих доступ лимитируется только техническими ограничениями серверной части Системы.

Мобильное приложение 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 (тutorials) 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 A1).

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

Мобильное приложение для физических лиц должно 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 1 млн зарегистрированных учетных записей.

Для обеспечения функциональности системы при максимальной нагрузке (100,000 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 мобильного приложения должно обеспечиваться надежностью функциональных модулей, программного обеспечения, комплексов технических и инженерных средств.

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

Ответственность за бесперебойную работу приложения несет Исполнитель проекта.

Мобильное приложение для физических лиц должно обеспечивать надежность функционирования в реальном масштабе и иметь программные или аппаратные средства адекватной реакции на ошибки (должны быть предусмотрены средства по резервному копированию) при неудачном завершении операции.

Система приложения должна функционировать круглосуточно, в непрерывном режиме, кроме времени проведения работ по резервному копированию данных, восстановлению данных, смене версий программного обеспечения, других профилактических работ по техническому обслуживанию, требующих остановку технических средств.

Приложение должно сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке операционной системы, восстановление программы должно происходить после перезапуска операционной системы и запуска исполняемого файла;
- при ошибках в работе аппаратных средств восстановление функции мобильного приложения возлагается на операционную систему;
- при ошибках, связанных с программным обеспечением, восстановление работоспособности возлагается на операционную систему;
- своевременная оповещения пользователей и обслуживающего персонала о случаях нештатной работы компонентов приложения;
- своевременная диагностика неисправностей и организация технического обслуживания;
- соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;
- проведения комплекса мероприятий отладки, поиска и исключения ошибок;
- ведения журналов системных сообщений и ошибок для последующего анализа и изменения конфигурации.

Для защиты аппаратуры от перепадов напряжения и коммутационных помех должны применяться сетевые фильтры.

Надежность программных средств должна обеспечиваться за счет следующих организационных мероприятий:

- предварительного обучения пользователей и обслуживающего персонала;
- своевременного выполнения процессов администрирования;
- соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;
- своевременное выполнение процедур резервного копирования данных.

Надежность программного обеспечения подсистем должна обеспечиваться за счет:

- надежности общесистемного ПО и ПО Разработчика;
- проведением комплекса мероприятий отладки, поиска и исключения ошибок.
- ведением журналов системных сообщений и ошибок по подсистемам для последующего анализа и изменения конфигурации.

Надежность создаваемой системы обеспечивается:

- высокой технологичностью разрабатываемых программных средств и организационного обеспечения, позволяющего сохранять циркулирующую в системе информацию при сбоях и других ситуациях, нарушающих или разрушающих устойчивость функционирования системы;
- выбором отказоустойчивого оборудования и его структурным резервированием;
- горячим резервированием наиболее важных узлов Системы, к которым относятся серверы базы данных, серверы приложений, компоненты сети хранения данных, оборудование, обеспечивающее связь подсистем, а также связь пользователей каждой подсистемы с серверами БД;
- выбором топологии телекоммуникационной и локальных вычислительных сетей, обеспечивающих вариантность маршрутизации потоков информации;
- дублированием носителей информации;
- высоким уровнем квалификации и организации работы обслуживающего персонала;
- организацией технического обслуживания, использованием современных методов и средств диагностики;
- отладкой и тестированием модулей всех подсистем;
- наличием исчерпывающих комплектов технической документации, обеспечивающих надежную эксплуатацию всех модулей подсистем;
- работой модулей подсистем, которые не должны вызывать разрушение, искажение и/или утрату сведений, хранящихся в прикладных автоматизированных информационных системах субъектов взаимодействия Системы.

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:

- О‘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»

4.1.6 Требования безопасности

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 фронтальный 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»;

О'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 РС, 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 РН 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 неизменяемого 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).

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 электронной подписи ЭЦП).

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 50°C °, ± 5 °C °;
- 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).

Мобильное приложение 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 (узбекский и русский языки).

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 должен быть полностью переведен на узбекский и русский языки с возможностью переключения между ними. Для каждого языка должны быть предусмотрены отдельные проверки на корректность отображения текста.

