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

«25» май 2026 г.
№ 390

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на информационную систему

«Платформа больших языковых моделей (LLM)»

на ___ листах

действует с «____» _____2026 г.

Ташкент – 2026 г.

Сокращения и определения

API	Программный интерфейс приложения – описание способов взаимодействия компьютерных программ
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
ИС	Информационная система — комплекс обработки информации, включающий вычислительное и коммуникационное оборудование, базы данных, системы управления базами данных и информационные ресурсы.
СУБД	Система управления базами данных
Пользователь	Пользователь информационной системы – это лицо (группа лиц, организация), пользующееся услугами информационной системы
Администратор	Пользователь или роль с расширенными правами доступа, осуществляющий управление информационной системой, ее настройками и пользователями
JSON	JavaScript Object Notation - текстовый формат обмена данными
Интеграция	Процесс взаимодействия информационных систем для обмена данными и обеспечения согласованного функционирования с использованием стандартных протоколов и форматов данных
DMZ	Demilitarized Zone (демилитаризованная зона), изолированный сетевой сегмент между внешней и внутренней сетью для размещения публичных сервисов и повышения уровня безопасности
KMS	Key Management Service (Система управления ключами)
HSM	Hardware Security Module (Аппаратный модуль безопасности)
MFA	Multi-factor authentication (Многофакторная аутентификация)
DLP	Data Loss/Leak Prevention (Защита от утечек)
SLA	Service Level Agreement (Соглашение об уровне обслуживания) — формальный контракт между поставщиком услуг и клиентом, который определяет измеримые показатели качества и доступности услуги, обязанности сторон
JIT	Just-In-Time (Точно в срок) — это управленческая концепция бережливого производства, при которой услуги предоставляется только тогда, когда они нужны, и на минимально требуемый срок
TLS	Transport Layer Security (Протокол защиты транспортного уровня) —криптографический протокол, обеспечивающий конфиденциальность, целостность данных и аутентификацию при

	передаче информации между узлами в сети
Rate limiting	Ограничение частоты запросов — это механизм защиты веб-сервисов, ограничивающий количество запросов от пользователя к API или сайту за определенное время
SIEM	Security Information and Event Management (система управления информацией и событиями безопасности), предназначенная для сбора и анализа событий ИБ в реальном времени для выявления угроз и инцидентов
WORM-хранилище	Write Once, Read Many (Записать один раз, читать много раз) — технология, обеспечивающая неизменяемость данных после их записи
RBAC log access	Role-Based Access Control (Ролевой контроль доступа к журналам) — система управления доступом к журналам событий (логам) на основе ролей пользователей, обеспечивающая безопасность за счет предоставления прав только на необходимые данные
Security gate	Шлюз безопасности — комплекс программных или аппаратных решений, обеспечивающих защиту инфраструктуры путем фильтрации трафика, контроля доступа и анализа угроз
REST	Архитектурный стиль взаимодействия веб-сервисов, использующий HTTP методы для обмена данными
SOAP	Протокол обмена структурированными сообщениями в веб-сервисах на основе XML
XML	Расширяемый язык разметки для хранения и передачи структурированных данных
OAuth 2.0	Протокол авторизации, обеспечивающий безопасный доступ к ресурсам без передачи учетных данных пользователя
IP allowlist	Список разрешённых IP-адресов, которым предоставляется доступ к системе или API
IRP	Incident Response Plan (План реагирования на инциденты информационной безопасности) — набор процедур и правил, определяющих действия персонала при обнаружении инцидентов информационной безопасности
IDS/IPS	Intrusion Detection System / Intrusion Prevention System (Система обнаружения и предотвращения вторжений) — комплекс программно-аппаратных средств, предназначенных для мониторинга сетевого трафика и событий системы с целью выявления и предотвращения несанкционированных действий и атак
WAF	Web Application Firewall (Межсетевой экран для веб-приложений) — средство защиты веб-приложений, предназначенное для фильтрации, мониторинга и блокировки вредоносных HTTP/HTTPS-запросов, направленных на эксплуатацию уязвимостей веб-сервисов
STT	Speech-to-Text (Преобразование речи в текст) — технология

	распознавания речи, обеспечивающая автоматическое преобразование голосового ввода пользователя в текстовую форму для дальнейшей обработки системой
TTS	Text-to-Speech (Преобразование текста в речь) — технология синтеза речи, обеспечивающая преобразование текстовой информации в голосовое воспроизведение для взаимодействия системы с пользователем
IABS	Integrated Automated Banking System (Интегрированная автоматизированная банковская система) — комплексная информационная система банка, предназначенная для автоматизации основных банковских процессов

1. ОБЩИЕ СВЕДЕНИЯ

Настоящее Техническое задание на реализацию проекта «Платформа больших языковых моделей (LLM)» разработано в соответствии с Государственным стандартом Республики Узбекистан O‘zDSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы».

1.1. Полное наименование ИС и ее условное обозначение

Полное наименование проекта: Информационная система «Платформа больших языковых моделей (LLM)».

Условное обозначение проекта: ИС «Платформа больших языковых моделей (LLM)».

Краткое наименование системы, принятое в настоящем ТЗ: ИС, Система, Проект.

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: Департамент информационных технологий.

1.3. Перечень документов, на основании которых создается ИС

Основанием для реализации Проекта являются следующие документы:

– Постановление Президента Республики Узбекистан № ПП-358 от 14.10.2024 г. «Об утверждении Стратегии развития технологий искусственного интеллекта до 2030 года»;

– Постановление Президента Республики Узбекистан № ПП-3270 от 12.09.2017 г. «О мерах по дальнейшему развитию и повышению устойчивости банковской системы Республики Узбекистан»;

– Постановление Президента Республики Узбекистан № ПП-3620 от 23.03.2018 г. «О дополнительных мерах по повышению доступности банковских услуг»;

– Указ Президента Республики Узбекистан № УП-189 от 22.10.2025 г. «О дополнительных мерах по дальнейшему развитию технологий искусственного интеллекта»;

– Стратегия развития АКБ «Банк развития бизнеса», утвержденная Наблюдательным советом банка (протокол № 15 от 19.06.2024 г.).

Техническая документация на реализацию Проекта разрабатывается в соответствии с Постановлением Президента Республики Узбекистан № ПП-4328 от 21.05.2019 г. «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 ИС

Плановые сроки выполнения работ по созданию ИС:

Начало работ — 01.04.2026 г.

Окончание работ — 15.12.2026 г.

Реализация проекта осуществляется в несколько стадий:

1 стадия — анализ требований проекта;

2 стадия — подготовка и обработка данных для обучения модели;

3 стадия — создание и обучение большой языковой модели (LLM);

4 стадия — интеграция с внутренними информационными системами и тестирование;

5 стадия — ввод в эксплуатацию и мониторинг функционирования.

Оформление результатов работ по созданию ИС должно осуществляться в соответствии с требованиями следующих нормативных документов:

1. O‘zDSt 1985:2018 «Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем»;
2. O‘zDSt 1986:2018 «Информационная технология. Информационные системы. Стадии создания»;
3. O‘zDSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы».

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

2.1. Назначение ИС

Информационная система «Платформа больших языковых моделей (LLM)» предназначена для создания, обучения, развертывания и эксплуатации больших языковых моделей в целях автоматизации процессов обработки и генерации текстовой информации, интеллектуального анализа данных и предоставления AI-сервисов для внутренних информационных систем Банка.

ИС ориентирована на решение следующих задач:

- обеспечение централизованной платформы для разработки, обучения, тестирования и эксплуатации больших языковых моделей;

- автоматизация обработки текстовых запросов и генерации ответов с использованием технологий искусственного интеллекта;
- обеспечение возможности интеграции AI-моделей с внутренними информационными системами Банка;
- предоставление сервисов интеллектуального анализа, поиска и обработки информации;
- поддержка многоязычного взаимодействия, включая узбекский, русский и английский языки;
- обеспечение централизованного хранения и обработки данных, используемых для обучения и функционирования моделей;
- обеспечение мониторинга, администрирования и управления жизненным циклом моделей искусственного интеллекта;
- обеспечение возможности масштабирования вычислительных ресурсов и AI-сервисов в зависимости от нагрузки и потребностей Банка;
- интеграция с внутренними и внешними источниками данных для обеспечения актуальности и полноты информации, используемой в работе моделей.

2.2. Цели создания системы

Целью создания ИС является формирование централизованной платформы больших языковых моделей (LLM) для внедрения и развития технологий искусственного интеллекта в деятельности Банка, автоматизации процессов обработки информации и повышения эффективности цифровых сервисов.

Создание ИС направлено на достижение следующих целей:

- создание единой платформы для разработки, обучения, тестирования и эксплуатации больших языковых моделей;
- автоматизация процессов обработки, анализа и генерации текстовой информации;
- повышение эффективности работы внутренних информационных систем и цифровых сервисов Банка за счёт внедрения AI-технологий;
- снижение нагрузки на сотрудников Банка путем автоматизации типовых операций обработки информации и пользовательских запросов;
- обеспечение возможности интеллектуального поиска, анализа данных и формирования ответов в автоматическом режиме;
- развитие инновационной AI-инфраструктуры Банка и повышение уровня технологической зрелости;

- обеспечение возможности масштабирования AI-сервисов и интеграции новых интеллектуальных модулей;
- создание технологической основы для дальнейшего внедрения систем искусственного интеллекта, видеоаналитики, интеллектуальных ассистентов и цифровых сервисов;
- обеспечение централизованного управления жизненным циклом моделей искусственного интеллекта и связанных с ними данных.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Объектом автоматизации является процесс разработки, обучения, эксплуатации и использования больших языковых моделей (LLM) в информационной инфраструктуре АКБ «Банк развития бизнеса».

В настоящее время использование технологий искусственного интеллекта в Банке характеризуется отсутствием единой централизованной платформы для работы с большими языковыми моделями, разрозненностью AI-инструментов и необходимостью ручной интеграции интеллектуальных сервисов с внутренними информационными системами. Обработка текстовой информации, анализ данных и выполнение интеллектуальных операций в значительной степени зависят от отдельных программных решений и требуют существенного участия специалистов.