Чтобы интерфейс МП был интуитивно понятным для пользователей с разным уровнем технических навыков, разрабатываемая система будет подвергнута нескольким уровням юзабилити-тестирования.

На ранних этапах разработки пользовательского интерфейса будут проводиться юзабилити-тесты с участием пользователей различных групп (технически подкованные пользователи, пользователи с минимальными навыками работы с компьютером). Основные задачи — тестирование интуитивности навигации, понятности интерфейса и его реакций на действия пользователей.

Сценарии будут включать в себя ключевые операции, такие как регистрация пользователя, выполнение транзакций, работа с отчетами и прочие функции. Тестируемые должны выполнять задания, связанные с этими функциями, в режиме реального времени, а наблюдатели будут фиксировать возникающие проблемы и уровень удобства выполнения операций.

После каждого этапа тестирования будет проводиться опрос участников, чтобы выяснить их впечатления, возникшие трудности и предложения по улучшению интерфейса. На основе полученной обратной связи интерфейс будет дорабатываться для повышения его интуитивности.

Будут собираться и анализироваться ключевые показатели юзабилити, такие как время на выполнение задачи, количество ошибок при взаимодействии с интерфейсом, уровень удовлетворенности пользователей и когнитивная нагрузка.

Для обеспечения доступности системы пользователям с ограниченными возможностями будет реализована поддержка стандартов WCAG 2.1, уровней А и АА. Эти стандарты включают следующие ключевые аспекты:

тексты и элементы управления будут обеспечены достаточной контрастностью (не менее 4.5:1 для текста и фоновых элементов), что сделает систему доступной для пользователей с нарушениями зрения, такими как дальтонизм или слабое зрение;

все текстовые элементы, включая элементы интерфейса и динамические компоненты, будут доступны для экранных читалок, что обеспечит доступ для пользователей с нарушениями зрения. Будет обеспечено использование атрибутов ARIA (Accessible Rich Internet Applications) для взаимодействия экранных читалок с элементами пользовательского интерфейса;

функциональные элементы системы будут доступны для пользователей, которые предпочитают или вынуждены пользоваться клавиатурой вместо мыши. Будут реализованы горячие клавиши для доступа к основным функциям, а также возможность полного использования системы через клавиатурные команды;

для ключевых функций системы будут предусмотрены визуальные и звуковые подсказки, что повысит удобство использования системы для людей с разными формами инвалидности.

Система будет проверяться с помощью автоматизированных инструментов для оценки доступности (WAVE или Axe), что позволит выявить несоответствия стандартам доступности и исправить их на этапе разработки.

Будут проведены специальные тесты с участием людей с различными формами инвалидности (например, пользователи экранных читалок, пользователи, работающие только с клавиатурой). Эти тесты позволят убедиться в том, что система действительно удобна и доступна для всех категорий пользователей.

После ввода системы в эксплуатацию будут проводиться регулярные аудиты доступности, чтобы убедиться, что в ходе обновлений и модификаций системы сохраняется её соответствие стандартам доступности.

Для упрощения разработки и обеспечения соответствия стандартам юзабилити и доступности разработчики будут обеспечены подробными рекомендациями и лучшими практиками по созданию доступных интерфейсов. Это поможет ускорить процесс разработки, соответствующей WCAG и стандартам эргономики.

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 транспортабельности для подвижных ИС*

Требования к транспортабельности не предъявляются.

4.1.9 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).

4.1.10 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.

4.1.11 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.

4.1.12 Дополнительные требования*

Дополнительные требования не предъявляются.

4.2 Требования к функциям (задачам), выполняемым системой приложения

Система должна представлять собой комплекс взаимосвязанных модулей, каждый из которых имеет своё функциональное назначение. Информационное взаимодействие между участниками системы должно быть автоматизировано и должно минимизировать вмешательство оператора, за исключением случаев физического отсутствия связи и иных нештатных ситуаций.

В системе будет внедрён централизованный процесс управления обновлениями и исправлениями (патчами) модулей, включающий регулярный мониторинг, планирование обновлений, а также тестирование и внедрение исправлений. Каждое обновление будет предварительно проверяться в тестовой среде, чтобы убедиться в его совместимости с остальными компонентами системы и минимизации возможных рисков сбоев.

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. Модуль «Регистрация пользователей»

Модуль обеспечивает первый контакт клиента с АКБ «Банк развития бизнеса», включает удаленную идентификацию, а также управляет основными процессами аутентификации, безопасностью входа и привязкой устройства.

Подмодуль «Регистрация и Идентификация»

Отвечает за сбор первичных данных, проведение обязательной удаленной биометрической идентификации через «MyID» и дистанционное открытие первого счета в Банке.

Подмодуль «Аутентификация и Сессии»

Отвечает за вход в систему, поддержку многофакторной аутентификации, управление активными сессиями и безопасное восстановление доступа.

Основные функциональные возможности модуля должны включать в себя:

Касательно регистрации и открытия счета:

Предоставление пошагового, многоязычного интерфейса для сбора персональных данных (ПИНФЛ, паспортные данные).

Программная интеграция с сервисом «MyID для юридически значимой удаленной биометрической идентификации.

Обеспечение возможности онлайн-открытия первого базового счета в АБС Банка, с автоматическим подписанием клиентской документации через МП.

Касательно входа и безопасности:

Поддержка авторизации по логину/паролю и с применением биометрической аутентификации (Touch ID / Face ID) с обязательным хранением биометрии на устройстве.

Реализация механизма привязки учетной записи к устройству (Device Binding) для повышения безопасности.

Обеспечение безопасного, многофакторного механизма восстановления доступа, включающего верификацию через ОТП-код и/или повторную идентификацию.

Функция отображения списка активных сессий и удаленного выхода из них для контроля пользователем своей безопасности.

4.2.2. Модуль «Персональный кабинет и профиль пользователя»

Модуль предоставляет клиенту доступ к персонализированным данным, настройкам безопасности, сервисной информации и расширенной обратной связи.

Подмодуль «Профиль и Настройки»

Отвечает за просмотр личных данных, управление настройками безопасности, уведомлениями и предпочтениями.

Подмодуль «Сервисная информация и Документы»

Предоставляет данные о расположении объектов Банка, курсах валют и доступ к юридически значимым документам.

Основные функциональные возможности модуля должны включать в себя:

Просмотр и инициирование изменения контактных данных (e-mail, адрес) с обязательной верификацией через ОТП.

Управление настройками безопасности: включение/выключение биометрической аутентификации, настройка гранулярности Push-уведомлений (например, только для списаний свыше 1 млн сум).

Предоставление хранилища электронных документов (договоры по кредитам, депозитам, выписки по счетам) с возможностью их просмотра и скачивания в PDF.

Отображение на интерактивной карте актуальной информации о расположении всех объектов Банка, включая фильтрацию по услугам (например, «Банкомат с приемом наличных USD»).

Предоставление прямых каналов связи со службой поддержки Банка: встроенный текстовый чат с поддержкой мультимедиа (скриншоты, голосовые сообщения) и раздел FAQ.

4.2.3. Модуль «Управление картами»

Модуль предоставляет клиенту АКБ «Банк развития бизнеса» полный удаленный онлайн-контроль над всеми его платежными инструментами, включая их эмиссию, настройки безопасности и управление лимитами.

Подмодуль «Оперативный контроль карт»

Отвечает за отображение актуальной информации о картах, блокировку/разблокировку и просмотр транзакций.

Подмодуль «Эмиссия и Настройки безопасности»

Отвечает за онлайн-открытие виртуальных карт, а также за управление PIN-кодами и индивидуальными лимитами для различных типов операций.

Основные функциональные возможности модуля должны включать в себя:

Отображение всех активных карт клиента с указанием актуального баланса, срока действия и возможностью отображения полного номера (с использованием ОТП-подтверждения).

Функция мгновенной блокировки и разблокировки любой карты с немедленным обновлением статуса в процессинговом центре.