Объект автоматизации охватывает процессы подготовки и обработки данных, обучения и эксплуатации моделей искусственного интеллекта, выполнения интеллектуального анализа информации, генерации текстового контента, а также предоставления AI-сервисов внутренним информационным системам Банка.

Автоматизация направлена на создание единой централизованной платформы больших языковых моделей, обеспечивающей использование технологий искусственного интеллекта для обработки естественного языка (NLP), интеллектуального поиска, генерации ответов и автоматизации работы с текстовой информацией.

В рамках объекта автоматизации выделяются следующие ключевые процессы:

– процесс подготовки и обработки данных, включающий сбор, очистку, структурирование и формирование наборов данных для обучения моделей;

– процесс обучения и тестирования больших языковых моделей, включающий настройку параметров моделей, проведение обучения, валидации и оценки качества работы моделей;

– процесс эксплуатации AI-моделей, предусматривающий выполнение запросов пользователей и информационных систем с использованием технологий обработки естественного языка;

– процесс интеграции с внутренними информационными системами Банка для обеспечения интеллектуальной обработки данных и автоматизации бизнес-процессов;

– процесс централизованного управления жизненным циклом моделей, включая мониторинг производительности, обновление моделей, контроль качества и управление вычислительными ресурсами;

– процесс обеспечения информационной безопасности и контроля доступа при работе с данными, моделями и AI-сервисами.

Дополнительно объект автоматизации включает процессы масштабирования вычислительных ресурсов, мониторинга работы AI-инфраструктуры и обеспечения отказоустойчивости платформы.

В результате автоматизации обеспечивается переход от разрозненного использования отдельных AI-инструментов к единой централизованной платформе больших языковых моделей, функционирующей в составе цифровой инфраструктуры Банка и обеспечивающей предоставление интеллектуальных сервисов для внутренних систем и пользователей.

Таким образом, объектом автоматизации является совокупность процессов создания, эксплуатации и использования больших языковых моделей, которые в рамках реализации информационной системы «Платформа больших языковых моделей» переводятся в единый централизованный цифровой контур с использованием технологий искусственного интеллекта.

4. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ СИСТЕМЕ

4.1 Требования к ИС в целом

В основе ИС должно лежать современное технологическое решение, обеспечивающее создание, обучение, развертывание и эксплуатацию больших языковых моделей (LLM) с использованием технологий искусственного интеллекта, обработки естественного языка (NLP) и распределенных вычислений.

ИС должна обеспечивать автоматизированную обработку, анализ и генерацию текстовой информации, а также предоставление AI-сервисов внутренним информационным системам и пользователям Банка.

Требования к безопасности AI компонентов:

– фильтрация и валидация входных данных перед передачей в AI-модель;

– контроль корректности и допустимости результатов, формируемых AI-моделью, перед их использованием во внутренних системах и сервисах Банка (output validation);

– ведение журналов запросов, ответов и действий системы для целей аудита, мониторинга и анализа;

– защита от злоупотреблений при взаимодействии с AI-моделями, включая предотвращение prompt-инъекций, некорректных запросов и попыток обхода ограничений модели;

– обеспечение контроля доступа к моделям, данным обучения и AI-сервисам;

– соответствие требованиям безопасности OWASP Top 10 для веб-приложений и API, а также рекомендациям OWASP ASVS.

Все компоненты системы должны быть реализованы с использованием современных технологий и фреймворков, обеспечивающих надежность, масштабируемость, отказоустойчивость и высокую производительность.

Система должна обеспечивать хранение служебных данных, журналов работы, параметров моделей и конфигурационных данных с использованием современных систем управления базами данных (PostgreSQL, MS SQL, Oracle или аналогичных решений).

ИС должна обеспечивать единый механизм аутентификации и авторизации пользователей и администраторов системы с применением механизмов разграничения доступа (RBAC) и многофакторной аутентификации для доступа к административным функциям и вычислительным ресурсам системы.

Интерфейс системы должен поддерживать работу на узбекском, русском и английском языках с возможностью дальнейшего расширения языковой поддержки.

При проектировании программного обеспечения ИС необходимо руководствоваться следующими основными принципами, соответствующими требованиям к системам, использующим технологии искусственного интеллекта:

Масштабируемость.

ИС должна сохранять стабильную работоспособность при увеличении объема данных, количества запросов и числа пользователей. Решение должно предусматривать возможность расширения вычислительных ресурсов по мере роста нагрузки без снижения качества работы больших языковых моделей и скорости обработки запросов.

Для обеспечения масштабируемости система должна поддерживать следующие возможности:

Инфраструктурная масштабируемость:

– возможность горизонтального расширения серверных и вычислительных ресурсов для обработки увеличивающегося потока запросов;

– возможность добавления дополнительных вычислительных узлов, включая GPU-ресурсы, для обеспечения корректной работы AI-моделей при росте нагрузки;

– возможность масштабирования подсистем хранения данных и сервисов обработки информации.

Балансировка нагрузки:

Система должна обеспечивать равномерное распределение входящих запросов между вычислительными ресурсами, предотвращая перегрузку отдельных компонентов. Балансировка нагрузки должна обеспечивать:

– устойчивую работу сервисов при увеличении количества пользователей и запросов;

– автоматическое перераспределение запросов на доступные ресурсы при возникновении сбоев отдельных узлов;

– возможность распределения нагрузки между несколькими экземплярами AI-моделей.

Работа с большими объемами данных:

Для стабильной работы системы при увеличении объема данных необходимо предусмотреть:

– применение механизмов оптимизации хранения данных и доступа к ним;

– использование механизмов кэширования для ускорения обработки запросов и снижения нагрузки на основные сервисы системы;

– поддержку распределенного хранения данных и обработки больших массивов информации.

Техническая поддержка масштабируемости:

– использование технологий контейнеризации и оркестрации контейнеров (Docker, Kubernetes или аналогичных решений) для автоматического распределения вычислительных ресурсов;

– возможность увеличения вычислительных ресурсов системы без остановки основных сервисов;

– поддержку автоматического мониторинга загрузки вычислительных ресурсов и масштабирования компонентов системы в зависимости от уровня нагрузки.

Надежность

ИС должна обеспечивать устойчивую работу, сохранность данных, параметров моделей и результатов обработки информации, а также возможность восстановления после аварийных ситуаций без потери логической целостности данных. Архитектура системы должна предусматривать механизмы резервного копирования, мониторинга,

отказоустойчивости и автоматического восстановления работы сервисов и AI-компонентов.

1. План восстановления после аварийных ситуаций

В системе должны быть установлены следующие параметры:

- RTO (время восстановления) — до 1 часа, что позволит минимизировать перерывы в работе сервисов системы;
- RPO (точка восстановления) — до 30 минут, обеспечивающая минимальную потерю данных и параметров моделей.

Для снижения рисков утраты данных должно обеспечиваться регулярное резервное копирование и синхронизация критически важных компонентов системы.

2. Меры по резервному копированию

Для обеспечения сохранности данных в аварийных ситуациях требуется:

- полное резервное копирование — не реже одного раза в 3 дня;
- инкрементное резервное копирование — не реже одного раза в 45 минут, что позволяет соблюдать установленный показатель RPO;
- резервное копирование конфигураций системы, журналов работы, параметров моделей и данных обучения;
- хранение резервных копий в отдельной инфраструктуре хранения данных или резервном дата-центре;
- шифрование резервных копий с использованием современных криптографических алгоритмов (например AES-256).

3. Резервирование системы

Для обеспечения высокой доступности Система должна включать:

- активно-пассивное резервирование серверов и вычислительных узлов, при котором при сбое основной узел автоматически заменяется резервным;
- использование кластеризации и механизмов балансировки нагрузки для предотвращения простоев;
- дублирование сетевых каналов, систем хранения данных и критически важных компонентов системы;
- возможность масштабирования вычислительных ресурсов, включая GPU-ресурсы, при росте нагрузки;
- автоматический перезапуск контейнеров и сервисов при отказах отдельных компонентов системы.

4. Этапы восстановления

- выявление причин сбоя;

- автоматическое переключение на резервные ресурсы;
- восстановление штатной работы сервисов и AI-компонентов;
- проверка целостности данных и корректности работы моделей;
- проведение анализа причин сбоя и выполнение корректирующих действий.

Информационная безопасность

При разработке Системы должны соблюдаться требования законодательства Республики Узбекистан, включая Закон Республики Узбекистан «О персональных данных», а также внутренние нормативные документы Банка по обеспечению информационной безопасности.

Система может обрабатывать служебные, технологические и пользовательские данные, используемые при обучении, эксплуатации и взаимодействии с большими языковыми моделями. В связи с этим должны быть реализованы организационные и технические меры защиты, направленные на предотвращение несанкционированного доступа, утечки, модификации, уничтожения данных и несанкционированного использования AI-моделей и вычислительных ресурсов.

1. Защита каналов передачи данных

Для защиты данных при передаче должны применяться следующие механизмы криптографической защиты:

- HTTPS (SSL/TLS) — для шифрования трафика между компонентами системы, пользовательскими интерфейсами и серверной инфраструктурой;
- использование протоколов TLS версии 1.2 или 1.3 для всех внешних и внутренних сетевых соединений;
- использование современных криптографических алгоритмов и сертификатов, выданных доверенными центрами сертификации;
- обязательная проверка подлинности сертификатов и защита от атак типа Man-in-the-Middle (MITM).

2. Шифрование данных

Для защиты данных в системе должны применяться современные криптографические механизмы, обеспечивающие конфиденциальность, целостность и защиту информации от несанкционированного доступа.

Используемые стандарты:

- AES-256 — для шифрования данных при хранении (data at rest);
- RSA — для защиты ключей шифрования и обмена криптографическими ключами;
- SHA-256 — для хеширования данных и проверки их целостности.

Управление криптографическими ключами (Key Management):

- использование системы управления ключами (KMS) или аппаратного модуля безопасности (HSM) для генерации, хранения и управления криптографическими ключами;
- ротация криптографических ключей: не реже одного раза в 90 дней для ключей шифрования данных и не реже одного раза в 180 дней для мастер-ключей;
- применение процедуры согласования доступа к криптографическим ключам (access approval) с обязательным документированием;
- ведение аудиторских журналов всех операций с ключами (создание, использование, ротация, отзыв и уничтожение);
- применение политики депонирования ключей (key escrow) для обеспечения непрерывности бизнес-процессов и восстановления доступа к данным при аварийных ситуациях.

3. Аутентификация и авторизация

Для обеспечения безопасного доступа к системе должны быть реализованы следующие механизмы аутентификации и управления доступом:

- JWT (JSON Web Token) — механизм подтверждения подлинности пользователей и сервисов с защитой криптографических ключей;
- MFA — пароль + SMS-код или иной механизм дополнительной верификации;
- разграничение прав доступа (RBAC) с назначением ролей и полномочий пользователей в соответствии с их функциональными обязанностями;
- автоматический тайм-аут пользовательской сессии — 60 минут при отсутствии активности;
- защита от перебора пароля: при 5 неудачных попытках входа учетная запись блокируется на 15 минут, после чего пользователю предоставляется повторно до 5 попыток входа; при повторных 5 неудачных попытках учетная запись блокируется до разблокировки администратором ИС.

Для администраторов ИС доступ должен осуществляться только с применением усиленной многофакторной аутентификации:

- пароль + аппаратный ключ FIDO2;
- блокировка учетной записи администратора после 5 неудачных попыток входа;
- доступ к административным функциям системы должен предоставляться только пользователям с соответствующими ролями и полномочиями.

4. Соответствие требованиям по защите данных

Для выполнения требований законодательства Республики Узбекистан в области защиты персональных данных в системе должны быть реализованы следующие меры:

- применение принципа минимизации данных (data minimization) — сбор и обработка только тех данных, которые необходимы для выполнения функций системы;
- хранение персональных и служебных данных в зашифрованном виде с использованием современных криптографических алгоритмов;
- проведение регулярных аудитов безопасности и проверок соблюдения требований защиты данных;
- контроль использования данных, применяемых для обучения и тестирования моделей искусственного интеллекта;
- исключение несанкционированного использования конфиденциальной информации при обучении и эксплуатации моделей.

Классификация данных и защита от утечек (DLP)

В системе должна быть реализована классификация обрабатываемых данных и меры предотвращения утечки информации.

Классификация данных должна осуществляться по уровням конфиденциальности:

- Публичные данные — информация, доступная неограниченному кругу лиц;
- Внутренние данные — информация, предназначенная для использования внутри Банка;
- Конфиденциальные данные — персональные данные, служебная информация и внутренние документы;
- Строго конфиденциальные данные — данные ограниченного доступа, параметры моделей, ключи шифрования и критически важная технологическая информация.

Для предотвращения утечек информации в системе должны быть реализованы следующие меры:

- ограничение доступа к данным на основе ролей пользователей (RBAC);
- контроль экспорта и передачи конфиденциальных данных за пределы системы;
- использование механизмов DLP для выявления попыток несанкционированной передачи данных;
- регистрация всех операций доступа к конфиденциальным данным в журналах аудита;
- автоматическая очистка пользовательских сессий и временных данных после завершения работы.

Жизненный цикл персональных данных:

- срок хранения данных определяется внутренними нормативными документами Банка и требованиями законодательства Республики Узбекистан;

- должен быть реализован автоматизированный процесс удаления или архивирования данных по истечении установленного срока хранения;
- логическое удаление данных из операционной базы данных с последующим физическим удалением при проведении регламентных процедур очистки;
- удаление или обезличивание данных в резервных копиях по мере истечения срока хранения;
- анонимизация данных для статистических и аналитических целей;
- ведение реестра операций обработки данных;
- документирование согласия субъекта на обработку персональных данных (consent management) при необходимости обработки персональных данных.

5. Защита от сетевых угроз

Для защиты системы от сетевых угроз должны применяться следующие меры:

- использование WAF для предотвращения атак типа SQL-инъекций, XSS, CSRF и других угроз веб-приложений;
- защита от DDoS-атак с применением механизмов мониторинга сетевого трафика, балансировки нагрузки и фильтрации подозрительных запросов;
- использование систем IDS/IPS для обнаружения и предотвращения сетевых атак;
- антивирусная защита серверной инфраструктуры и регулярное обновление антивирусных баз;
- сегментация сети и размещение публичных компонентов системы в DMZ-сегменте;
- ограничение сетевого доступа к вычислительным ресурсам и AI-моделям в соответствии с политиками информационной безопасности Банка.

Стандартизация и унификация

Компоненты ИС должны быть реализованы с использованием единых подходов к разработке, интеграции и сопровождению программного обеспечения.

Для обеспечения унификации система должна:

- использовать единые стандарты взаимодействия между компонентами системы;
- обеспечивать единообразный подход к обработке данных, управлению моделями и вычислительными ресурсами;
- поддерживать интеграцию с внутренними и внешними информационными системами Банка через стандартизированные API;
- использовать единые механизмы аутентификации, авторизации и журналирования событий;
- обеспечивать централизованное управление конфигурациями, параметрами моделей и настройками сервисов;

- использовать единую систему классификации данных и терминологии.

Интерфейс системы должен поддерживать работу на узбекском, русском и английском языках.

4.1.1 Требования к структуре и функционированию ИС

Информационная система «Платформа больших языковых моделей (LLM)» должна включать в себя следующий функционал:

- подготовка, обработка и хранение данных, используемых для обучения и эксплуатации больших языковых моделей;
- обучение, дообучение и тестирование моделей искусственного интеллекта;
- выполнение обработки текстовых запросов с использованием технологий обработки естественного языка (NLP);
- предоставление сервисов взаимодействия с AI-моделями через API;
- интеграция с внутренними информационными системами Банка для получения и обработки данных;
- обеспечение централизованного управления моделями, конфигурациями и вычислительными ресурсами;
- мониторинг работы моделей, вычислительных ресурсов и сервисов системы;
- регистрация и журналирование системных событий, запросов и операций для целей мониторинга, аудита и анализа;
- обеспечение информационной безопасности при обработке данных и эксплуатации AI-моделей.

Архитектура системы должна обеспечивать возможность интеграции с внутренними информационными системами Банка, внешними сервисами, аналитическими платформами и иными системами посредством стандартизированных API и сервисных механизмов взаимодействия.

Система должна предусматривать возможность дальнейшего расширения функциональности, включая подключение новых моделей искусственного интеллекта, увеличение вычислительных ресурсов и развитие сервисов обработки данных и интеллектуального анализа информации.

4.1.1.1 Перечень сторонних ИС, с которыми должно быть обеспечено взаимодействие

Для обеспечения функционирования информационной системы «Платформа больших языковых моделей (LLM)» должно быть реализовано взаимодействие с внутренними информационными системами, источниками данных и вычислительными сервисами.

В рамках проекта предусматривается интеграция со следующими информационными системами и сервисами:

– внутренняя банковская система IABS — для получения и обработки данных, необходимых для обучения, тестирования и эксплуатации AI-моделей;

– внутренние базы данных и хранилища данных Банка — для подготовки обучающих выборок, хранения результатов обработки и аналитической информации;

– системы мониторинга и журналирования — для контроля работоспособности сервисов, мониторинга вычислительных ресурсов и ведения журналов событий;

– сервисы управления вычислительными ресурсами и контейнерной инфраструктурой — для обеспечения функционирования AI-моделей и распределения вычислительной нагрузки;

– внешние и внутренние API-сервисы — для взаимодействия с прикладными системами и предоставления доступа к функциональности LLM-платформы.

Взаимодействие ИС с указанными системами должно осуществляться через защищенные программные интерфейсы (API) с использованием стандартных протоколов обмена данными.

Для интеграционного взаимодействия должны использоваться следующие форматы передачи данных:

– JSON — при взаимодействии через REST API;

– XML — при интеграции с системами, использующими SOAP.

Форматы передаваемых данных, параметры интеграции и состав информационного обмена определяются на этапе технического проектирования и документируются в составе проектной документации.

Разработка и настройка интеграционных механизмов осуществляется Исполнителем при взаимодействии с Заказчиком с соблюдением требований информационной безопасности и внутренних стандартов Банка.

4.1.1.2 Требования к режимам функционирования ИС

Информационная система «Платформа больших языковых моделей (LLM)» должна функционировать круглосуточно и круглогодично, за исключением времени проведения плановых профилактических работ или устранения аварийных ситуаций в инфраструктуре Банка, вычислительных ресурсах, каналах связи, аппаратном и программном обеспечении.

Система должна поддерживать следующие режимы функционирования:

1. **Штатный режим** – основной режим работы системы. В данном режиме ИС обеспечивает полный набор функций, включая обработку запросов, выполнение

задач обработки естественного языка, взаимодействие через API, работу AI-моделей, обработку данных и выполнение вычислительных операций.

2. **Сервисный режим** – режим проведения плановых технических работ (обслуживание оборудования, обновление программного обеспечения, обновление или дообучение моделей, настройка или модернизация компонентов системы). В данном режиме допускается ограниченная работа отдельных сервисов системы.
3. **Аварийный режим** – режим функционирования системы при возникновении непредвиденных ситуаций или сбоев. В данном режиме система может функционировать с ограниченным набором сервисов до устранения причин сбоя и восстановления штатного режима работы.

Для обеспечения функционирования системы в аварийных ситуациях должны быть предусмотрены следующие мер:

- отказоустойчивость серверных и вычислительных компонентов системы за счёт использования резервных ресурсов;
- автоматическое уведомление администраторов системы о возникновении аварийных ситуаций;
- временное ограничение функциональности отдельных сервисов системы до минимально необходимого уровня;
- автоматическое отключение некритичных компонентов системы для ускорения восстановления работоспособности;
- автоматическая синхронизация данных и конфигураций с резервными копиями;
- регулярное резервное копирование данных, параметров моделей, конфигураций и журналов работы системы;
- автоматический перезапуск сервисов и контейнеров при возникновении программных сбоев;
- возможность переключения вычислительной нагрузки на резервные вычислительные ресурсы.