Обеспечение онлайн-эмиссии виртуальных карт (Visa, Humo, Uzcard) с автоматическим отображением реквизитов в защищенном режиме.

Реализация функции онлайн-заказа физической карты с выбором дизайна и адреса доставки.

Предоставление пользователю возможности самостоятельно настраивать лимиты на различные типы операций: интернет-платежи, операции в банкоматах, операции за пределами страны.

Формирование выписки по карте за выбранный период в форматах PDF/Excel.

4.2.4. Модуль «СМС служба»

Модуль обеспечивает надежный, резервированный и безопасный канал доставки всех уведомлений и одноразовых паролей, используя как СМС, так и Push-технологии.

Подмодуль «Доставка Уведомлений»

Отвечает за генерацию, отправку и управление критическими СМС-сообщениями (ОТР, подтверждения транзакций) и Push-уведомлениями.

Подмодуль «Резервирование и Отчетность»

Отвечает за переключение между провайдерами СМС, управление приоритетами доставки и детальное логирование.

Основные функциональные возможности модуля должны включать в себя:

Управление генерацией и доставкой ОТР-кодов с контролем частоты запросов, сроком действия и лимитами на отправку (антифрод).

Реализация механизма автоматического переключения (Failover) между несколькими провайдерами СМС-услуг («playmobile», «EastTelecom») с учетом задержки доставки.

Управление приоритетами доставки: критические (ОТР, списания) отправляются по СМС, некритические (маркетинг) – через Push-уведомления.

Отправка Push-уведомлений (FCM/APNS) как основного канала информирования, с обязательным механизмом проверки статуса доставки.

Предоставление интерфейса для отчетности по расходам на СМС, включая статистику по доставленным, недоставленным и просроченным сообщениям.

Поддержка отправки сервисных сообщений и системных предупреждений о временной недоступности функций.

4.2.5. Модуль «Переводы Р2Р»

Модуль обеспечивает все виды высокоскоростных денежных переводов между счетами и картами, а также выполняет функции конвертации валюты и управления регулярными

платежами.

Подмодуль «Транзакционные переводы»

Отвечает за P2P-переводы внутри Банка и на карты сторонних банковских систем (Humo, Uzcard, международные).

Подмодуль «Конвертация и Планирование»

Отвечает за обмен валют, поддержку инновационных методов оплаты и создание регулярных переводов.

Основные функциональные возможности модуля должны включать в себя:

Обеспечение мгновенных переводов между любыми собственными счетами и картами клиента.

Реализация P2P-переводов по номеру карты Humo/Uzcard и по номеру телефона (при наличии интеграции с межбанковской системой переводов) с обязательным отображением имени получателя до подтверждения.

Функция мгновенной конвертации средств между валютными счетами клиента с отображением курса Банка в момент совершения операции.

Поддержка создания регулярных (по расписанию) P2P-переводов с автоматическим напоминанием о дате списания.

Предоставление возможности сохранения шаблонов переводов и добавления получателей в Избранное.

Поддержка инициирования платежей и переводов с использованием QR-кодов.

4.2.6. Модуль «Платежи и история платежей»

Модуль обеспечивает оплату услуг, управление регулярными платежами, а также предоставляет клиенту инструменты для финансовой аналитики и отчетности.

Подмодуль «Оплата услуг и Фискализация»

Отвечает за доступ к агрегированным платежам, проверку задолженностей и обязательную регистрацию транзакций через ОФД.

Подмодуль «История, Аналитика и Шаблоны»

Отвечает за хранение, отображение, фильтрацию и анализ истории всех финансовых операций.

Основные функциональные возможности модуля должны включать в себя:

Обеспечение доступа ко всем агрегированным платежам (коммунальные услуги, интернет, штрафы, налоги) через интеграцию с «Paynet», «MyGov» и «Munis».

Функция проверки задолженности по лицевому счету или абонентскому номеру до совершения платежа.

Обязательная фискализация всех подлежащих регистрации платежей через интеграцию с

ОФД с генерацией электронного фискального чека.