В целом система должна обеспечивать непрерывность функционирования сервисов обработки данных и AI-моделей, а также минимизацию потерь данных и времени простоя при возникновении внештатных ситуаций до полного восстановления штатного режима работы.

4.1.1.3 Перечень и описание сценариев использования ИС

Ниже приведено описание ролей и сценариев использования информационной системы «Платформа больших языковых моделей (LLM)».

Администратор ИС:

Роль администратора ИС является обобщающей и может выполняться несколькими ответственными специалистами (системный администратор, администратор баз данных, ML-инженер, специалист по информационной безопасности) в пределах предоставленных полномочий.

Основные функции:

- создание и управление учетными записями администраторов системы;
- назначение ролей и прав доступа в соответствии с матрицей доступа (Access Matrix);
- разработка и ведение документированной матрицы доступа, определяющей права ролей на уровне функций, моделей, API и данных системы;
- настройка и конфигурирование параметров работы системы и AI-моделей;
- управление процессами обучения, дообучения и развертывания моделей;
- мониторинг работоспособности системы, вычислительных ресурсов и AI-сервисов;
- управление журналами событий и логами безопасности;
- резервное копирование и восстановление данных, конфигураций и параметров моделей;
- устранение ошибок и обеспечение стабильной работы системы.

Права доступа:

Администратор имеет доступ к функциям администрирования системы, включая настройку параметров, управление моделями, просмотр журналов событий и управление конфигурацией сервисов.

Управление привилегированным доступом (PAM):

Для административных операций должны применяться следующие механизмы:

- использование принципа Just-In-Time (JIT) — предоставление привилегированного доступа только на время выполнения административных операций;
- процедура аварийного доступа (break-glass) с обязательным последующим аудитом действий;
- регистрация административных сессий (session recording) при выполнении критических операций;
- обязательная многофакторная аутентификация при входе в систему и выполнении операций управления доступом и конфигурациями.

Сценарий использования A1: Администрирование и управление системой

Условия запуска: необходимость настройки параметров системы, управления доступом, мониторинга работы сервисов или управления AI-моделями.

Основное действующее лицо: Администратор ИС.

Порядок выполнения:

- авторизация администратора в системе с использованием многофакторной аутентификации;
- просмотр текущего состояния системы, вычислительных ресурсов и журналов событий;
- настройка параметров системы, API, AI-моделей или изменение прав доступа;
- запуск или управление процессами обучения и развертывания моделей;
- сохранение изменений и регистрация выполненных действий в журнале аудита

Входные данные: учетные данные администратора и параметры конфигурации системы.

Выходные данные: обновленные параметры конфигурации, изменения состояния сервисов и записи в журналах событий.

Внутренняя информационная система / прикладной сервис

Внешние и внутренние прикладные системы взаимодействуют с LLM-платформой посредством API для выполнения задач обработки естественного языка и интеллектуального анализа данных.

Основные функции:

- отправка запросов на обработку текстовых данных;
- получение результатов обработки AI-моделями;
- использование сервисов генерации, классификации, анализа и обработки текстов;
- интеграция AI-функциональности в прикладные системы Банка.

Сценарий использования S1: Взаимодействие внешней системы с LLM-платформой

Условия запуска: прикладная система направляет запрос на обработку данных в LLM-платформу.

Основное действующее лицо: Внутренняя информационная система или прикладной сервис.

Порядок выполнения:

- прикладная система направляет запрос через API;
- система выполняет проверку авторизации и параметров запроса;
- запрос передается на обработку AI-модели;
- система формирует результат обработки;
- результат возвращается во внешнюю систему через API;
- информация о выполнении операции фиксируется в журнале событий.

Обеспечение надежности: при возникновении ошибок система должна возвращать стандартизированные сообщения об ошибках, регистрировать инциденты и обеспечивать возможность повторной обработки запросов.

Примечание: все действия пользователей, системные события и операции взаимодействия через API фиксируются в журналах событий для целей мониторинга, аудита и обеспечения информационной безопасности.

4.1.1.4 Требования по диагностированию

Информационная система «Платформа больших языковых моделей (LLM)» должна предоставлять инструменты для диагностики состояния системы и её компонентов, а также обеспечивать мониторинг работоспособности AI-моделей, вычислительных ресурсов и интеграционных сервисов.

Диагностика должна обеспечивать своевременное выявление ошибок, сбоев и отклонений в работе системы.

Мониторинг состояния системы

Диагностика программных и технических компонентов системы должна осуществляться с использованием стандартных средств операционных систем серверов, программных средств управления базами данных, платформ контейнеризации и оркестрации, а также специализированных систем мониторинга.

В режиме реального времени система должна отслеживать состояние основных компонентов, включая:

– загрузку вычислительных ресурсов (процессор, оперативная память, GPU, дисковая подсистема);

– время отклика AI-сервисов и API;

– состояние сетевых соединений;

– состояние баз данных и хранилищ данных;

– доступность интеграционных сервисов и внешних систем;

– корректность работы AI-моделей и сервисов обработки данных;

– использование вычислительных ресурсов моделями искусственного интеллекта;

– состояние контейнеров, кластеров и сервисов оркестрации.

Регистрация ошибок и аварий

Все ошибки, предупреждения и сбои системы должны автоматически фиксироваться в журналах событий.

Журналы должны содержать сведения о:

– времени возникновения события;

– типе ошибки или сбоя;

– компоненте системы, в котором возникла ошибка;

– параметрах работы системы на момент возникновения события;

– идентификаторе сервиса или AI-модели, в работе которой возникла ошибка.

Данные журналы должны использоваться для последующего анализа, аудита и устранения причин возникновения ошибок.

Графическая визуализация

Должны быть реализованы дашборды для отображения ключевых показателей работы системы в целом и отдельных компонентов.

Дашборды должны обеспечивать визуальный контроль:

– загрузки вычислительных ресурсов;

– состояния AI-моделей и API-сервисов;

– активности пользователей и интеграционных запросов;

– состояния обработки данных;

– статистики ошибок и отказов.

Система оповещений

Должен быть реализован механизм автоматических уведомлений при обнаружении проблем с возможностью настройки уровней критичности оповещений.

Система должна обеспечивать:

– автоматическое уведомление ответственных специалистов о сбоях и критических событиях;

– регистрацию инцидентов безопасности и отказов сервисов;

– возможность автоматического перезапуска сервисов и контейнеров при возникновении программных сбоев;

– поддержку механизмов автоматического масштабирования вычислительных ресурсов при росте нагрузки.

Отчетность и контроль доступа

Система должна обеспечивать формирование периодических отчетов о состоянии системы, включая статистику работы AI-моделей, вычислительных ресурсов, API и интеграционных сервисов.

Доступ к средствам мониторинга, журналам событий и дашбордам должен предоставляться только уполномоченным пользователям в соответствии с ролевой моделью доступа (RBAC).

Периодическое обслуживание

Тестирование и диагностика программно-технических компонентов должны выполняться автоматически при запуске системы и в процессе эксплуатации.

Для всех компонентов системы должен обеспечиваться регулярный контроль состояния, проверка работоспособности AI-моделей, вычислительных ресурсов и профилактическое обслуживание для поддержания стабильной работы ИС.

4.1.1.5 Перспективы развития и модернизации ИС

При разработке Информационной системы «Платформа больших языковых моделей (LLM)» должны быть предусмотрены возможности последующей модернизации и расширения функциональных возможностей системы при минимальных временных и финансовых затратах.

Архитектура системы должна обеспечивать гибкость, масштабируемость и возможность адаптации к развитию технологий искусственного интеллекта, увеличению объемов данных и росту количества интеграций.

Перспективы развития системы включают следующие направления:

Развитие моделей искусственного интеллекта

- повышение качества и точности генерации текстов и обработки запросов;
- внедрение новых архитектур и версий больших языковых моделей (LLM);
- оптимизация моделей для повышения производительности и снижения времени отклика;
- внедрение механизмов дообучения (fine-tuning) и адаптации моделей под внутренние задачи Банка;
- развитие механизмов Retrieval-Augmented Generation (RAG) для работы с внутренними базами знаний и документами.

Расширение функциональных возможностей платформы

- поддержка дополнительных сценариев использования моделей искусственного интеллекта;
- расширение возможностей API для интеграции с внутренними и внешними информационными системами;
- внедрение инструментов аналитики, мониторинга качества ответов и оценки эффективности моделей;
- развитие сервисов обработки естественного языка (NLP), включая классификацию, суммаризацию, поиск и интеллектуальный анализ текстов.

Развитие интеграционных возможностей

- интеграция с дополнительными внутренними системами Банка;
- интеграция с корпоративными хранилищами данных, базами знаний и документооборотом;
- поддержка взаимодействия с внешними AI-сервисами и платформами;

- развитие API и механизмов безопасного обмена данными.

Расширение языковой поддержки

- повышение качества обработки узбекского языка;
- поддержка дополнительных языков;
- развитие многоязычных моделей и механизмов автоматического перевода.

Техническое развитие системы

- модернизация серверной инфраструктуры и вычислительных ресурсов;
- внедрение новых механизмов масштабирования и балансировки нагрузки;
- оптимизация использования GPU/TPU-ресурсов;
- развитие механизмов контейнеризации, оркестрации и автоматизации развертывания.

Развитие механизмов информационной безопасности

- внедрение новых механизмов защиты AI-моделей и API;
- совершенствование механизмов фильтрации пользовательских запросов и контроля ответов моделей;
- развитие средств мониторинга, аудита и обнаружения инцидентов информационной безопасности;
- внедрение дополнительных механизмов защиты персональных и служебных данных.

Модернизация системы должна осуществляться с учетом:

- изменений нормативно-правовых актов и требований законодательства Республики Узбекистан;
- развития технологий искусственного интеллекта и больших языковых моделей;
- появления новых требований к информационной безопасности и защите данных;
- увеличения нагрузки и объемов обрабатываемых данных.