Возможность создания, управления и временного приостановления регулярных автоплатежей по заданным шаблонам.

Предоставление детализированной истории всех операций с возможностью сложной фильтрации и выгрузки данных в форматах Excel/PDF.

Автоматическое формирование диаграмм и графиков расходов/доходов, с интеллектуальной категоризацией операций и сравнением трат с предыдущими периодами.

4.2.7. Модуль «Администрирование»

Модуль предназначен исключительно для сотрудников Банка, обеспечивая высокий уровень контроля рисков, AML-мониторинга, аудита и управления бизнес-логикой системы.

Подмодуль «Управление ролями и персоналом»

Отвечает за создание, назначение и управление правами доступа для сотрудников Банка, с обязательной фиксацией истории изменений прав.

Подмодуль «Мониторинг, Риски и AML»

Отвечает за отслеживание финансовых операций, управление лимитами, Velocity Checks и аудит системных событий.

Подмодуль «Конфигурация Бизнес-логики»

Отвечает за удаленную настройку тарифов, текстов уведомлений и параметров системы без участия разработчиков.

Основные функциональные возможности модуля должны включать в себя:

Касательно управления сотрудниками:

Предоставление интерфейса для создания, редактирования и назначения различных ролей с детализацией прав доступа до уровня API-вызова.

Аутентификация сотрудников Банка с использованием многофакторного метода (MFA), отличного от используемого клиентами.

Касательно мониторинга и AML:

Предоставление Модераторам интерфейса для поиска, фильтрации и маркировки подозрительных операций в соответствии с политикой AML Банка.

Реализация антифрод-системы, включающей Geolocation checks (проверка страны транзакции и IP-адреса) и Velocity checks (контроль частоты и суммы транзакций).

Возможность установки, изменения и временной блокировки суточных, недельных и месячных лимитов для отдельных клиентов.

Касательно аудита и конфигурации:

Предоставление инструмента для удаленной настройки тарифов на P2P-переводы и конвертацию, которые немедленно применяются в МП.

Формирование регуляторной отчетности по финансовым операциям в форматах, требуемых Центральным Банком.

Обеспечение детального журнала системных логов и аудита, с возможностью поиска по идентификатору транзакции для сквозного контроля.

4.2.8. Модуль «Интеграции»

Модуль функционирует как единый API-шлюз, обеспечивающий безопасное, отказоустойчивое и стандартизированное взаимодействие со всеми внешними (платежные системы, госсервисы) и внутренними (АБС) системами.

Подмодуль «API-Шлюз и Маршрутизация»

Обеспечивает единую точку входа, балансировку нагрузки и управление потоками запросов к конечным системам.

Подмодуль «Безопасность и Преобразование Протоколов»

Отвечает за аутентификацию, авторизацию, токенизацию, шифрование и конвертацию данных между стандартами.

Основные функциональные возможности модуля должны включать в себя:

Функционирование в качестве единого API-шлюза с поддержкой динамической маршрутизации запросов к АБС, процессингу, MyID, КАТМ и процессингу ПИЕТО.

Реализация механизмов Circuit Breaker и Time-out Control для предотвращения каскадных сбоев при недоступности внешних систем.

Управление всеми ключами, сертификатами и токенами, необходимыми для аутентификации внешних ИС, с ротацией ключей в соответствии с регламентом ИБ.

Обеспечение токенизации конфиденциальных данных (полных номеров карт) и сквозного шифрования для соответствия стандартам безопасности.

Автоматическое преобразование протоколов и данных между форматом JSON/RESTful и требованиями внешних систем с обязательной валидацией входных и выходных данных.

Журналирование (логирование) всех запросов и ответов с фиксацией времени и статуса для целей аудита и сверки.

4.2.9. Модуль «Депозиты»

Модуль предоставляет пользователю полный набор инструментов для открытия в режиме онлайн, управления и мониторинга всех его срочных и сберегательных вкладов.

Подмодуль «Мониторинг вкладов» Отвечает за отображение полной информации по текущим и закрытым депозитным счетам, включая сумму, срок, процентную ставку и историю начисления процентов.