При развитии системы должна обеспечиваться совместимость новых компонентов с существующей архитектурой, а также сохранность накопленных данных, журналов событий, параметров моделей и результатов обучения.

4.1.2 Требования к взаимодействию со сторонними информационными системами

Взаимодействие Информационной системы «Платформа больших языковых моделей (LLM)» со сторонними информационными системами должно обеспечиваться в соответствии с требованиями государственных стандартов O‘zDSt 2590:2012 «Информационная технология» и O‘zDSt 2864:2014 «Информационная технология. Межведомственная интеграционная платформа. Общие технические условия».

Интеграция должна осуществляться через сервис-ориентированную архитектуру, основанную на веб-сервисах и единых стандартах обмена данными, включающих согласованные форматы данных, классификаторы и описания структур информации. Программные средства веб-сервисов должны фиксировать каждый факт передачи и приема информации, включая уникальный идентификатор сообщения, направление передачи (прием/отправка), дату и время операции, идентификатор взаимодействующей системы и результат обработки сообщения.

ИС должна обеспечивать возможность взаимодействия с внутренними информационными системами Банка, внешними API и прикладными сервисами для получения, обработки и генерации текстовых данных с использованием больших языковых моделей (LLM). В рамках интеграционного взаимодействия осуществляется передача и прием текстовых запросов пользователей, служебных параметров обработки запросов, результатов генерации модели, метаданных запросов, а также данных, необходимых для мониторинга и журналирования работы системы.

Обмен информацией осуществляется посредством веб-сервисов с использованием протоколов REST API и/или SOAP с применением форматов JSON (для REST API) и XML (для SOAP-сервисов).

В рамках реализации системы использование сторонних баз данных не предусматривается. При необходимости подключения внешних информационных ресурсов или моделей их перечень и параметры взаимодействия подлежат уточнению на этапе технического проектирования.

Результаты операций по обмену данными (прием и передача информации) должны регистрироваться в журнале событий системы и предоставляться по запросу администратора информационной системы.

Для обеспечения защищенного обмена данными при интеграции с внешними информационными системами должны быть реализованы меры защиты, соответствующие требованиям внутренних политик информационной безопасности Банка, а также рекомендациям OWASP ASVS и NIST. Интеграционные интерфейсы должны поддерживать защищенные каналы передачи данных с использованием протокола TLS версии 1.2 или выше. Доступ к API должен осуществляться с использованием механизмов аутентификации и авторизации, включая OAuth 2.0 или аналогичные механизмы управления доступом.

Для интеграционных сервисов должны быть реализованы ограничения сетевого доступа, включая использование списков разрешенных IP-адресов (IP allowlist), а также

механизмы ограничения количества запросов (rate limiting) для предотвращения злоупотреблений и перегрузки системы.

Все входящие и исходящие интеграционные сообщения должны проходить проверку структуры и формата данных (schema validation) для исключения передачи некорректных, вредоносных или модифицированных данных. Факты обращения к интеграционным интерфейсам, а также ошибки аутентификации и попытки несанкционированного доступа подлежат обязательному протоколированию и хранению в журналах событий системы для целей мониторинга и аудита безопасности.

4.1.3 Требования к численности и квалификации пользователей

Информационная система «Платформа больших языковых моделей (LLM)» предназначена для использования сотрудниками Банка, а также интеграционными прикладными сервисами и информационными системами, взаимодействующими с LLM-платформой через API.

Максимальное количество пользователей системы определяется техническими возможностями серверной инфраструктуры, параметрами вычислительных ресурсов и архитектурой программного обеспечения.

Система должна обеспечивать возможность одновременной обработки не менее 100 пользовательских запросов к LLM-моделям с возможностью дальнейшего масштабирования в зависимости от технических возможностей серверной инфраструктуры.

Для взаимодействия с системой пользователи должны обладать базовыми навыками работы с информационными системами и цифровыми сервисами. Для технических специалистов, осуществляющих интеграцию с системой, требуется знание принципов работы API, форматов JSON/XML и механизмов аутентификации.

Для обеспечения эксплуатации и сопровождения системы выделяются следующие ответственные лица:

– системный администратор — 1 человек;

– администратор баз данных — 1 человек;

– специалист по информационной безопасности — 1 человек;

– ML/AI инженер — 1 человек.

Ответственные специалисты должны обладать квалификацией в области информационных технологий, включая навыки администрирования серверных систем, управления базами данных, сопровождения AI/LLM-моделей, мониторинга производительности системы и обеспечения информационной безопасности.

Особые требования к режиму работы пользователей не предъявляются. Система функционирует в круглосуточном режиме с возможностью перехода в сервисный и аварийный режимы функционирования.

4.1.4 Показатели назначения

Степень приспособляемости системы к изменениям процессов и методов работы

Система должна обеспечивать адаптацию к увеличению нагрузки при росте количества пользователей, интеграционных сервисов и объема запросов к большим языковым моделям (LLM). Архитектура системы должна обеспечивать возможность подключения новых моделей, расширения вычислительных ресурсов и изменения сценариев обработки запросов без необходимости существенной переработки программного обеспечения.

Система должна поддерживать изменяющиеся требования по информационной безопасности, обеспечивая сохранность, конфиденциальность и целостность обрабатываемых данных.

Система должна обеспечивать возможность одновременной обработки не менее 100 пользовательских запросов к LLM-моделям. Ограничение количества одновременно обрабатываемых запросов определяется техническими характеристиками серверной инфраструктуры и вычислительных ресурсов системы.

Вероятностно-временные характеристики, при которых сохраняется целевое назначение системы

Целевое назначение системы должно сохраняться на протяжении всего срока эксплуатации. Срок эксплуатации определяется устойчивой работой серверного оборудования, своевременным обновлением программных компонентов, AI/LLM-моделей и проведением мероприятий по сопровождению и модернизации системы.

Работоспособность системы не должна нарушаться при превышении номинальной нагрузки. В случае увеличения нагрузки допускается пропорциональное увеличение времени обработки запросов либо временное ограничение обработки низкоприоритетных запросов.

Нагрузочное тестирование и стресс-тестирование

Для обеспечения функциональности при максимальной нагрузке должно быть проведено нагрузочное тестирование с использованием сценариев стресс-тестирования.

Критерии тестирования:

- производительность серверной инфраструктуры и подсистем хранения данных;
- пропускная способность сети;
- время отклика API;

- время обработки пользовательских запросов;
- производительность LLM-моделей при генерации ответов.

Сценарии нагрузочного тестирования:

- проверка работы системы на различных уровнях нагрузки для моделирования реальных условий эксплуатации;
- моделирование одновременной обработки большого количества запросов к LLM-моделям;
- моделирование резких всплесков нагрузки при массовом обращении внешних систем и пользователей.

Стресс-тестирование:

- определение пределов производительности системы для оценки максимального количества одновременно обрабатываемых запросов без критических сбоев;
- использование специализированных инструментов тестирования (Apache JMeter, LoadRunner или аналогичных средств).

Допустимые пороги при максимальной нагрузке:

- время отклика API системы — не более 3 секунд для стандартных запросов;
- среднее время генерации ответа LLM — определяется параметрами используемой модели и вычислительной инфраструктуры;
- процент загрузки вычислительных ресурсов серверной инфраструктуры (CPU, GPU и оперативной памяти) — не более 85%.

Автоматическое восстановление после сбоев и аварий:

Для обеспечения устойчивой работы системы должны быть предусмотрены следующие механизмы:

- регулярное резервное копирование данных и конфигураций системы не реже одного раза в сутки;
- максимальное время восстановления системы после сбоя — не более 2 часов;
- автоматическое переключение на резервные вычислительные ресурсы при сбое основных компонентов;
- автоматическое восстановление работоспособности сервисов после снижения нагрузки до номинального уровня.

Поддержка работоспособности и целевого назначения системы:

Для обеспечения стабильной работы системы должны быть предусмотрены:

- постоянный мониторинг производительности, доступности и безопасности системы;

- регулярные обновления программных компонентов, библиотек и AI/LLM-моделей с минимальным временем простоя;
- контроль состояния серверной инфраструктуры, API и сервисов обработки запросов;
- мониторинг качества генерации ответов моделей и корректности обработки пользовательских запросов.

4.1.5 Требования к надежности

Надежность ИС должна обеспечиваться стабильной работой программного обеспечения, AI/LLM-моделей, интеграционных сервисов, API-интерфейсов, а также комплексов технических и инженерных средств.

Ответственность за работу системы:

Бесперебойная работа технических и инженерных средств возлагается на Заказчика проекта.

Бесперебойная работа программного обеспечения, LLM-платформы, интеграционных механизмов и функциональности системы возлагается на Исполнителя проекта.

Общие требования:

Система должна функционировать круглосуточно, в непрерывном режиме, за исключением времени проведения планового резервного копирования, восстановления данных, обновления программного обеспечения, обновления AI/LLM-моделей и других профилактических работ.

Система должна сохранять работоспособность и обеспечивать восстановление функций при внештатных ситуациях, включая:

- сбои в электроснабжении аппаратной части;
- ошибки аппаратных средств;
- ошибки программного обеспечения;
- сбои в работе отдельных компонентов системы;
- перегрузку вычислительных ресурсов при обработке AI/LLM-запросов;
- недоступность отдельных интеграционных сервисов или API.

Система должна обеспечивать:

- своевременное оповещение администраторов и обслуживающего персонала о случаях нештатной работы;
- диагностику неисправностей и организацию технического обслуживания;
- соблюдение правил эксплуатации и технического обслуживания;

- ведение журналов системных сообщений, ошибок и событий безопасности для анализа и корректировки конфигурации;
- мониторинг состояния AI/LLM-сервисов и вычислительных ресурсов.

Защита аппаратуры

Для обеспечения надежности технической инфраструктуры должны применяться следующие меры:

- применение сетевых фильтров для защиты от перепадов напряжения и коммутационных помех;
- использование отказоустойчивого оборудования и его структурное резервирование;
- горячее резервирование критически важных узлов системы (серверы приложений, серверы AI/LLM-моделей, серверы баз данных, элементы сетевой инфраструктуры);
- дублирование носителей информации и элементов телекоммуникационной сети с обеспечением альтернативной маршрутизации потоков данных;
- резервирование GPU-ресурсов или вычислительных узлов, используемых для работы LLM-моделей.