Подмодуль «Открытие и управление» Отвечает за процесс дистанционного оформления новых депозитов и выполнение операций по существующим вкладам (пополнение, частичное

снятие, автопролонгация).

Основные функциональные возможности модуля должны включать в себя:

Просмотр списка всех активных и закрытых депозитов с детализацией по каждому вкладу.

Онлайн-калькулятор, позволяющий рассчитать потенциальную доходность нового вклада на основе суммы и срока.

Функция открытия нового депозита с выбором условий и подписанием электронного договора (с верификацией через ОТП).

Проведение операций пополнения депозитного счета с привязанной карты или текущего счета.

Возможность частичного снятия средств (если предусмотрено условиями вклада) или досрочного закрытия депозита.

Настройка и управление автопролонгацией вклада по истечении срока.

4.2.10. Модуль «Кредиты»

Модуль обеспечивает пользователю возможность дистанционной подачи заявки на кредит, а также полный контроль и удобное управление текущим кредитным портфелем, включая погашение задолженности.

Подмодуль «Кредитный портфель» Отвечает за предоставление актуальной информации по всем действующим кредитам, включая график платежей и детализацию задолженности.

Подмодуль «Оформление и погашение» Отвечает за процесс подачи онлайн-заявки на кредитные продукты, выбор страховых программ и проведение операций по погашению задолженности.

Основные функциональные возможности модуля должны включать в себя:

Отображение списка активных и закрытых кредитов с указанием суммы основного долга, процентной ставки и даты следующего платежа.

Просмотр детализированного графика платежей с возможностью отметить уже оплаченные и предстоящие платежи.

Формирование и подача онлайн-заявки на выбранный кредитный продукт с автоматическим скорингом.

Выбор и оформление страхового договора через партнера в рамках кредитного процесса (с интеграцией, как указано в U5).

Проведение ежемесячного планового погашения или досрочного погашения кредита с выбором карты/счета списания.

Получение справки о текущей задолженности или справки о полном погашении кредита в электронном виде.

4.2.11. Модуль «Валютные операции»

Модуль предоставляет пользователю инструменты для управления своими валютными счетами и осуществления внутренних операций по обмену валюты (конверсии/конвертации) по курсу Банка.

Подмодуль «Курсы и счета» Отвечает за отображение текущих курсов валют, а также за просмотр балансов и истории операций по всем валютным счетам клиента.

Подмодуль «Конвертация». Отвечает за выполнение операций по обмену денежных средств в национальной валюте на иностранную валюту между своими счетами.

Подмодуль «Конверсия». Отвечает за выполнение операций по обмену денежных средств в иностранной валюте на другую иностранную валюту.

Основные функциональные возможности модуля должны включать в себя:

Отображение актуального официального курса Банка для покупки и продажи валюты.

Просмотр списка всех валютных счетов и карт с их текущими балансами.

Функция онлайн-обмена валюты (конверсии/конвертации) между любыми собственными счетами клиента (например, с UZS на USD или с EUR на UZS).

Калькулятор обмена, который в реальном времени рассчитывает сумму зачисления на основе введенной суммы списания и текущего курса.

Возможность открыть новый валютный счет (например, USD или EUR) в дистанционном режиме.

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

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.

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 объемах, достаточных для восстановления информации в подсистеме хранения данных.

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 – кириллица и латиница), русский (шрифт – кириллица). Информация в базе должна храниться на том языке, на котором она была введена.

4.3.4 Требования к программному обеспечению

Мобильное приложение для физических лиц должно быть разработано с использованием современных технологий, обеспечивающих высокую производительность, безопасность и

удобство работы на всех поддерживаемых платформах. Программное обеспечение должно включать серверную и клиентскую части, интеграцию с внешними системами, базами данных и API, а также поддержку защиты данных и обеспечения высокой доступности приложения.

Клиентская часть

Приложение должно быть совместимо с платформами iOS и Android.

Поддерживаемые версии ОС: iOS 15 и выше для устройств Apple и Android 5 и выше для устройств на базе Android.