Надежность программного обеспечения

Надежность программного обеспечения должна обеспечиваться:

- использованием программных средств, обеспечивающих сохранение информации при сбоях;
- проведением тестирования программных компонентов, API и AI/LLM-моделей;
- ведением журналов системных сообщений и ошибок;
- соблюдением правил эксплуатации и регулярным администрированием системы;
- регулярным резервным копированием данных и конфигураций;
- контролем стабильности работы AI/LLM-сервисов и интеграционных компонентов;
- использованием механизмов автоматического перезапуска сервисов при возникновении ошибок;
- контролем корректности ответов AI-моделей и обработкой нештатных сценариев.

Защита данных от отказов и сбоев

Для обеспечения сохранности данных и непрерывности функционирования системы должны быть реализованы следующие меры:

- резервирование критически важных компонентов серверной инфраструктуры, включая процессоры, оперативную память, сетевые интерфейсы и системы хранения данных;
- использование RAID-массивов и механизмов репликации данных;

- автоматическое переключение на резервные вычислительные ресурсы при отказе отдельных серверных компонентов;
- применение кластеризации и механизмов балансировки нагрузки;
- защита данных от сбоев общего и специального программного обеспечения;
- сохранение конфигураций AI/LLM-моделей и параметров системы в резервных копиях.

Методы оценки и контроля надежности

Разработка системы и проверка её надежности выполняются в соответствии с действующими нормативными правовыми актами и организационно-распорядительными документами.

Разрабатываются методики и инструкции для пользователей системы, включая эксплуатационную документацию и регламенты сопровождения системы.

Нормативно-техническая документация должна соответствовать следующим стандартам:

- O‘zDSt 1985:2018 «Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем»;
- O‘zDSt 1986:2018 «Информационная технология. Информационные системы. Стадии создания»;
- O‘zDSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы».

4.1.6 Требования к информационной безопасности

Архитектура системы

Архитектура системы должна обеспечивать логическое и сетевое разделение внешних и внутренних компонентов ИС. Прямой доступ к базам данных, AI/LLM-сервисам и внутренним API из публичных сетей (Интернет) должен быть запрещён.

Компоненты системы, обеспечивающие внешнее взаимодействие с пользователями и интеграцию через API, должны размещаться в отдельном защищённом сегменте сети (DMZ), обеспечивающем изоляцию внутренней инфраструктуры Банка и защиту от внешних угроз.

Во внешнем сегменте допускается размещение следующих компонентов:

- API-шлюзы;
- веб-интерфейсы;
- сервисы обработки пользовательских запросов;
- интеграционные сервисы.

Внутренние компоненты системы (базы данных, AI/LLM-модули, системы хранения данных, сервисы администрирования и мониторинга) должны размещаться во внутреннем защищённом контуре сети с ограничением прямого внешнего доступа.

Межсетевое взаимодействие между сегментами должно осуществляться через контролируемые каналы связи с применением межсетевых экранов (Firewall), WAF и механизмов фильтрации сетевого трафика.

Контроль действий и ведение журналов

Все действия пользователей, администраторов и системных компонентов должны подлежать обязательному протоколированию с хранением журналов событий в формате syslog или эквивалентном стандарте не менее 3 лет.

Протоколирование должно включать:

- обращения к API и AI/LLM-сервисам;
- действия пользователей при взаимодействии с системой, включая ввод запросов и получение ответов;
- действия администраторов системы, включая изменение настроек, управление ролями и правами доступа, обновление компонентов и выполнение операций сопровождения;
- события аутентификации и авторизации;
- системные события, включая состояние серверов, ошибки сервисов, сбои интеграционных компонентов и критические инциденты безопасности;
- события доступа к конфиденциальным данным и попытки несанкционированного доступа.

Для обеспечения целостности и неизменяемости журналов должно использоваться WORM-хранилище или эквивалентная технология защиты журналов.

Журналы событий должны быть интегрированы с SIEM-системой для централизованного мониторинга, корреляции событий безопасности, выявления инцидентов и проведения аудита информационной безопасности.

Доступ к журналам событий должен предоставляться только уполномоченным пользователям на основе ролевой модели доступа (RBAC) с обязательной регистрацией всех операций просмотра, экспорта и удаления журналов.

Требования к неизменяемости логов и интеграции с SIEM:

Система должна обеспечивать защиту журналов аудита от изменения, удаления и несанкционированного доступа, а также интеграцию с SIEM-системой для своевременного выявления и анализа инцидентов информационной безопасности.

Для обеспечения неизменяемости и защищённого хранения журналов должны быть реализованы следующие меры:

- использование WORM-хранилища (Write Once Read Many), S3 Object Lock или аналогичных технологий хранения неизменяемых данных;
- централизованная передача журналов событий в SIEM-систему (QRadar или аналогичную систему) в режиме, близком к реальному времени;
- применение ролевого разграничения доступа (RBAC) к журналам аудита;
- использование механизмов криптографической подписи или контроля целостности записей журналов;
- регистрация всех операций доступа, просмотра, экспорта и удаления журналов событий;
- синхронизация времени серверов и компонентов системы с использованием доверенного источника времени для обеспечения корректности временных меток журналов.

Журналы аудита должны использоваться для мониторинга событий безопасности, расследования инцидентов, проведения внутреннего аудита и контроля соблюдения требований информационной безопасности Банка.

Сценарии мониторинга SIEM (Use-cases) с уровнями критичности:

Для своевременного выявления инцидентов информационной безопасности система должна поддерживать интеграцию с SIEM и обработку событий безопасности с назначением уровней критичности.

Основные сценарии мониторинга:

- множественные неудачные попытки входа (brute-force) — уровень Critical;
- изменение прав доступа, ролей и политик безопасности — уровень High;
- доступ к системе или данным в нерабочее время — уровень Medium;
- массовая выгрузка или экспорт данных — уровень Critical;
- аномальная активность AI/LLM-модели или резкое увеличение количества запросов — уровень High;
- попытки обращения к запрещённым API или сервисам — уровень High;
- ошибки аутентификации сервисных учетных записей — уровень Medium.

Система должна поддерживать ежедневный и еженедельный контроль журналов событий и инцидентов информационной безопасности.

Протоколирование должно включать:

- события аутентификации и авторизации (успешные и неуспешные попытки входа, завершение сессий);

- действия администраторов и пользователей, связанные с изменением конфигурации системы;
- операции создания, изменения и удаления данных;
- события доступа к API и интеграционным интерфейсам;
- подтверждение целостности конфигураций и системных компонентов.

Безопасность контента и конфиденциальность

Система должна обеспечивать защиту, целостность и конфиденциальность обрабатываемых данных.

Для этого должны быть реализованы следующие меры:

- контроль целостности и неизменяемости данных и журналов;
- ограничение типов и размеров загружаемых файлов;
- проверка загружаемых файлов на наличие вредоносного содержимого;
- шифрование данных в СУБД с использованием встроенных механизмов или сертифицированных криптографических средств;
- применение цифровой подписи и механизмов контроля целостности для критически важных данных и конфигураций;
- ограничение доступа к данным в соответствии с ролевой моделью безопасности (RBAC).

Жизненный цикл и поддержка

Все программные компоненты системы должны поддерживаться Исполнителем в течение всего срока эксплуатации системы.

Для обеспечения безопасной и стабильной работы системы должны выполняться:

- регулярное обновление программных компонентов и устранение выявленных уязвимостей;
- установка обновлений безопасности и патчей;
- регулярный аудит информационной безопасности;
- проведение тестирования на уязвимости, нагрузочного и стресс-тестирования;
- проверка устойчивости системы к некорректным или вредоносным пользовательским запросам;
- проведение резервного копирования и проверка процедур восстановления;
- предоставление Заказчику права проведения тестирования на проникновение (penetration testing) с обязательным устранением выявленных критических уязвимостей.

Управление изменениями (Change Management)

Для внесения изменений в компоненты системы должен применяться регламентированный процесс управления изменениями, обеспечивающий контроль безопасности и минимизацию рисков нарушения работоспособности системы.

В рамках процесса управления изменениями должны быть реализованы следующие меры:

- согласование изменений через Совет по изменениям (CAB — Change Advisory Board) с обязательным участием представителей службы информационной безопасности;
- обязательная проверка безопасности (Security Gate) перед внедрением изменений в промышленную среду;
- документирование всех изменений, включая описание, состав изменений, результаты тестирования и ответственных лиц;
- применение процедуры экстренных изменений с последующим обязательным ретроспективным согласованием;
- предварительное тестирование процедуры отката (rollback) перед каждым релизом;
- разделение сред разработки, тестирования и промышленной эксплуатации.

Требования к безопасному жизненному циклу разработки (Secure SDLC)

Разработка, тестирование и внедрение компонентов системы должны выполняться в рамках безопасного жизненного цикла разработки программного обеспечения (Secure SDLC).

При реализации процессов разработки и CI/CD должны применяться следующие меры безопасности:

- SAST (Static Application Security Testing) — статический анализ исходного кода;
- DAST (Dynamic Application Security Testing) — динамическое тестирование приложений;
- SCA (Software Composition Analysis) — анализ сторонних библиотек и зависимостей на наличие уязвимостей;
- Secret Scanning — автоматическое выявление секретов и учетных данных в исходном коде;
- IaC Scanning — проверка конфигураций инфраструктуры как кода;
- обязательный Code Review для критически важных компонентов системы;
- автоматизированная проверка безопасности перед публикацией изменений в промышленную среду;
- ведение журналов операций CI/CD и контроля изменений.

Разработка системы должна предусматривать минимизацию использования небезопасных или неподдерживаемых компонентов программного обеспечения.

Соответствие стандартам

Система должна соответствовать действующим нормативным требованиям Республики Узбекистан, а также международным стандартам в области информационных технологий и информационной безопасности.

При разработке, внедрении и эксплуатации системы должны учитываться требования следующих нормативных документов и 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»;
- O‘z DSt ISO/IEC 27002:2018 — «Информационная технология. Практические правила управления информационной безопасностью»;
- рекомендации OWASP Top 10 и OWASP ASVS;
- рекомендации NIST по обеспечению информационной безопасности и безопасной разработке программного обеспечения.

Мониторинг, аудит и реагирование на инциденты

Для своевременного выявления угроз информационной безопасности, предотвращения несанкционированного доступа и минимизации последствий инцидентов в системе должны быть реализованы механизмы мониторинга, аудита и реагирования на инциденты информационной безопасности.

В системе должны применяться следующие меры:

- использование IDS/IPS для обнаружения и предотвращения сетевых атак и попыток несанкционированного доступа;
- протоколирование критических операций, включая:
  - входы и выходы пользователей;
  - неудачные попытки аутентификации;
  - изменение ролей и прав доступа;
  - действия администраторов системы;
  - операции изменения конфигурации системы
- автоматическое уведомление администраторов и специалистов по информационной безопасности при выявлении подозрительной активности;

- регулярный анализ журналов событий и проведение аудита безопасности;
- проведение периодического сканирования уязвимостей и проверки защищенности компонентов системы.

Для реагирования на инциденты информационной безопасности должен быть разработан и поддерживаться IRP (Incident Response Plan), включающий:

- идентификацию и классификацию инцидентов;
- локализацию и ограничение воздействия инцидента;
- восстановление работоспособности системы;
- документирование инцидентов и результатов расследования;
- уведомление уполномоченных лиц и регулирующих органов в случаях, предусмотренных законодательством и внутренними нормативными документами Банка;
- анализ причин инцидента и реализацию мер по предотвращению повторных случаев.

RP должен предусматривать:

- подготовку сценариев реагирования (playbook) для типовых инцидентов, включая:
  - утечку данных;
  - DDoS-атаки;
  - компрометацию учетных записей;
  - вредоносное программное обеспечение (ransomware);
- распределение ролей и ответственности между ответственными сотрудниками;
- регламент времени реагирования на инциденты:
  - Critical — до 1 часа;
  - High — до 2 часов;
  - Medium — до 4 часов;
  - Low — до 24 часов;
- проведение тестирования и актуализации плана реагирования не реже одного раза в квартал.

Безопасность технических средств

Технические средства системы должны соответствовать требованиям безопасности, надежности и электромагнитной защиты, установленным нормативными документами Республики Узбекистан и действующими стандартами.

При эксплуатации технических средств должны соблюдаться следующие требования:

- монтаж, наладка, эксплуатация и техническое обслуживание оборудования должны исключать воздействие опасных уровней электрического тока, электромагнитных полей, шума и вибраций;
- оборудование должно обеспечивать защиту персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003-75 и ГОСТ 12.2.007.0-75;
- электропитание оборудования должно предусматривать защиту от перегрузок, коротких замыканий и аварийное отключение;
- кабели электропитания и линии связи должны быть защищены от повреждений и несанкционированного доступа;
- помещения серверной инфраструктуры и дата-центров должны соответствовать требованиям O‘z DSt 2875:2014 и RH 45-201:2011;
- серверное оборудование должно быть подключено к источникам бесперебойного питания (ИБП);
- критически важные компоненты инфраструктуры должны быть защищены от отказов аппаратных компонентов, включая процессоры, оперативную память, сетевые интерфейсы и системы хранения данных;
- должны применяться механизмы аппаратного резервирования и автоматического переключения на резервные компоненты при отказах;
- оборудование должно обеспечивать устойчивость к внешним электромагнитным воздействиям и соответствовать требованиям по электромагнитной совместимости;
- все используемые технические и программные средства должны быть серийными, поддерживаемыми производителем и сертифицированными в установленном порядке.

Разграничение доступа и аутентификация

Система должна обеспечивать разграничение доступа пользователей к функциям и данным на основе ролевой модели доступа (RBAC).

Для обеспечения безопасности доступа должны быть реализованы следующие меры:

- идентификация и аутентификация пользователей с использованием уникальных учетных записей;
- использование паролей длиной не менее 8 символов с обязательным наличием цифр и специальных символов;
- возможность самостоятельного изменения пароля пользователем;
- автоматическая блокировка пользовательской сессии при отсутствии активности;

- ограничение количества неуспешных попыток аутентификации с временной блокировкой учетной записи;
- применение многофакторной аутентификации для административных учетных записей;
- ведение журналов действий пользователей и администраторов;
- предоставление доступа к журналам только уполномоченным администраторам;
- запрет изменения и удаления записей журналов событий;
- контроль корректности вводимых данных по типу, формату и допустимым диапазонам значений;
- ограничение типов загружаемых файлов и контроль их максимального размера.

Сохранность информации при авариях

Система должна обеспечивать сохранность информации и возможность восстановления данных при возникновении аварийных ситуаций, программных сбоев или отказов аппаратных компонентов.

Для обеспечения сохранности данных должны быть реализованы следующие меры:

- возможность полного или частичного восстановления данных;
- резервирование и дублирование данных на резервные устройства хранения;
- регулярное резервное копирование баз данных с хранением резервных копий в отдельной инфраструктуре;
- восстановление данных в согласованное и непротиворечивое состояние после сбоев;
- применение механизмов репликации и резервирования данных;
- контроль успешности выполнения процедур резервного копирования и восстановления.

Защита от внешних воздействий

Технические средства системы должны быть защищены от внешних воздействий, способных повлиять на стабильность и безопасность функционирования системы.

Для обеспечения защиты должны соблюдаться следующие требования:

- размещение серверного оборудования вдали от источников тепла и электромагнитных помех;
- соблюдение климатических условий эксплуатации:
  - температура — от 10 °C до 50 °C;
  - относительная влажность — от 15 % до 60 %;
  - атмосферное давление — от 84 до 107 кПа;

- подключение серверного оборудования к источникам бесперебойного питания (ИБП);
- защита оборудования от перепадов напряжения и аварийного отключения электропитания;
- обеспечение устойчивости технических средств к воздействию электромагнитных помех и радиоэлектронных воздействий;
- соблюдение требований электромагнитной совместимости (ЭМС);
- исключение взаимного влияния компонентов системы и внешних источников радиоэлектронных помех.

Защита от сбоев компонентов

Архитектура системы должна обеспечивать отказоустойчивость и сохранность данных при сбоях программных и аппаратных компонентов.

Для обеспечения устойчивой работы системы должны быть реализованы следующие меры:

- защита данных от сбоев общего и специального программного обеспечения;
- обеспечение работоспособности системы при отказе отдельных подсистем или серверов;
- применение механизмов кластеризации, резервирования и автоматического переключения на резервные ресурсы;
- обеспечение отказоустойчивости при сбоях процессоров, оперативной памяти, сетевых интерфейсов и систем хранения данных;
- исключение единой точки отказа (Single Point of Failure) для критически важных компонентов;
- автоматическое восстановление работоспособности системы после сбоев;
- использование резервных копий и механизмов репликации для восстановления данных и сервисов.

4.1.7 Требования к эргономике и технической эстетике

Интерфейс и навигация

Интерфейс системы должен обеспечивать удобное и интуитивно понятное взаимодействие пользователей с сервисами платформы больших языковых моделей (LLM) и связанными прикладными сервисами.

Интерфейс системы должен:

- иметь логически организованную структуру и понятные элементы навигации;
- обеспечивать минимальное количество действий для выполнения основных операций;

- корректно отображаться на различных типах устройств и разрешениях экранов;
- обеспечивать понятное отображение информации и результатов обработки запросов;
- поддерживать отображение уведомлений, сообщений об ошибках и результатов выполнения операций;
- обеспечивать единообразие элементов интерфейса и навигации во всех модулях системы.

При использовании API-интерфейсов система должна обеспечивать:

- стандартизированные форматы запросов и ответов;
- единообразную структуру сообщений об ошибках;
- документирование API и параметров взаимодействия;
- поддержку механизмов версионирования API.

Визуальная эстетика и корпоративный стиль

Пользовательские интерфейсы прикладных компонентов системы должны соответствовать корпоративному стилю Банка.

При разработке интерфейсов должны соблюдаться следующие требования:

- использование читаемых шрифтов и контрастных цветовых схем;
- унификация графических элементов и компонентов интерфейса;
- минимизация визуально перегруженных элементов;
- обеспечение удобства восприятия информации при длительной работе пользователей с системой.

Поддержка нескольких языков

Система должна поддерживать:

- узбекский язык;
- русский язык;
- английский язык.

Для каждого поддерживаемого языка должны обеспечиваться:

- корректное отображение текстовой информации;
- поддержка локализации интерфейсов и сообщений системы;
- единообразие терминологии и форматов отображения данных.

Удобство использования и юзабилити

При разработке системы должны применяться принципы usability и user experience (UX).

Для обеспечения удобства использования должны быть реализованы:

- проведение тестирования пользовательских сценариев;

- отображение понятных уведомлений и подсказок;
- информирование пользователей о возникающих ошибках и способах их устранения;
- логическая группировка элементов управления и параметров системы;
- обеспечение быстрого отклика интерфейсов и сервисов системы.

Общие требования

Система должна обеспечивать:

- минимизацию избыточных визуальных эффектов, влияющих на производительность;
- стабильную работу интерфейсов при различных уровнях нагрузки;
- совместимость с современными браузерами и программными платформами;
- соответствие требованиям эргономики и технической эстетики, установленным действующими нормативными документами.

Результат

Интерфейсы и сервисы системы должны обеспечивать удобство эксплуатации, снижение вероятности ошибок пользователей и эффективное взаимодействие с платформой больших языковых моделей (LLM).