Приложение должно корректно работать на всех поддерживаемых версиях ОС с учетом возможных обновлений операционных систем.

Языки программирования и технологии

iOS: Swift 5 или выше для разработки под iOS, с использованием фреймворка UIKit или SwiftUI.

Android: Kotlin для разработки под Android, с использованием Android Jetpack и Material Design.

Приложение должно быть разработано с использованием принципов Clean Architecture, что позволяет легко вносить изменения и обновления, а также соблюдать принципы модульности.

Серверная часть

Требования к серверному программному обеспечению

Серверное ПО должно поддерживать модульную архитектуру (микросервисную), что позволяет гибко масштабировать отдельные компоненты при увеличении нагрузки.

Серверные API должны быть RESTful или GraphQL для взаимодействия с клиентской частью и обеспечивать быструю обработку запросов.

Поддержка отказоустойчивости и балансировки нагрузки между серверами для обеспечения бесперебойной работы при высоких нагрузках.

Языки программирования и технологии

Основные языки для серверной части: Node.js или Python для обработки запросов и бизнес-логики.

Базы данных: реляционная база данных (PostgreSQL или MySQL) для хранения структурированных данных и документоориентированная база данных (MongoDB) для хранения неструктурированных данных.

СУБД и кэширование: для кэширования рекомендуется Redis или Memcached для ускорения отклика на запросы.

4.3.5 Требования к техническому обеспечению

Используемые технические средства должны иметь достаточные количественные и качественные показатели для полноценной работы системы мобильного приложения.

К техническим средствам системы мобильного приложения относятся:

- сервер БД;
- Сервер приложений Системы;

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

- 12 ядер, работающий на частоте не ниже 4.5 ГГц;
- ОЗУ объемом не менее 128 ГБ;
- Жесткий диск 2000 Гб;
- Сетевой интерфейс для работы между серверами.

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

- 12 ядер, работающий на частоте не ниже 4.5 ГГц;
- ОЗУ объемом не менее 128 ГБ;
- Жесткий диск 2000 Гб;
- Сетевой интерфейс для работы между серверами.

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

Мобильное приложение для физических лиц должно 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 правовых документы;
- инструкции пользователей ПО;
- должностные инструкции персонала, выполняющего работы с использованием Системы и ее компонентов.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Перечень стадий и этапов работ по созданию мобильного приложения должен соответствовать требованиям О'z DST 1986:2018. Состав и содержание работ, перечень документов, предъявляемых по окончании соответствующих стадий и этапов работ, приведены в таблице

Перечень стадий и этапов создания Мобильного приложения для физических лиц

Таблица 1.

№ Этап а	Наименование работ и их содержание	Сроки выполнения		Исполнитель	Результат
		Начало	Окончание		
1	Изучение объекта информатизации				Сбор данных необходимых для реализации проекта
2	Разработка концепции				Документ, описывающий общие положения проекта
3	Разработка технического задания				Техническое задание на создание ИС
4	Согласование ТЗ				Документы

	и получение других необходимых документов				(Паспорт, Концепция, ТЗ), дающие право на разработку ПО ИС
5	Рабочий проект				Разработка ИС и его составных частей Разработка документации по программному обеспечению и эксплуатации Строительно-монтажные работы Первоначальное тестирование ИС
6	Тестирование и доработка системы				Проверка работоспособности ИС и устранение возникших проблем. Акт о проведении теста
7	Профессиональная эксплуатация системы				Акт ввода Информационной системы в эксплуатацию

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 Мобильного приложения 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 мобильного приложения 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.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Перечень документов технического и рабочего проектирования должен соответствовать номенклатуре, приведенной в О⁴zDSt 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:

Департамента ИТ

АКБ «Банк развития бизнеса»

_____ 3. Орифходжаев
(подпись)

Проектный менеджер

(подпись)

Бизнес аналитик

(подпись)

согласные: А.Икрамов

<https://hujjat.brb.uz/?pin=kF55eM88&id=607b2778-5bb3-4fee-94cb-dc8fc17e726f>