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

1. Условия эксплуатации и регламент

- Условия эксплуатации, режим работы и периодичность технического обслуживания компонентов системы должны соответствовать эксплуатационной документации производителей оборудования и программного обеспечения.
- Система должна функционировать в круглосуточном режиме при обеспечении бесперебойного электропитания и отказоустойчивой инфраструктуры.
- Плановое техническое обслуживание компонентов системы (серверное оборудование, сетевые устройства, системы хранения данных, источники бесперебойного питания) должно проводиться не реже одного раза в год.
- Обслуживание включает:
    - визуальный и аппаратный осмотр оборудования;
    - очистку компонентов от пыли и загрязнений;
    - проверка и подтяжка контактных соединений;
    - контроль параметров работы оборудования и систем;

- тестирование взаимодействия всех ключевых компонентов системы.

- Размещение оборудования должно соответствовать требованиям промышленной, пожарной и информационной безопасности.

2. Размещение оборудования и требования к площадям и электроснабжению

- Размещение компонентов системы осуществляется в защищённых помещениях Заказчика или в сертифицированных дата-центрах.
- Помещения должны обеспечивать физическую защиту оборудования и ограничение несанкционированного доступа.
- Электропитание должно соответствовать следующим требованиям:
  - подключение к источникам бесперебойного питания с автономной работой не менее 15 минут;
  - резервирование питания критически важных узлов системы;
  - соответствие параметров электроснабжения требованиям ГОСТ 32144-2013.

3. Требования к персоналу

- Численность и квалификация обслуживающего персонала определяются на этапе ввода системы в эксплуатацию.
- Специалисты должны обеспечивать:
  - эксплуатацию и сопровождение программно-технических средств;
  - настройку и администрирование компонентов системы;
  - мониторинг работы сервисов и анализ их состояния;
  - реагирование на аварийные и внештатные ситуации.
- Персонал должен обладать компетенциями в области:
  - информационных технологий и системной архитектуры;
  - эксплуатации серверной и сетевой инфраструктуры;
  - работы с системами обработки данных и сервисами виртуального помощника;
  - обеспечения информационной безопасности.

4. Запасные части и компоненты

- Система является стационарной и разворачивается на инфраструктуре Заказчика.
- Требования к отдельным комплектам запасных изделий и приборов не устанавливаются.

5. Регламент обслуживания

- Эксплуатация и обслуживание системы осуществляются службой эксплуатации Заказчика в соответствии с эксплуатационной документацией.
- В обязанности персонала входит:

- настройка и сопровождение компонентов системы;
- анализ работы программных и аппаратных средств;
- поддержка пользователей в рамках регламентированных полномочий;
- контроль функционирования ключевых сервисов системы.

6. Санитарные нормы и электромагнитное воздействие

- Уровни электромагнитных излучений должны соответствовать установленным санитарным нормам и не превышать допустимые значения.
- Должны соблюдаться требования:
  - санитарных норм допустимых уровней электромагнитных полей радиочастот (СанПиН № 0064-96);
  - санитарных норм уровней электростатических полей на рабочих местах (СанПиН № 0121-01).

4.1.10 Требования к патентной и лицензионной чистоте

- Все проектные решения, используемые при разработке и внедрении системы, должны соответствовать требованиям патентной чистоты в соответствии с законодательством Республики Узбекистан.
- Авторские и имущественные права на создаваемое программное обеспечение определяются действующим законодательством Республики Узбекистан и условиями договора между Заказчиком и Исполнителем.
- Лицензирование программного обеспечения должно обеспечивать:
  - бессрочное право использования системы;
  - отсутствие ограничений по количеству пользователей;
  - отсутствие ограничений по количеству развертываний и техническим характеристикам используемой инфраструктуры.
- При использовании сторонних программных продуктов, библиотек и сервисов условия лицензирования не должны ограничивать функциональность системы или препятствовать её эксплуатации по назначению.

4.1.11 Требования по стандартизации и унификации

Для обеспечения единообразия реализации функций и снижения сложности сопровождения система должна быть построена на основе принципов стандартизации и унификации.

Проектные решения при реализации функций системы должны обеспечивать:

- соблюдение единых правил построения пользовательских интерфейсов;
- единообразную реакцию системы на некорректные действия пользователей и ошибки ввода;

- использование унифицированных справочников и классификаторов при заполнении реквизитов;
- применение фиксированного и согласованного перечня терминов и определений при взаимодействии пользователя с системой и виртуальным помощником;
- единый подход к разграничению прав доступа пользователей к данным и функциям системы;
- максимальное использование стандартных библиотек, фреймворков и компонентных решений.

Программное обеспечение системы должно строиться на основе модульной и компонентной архитектуры с использованием повторно применяемых программных модулей для реализации типовых функций.

Функционирование системы должно обеспечиваться за счёт применения:

- стандартных программно-аппаратных комплексов;
- унифицированных форм представления и обмена данными;
- единых международных и отраслевых классификаторов;
- общепринятых международных стандартов в области информационных технологий.

Унификация проектных решений должна обеспечиваться за счёт:

- единообразного подхода к реализации однотипных функций;
- стандартизации технического, информационного, лингвистического и организационного обеспечения системы.

Единообразие решений достигается за счёт:

- унификации функциональной структуры и взаимодействия компонентов системы;
- применения единых подходов к реализации сервисов, включая взаимодействие с LLM-компонентами и внешними API.

Унификация технических решений обеспечивается за счёт:

- использования серийного и стандартизированного оборудования;
- минимизации разнообразия используемых технических компонентов;
- применения типовых архитектурных решений для вычислительной и сетевой инфраструктуры.

4.1.12 Дополнительные требования*

Дополнительные требования не предъявляются.

4.2 Требования к функциям (задачам), выполняемым ИС

1. **Общая структура системы:**

- Система должна представлять собой набор взаимосвязанных программных компонентов и сервисов, обеспечивающих функционирование платформы больших языковых моделей (LLM) и прикладных сервисов виртуального помощника.
- Взаимодействие между компонентами системы должно быть автоматизировано и не требовать вмешательства оператора, за исключением случаев аварийных ситуаций, отсутствия связи или проведения регламентных работ.

2. **Процесс управления обновлениями и исправлениями модулей:**

- В системе должен быть реализован централизованный механизм управления обновлениями (patch management), включающий:
    - мониторинг состояния компонентов системы;
    - планирование и согласование обновлений;
    - тестирование изменений в изолированной среде;
    - внедрение обновлений в продуктивную среду.
- Все изменения должны предварительно проходить проверку на совместимость с существующими компонентами системы.

3. **Регулярное обновление модулей:**

- Для поддержания актуальности функциональности и безопасности системы должны выполняться регулярные обновления.
- Обновления выпускаются:
    - в виде плановых релизов (не реже одного раза в квартал);
    - внепланово — при выявлении критических ошибок или уязвимостей.

4. **Процесс экстренного патчирования:**

- Для устранения критических уязвимостей и ошибок должен быть предусмотрен механизм экстренного обновления компонентов системы.
- Экстренные изменения допускается внедрять в сокращённом цикле тестирования при обязательном последующем контроле стабильности и корректности работы системы.

5. **Документация и уведомления:**

- Все обновления должны сопровождаться документацией, включающей:
    - описание внесённых изменений;
    - влияние на функциональность системы;
    - при необходимости — инструкции по эксплуатации после обновления.

- Пользователи и администраторы системы должны своевременно получать уведомления о внесённых изменениях через встроенные механизмы оповещения или административные каналы.

6. **План действий при возникновении проблем:**

- В системе должен быть предусмотрен регламент восстановления работоспособности при сбоях, возникающих в процессе обновления, включая:
    - откат изменений (rollback);
    - восстановление из резервных копий;
    - проверку целостности и работоспособности системы после восстановления;
    - контроль стабильности работы после возврата к предыдущей версии.

4.3 Требования к видам обеспечения

4.3.1 Требования к математическому обеспечению*

При разработке системы должны использоваться современные математические методы, модели и алгоритмы, обеспечивающие корректную и эффективную обработку данных, а также функционирование сервисов платформы больших языковых моделей (LLM).

Математическое обеспечение системы должно включать:

- применение стандартных методов обработки естественного языка (NLP) для анализа пользовательских запросов;
- использование алгоритмов машинного обучения и глубокого обучения для работы языковых моделей;
- применение вероятностных и статистических моделей для оценки и ранжирования ответов системы;
- использование алгоритмов оптимизации для повышения производительности и точности обработки запросов;
- реализацию механизмов фильтрации, нормализации и предобработки входных данных пользователей.

Для обеспечения качества работы системы должны использоваться проверенные и документированные алгоритмы, обеспечивающие воспроизводимость результатов и стабильность работы сервисов.

Математические модели и алгоритмы должны быть реализованы с учетом требований масштабируемости, устойчивости к нагрузкам и возможности последующего улучшения без нарушения целостности функционирования системы.

4.3.2 Требования к информационному обеспечению

Состав, структура и способы организации данных в системе определяются на этапе рабочего проектирования с учётом требований функциональности платформы и интеграции с внешними и внутренними информационными системами.

Организация информационного обмена:

Обмен данными между компонентами системы должен осуществляться через унифицированные интерфейсы (API) с использованием согласованных форматов данных, обеспечивающих корректность, целостность и согласованность информации при передаче между сервисами системы.

Хранение данных:

Хранение данных системы должно осуществляться с использованием современной системы управления базами данных (СУБД) реляционного типа.

Для обеспечения целостности, согласованности и отказоустойчивости данных должны использоваться встроенные механизмы СУБД, включая транзакционность и контроль целостности.

Структура базы данных:

База данных системы должна быть структурирована с соблюдением принципов нормализации и включать следующие основные логические разделы:

- Раздел основных данных — для хранения ключевой информации, используемой функциональными модулями системы;
- Раздел служебных данных — для хранения конфигурационной информации и параметров функционирования системы;
- Раздел журналов и мониторинга — для хранения логов, событий системы и данных аудита.

Структура базы данных должна соответствовать требованиям O‘zDSt 1135:2007.

Совместимость информационного обеспечения:

Информационное обеспечение системы должно обеспечивать совместимость с внешними и внутренними информационными ресурсами по:

- структуре данных;
- форматам обмена;
- методам кодирования;
- правилам идентификации и адресации;
- формам представления информации.

Используемые стандарты и классификаторы:

При разработке системы должны применяться стандартные и зарегистрированные

классификаторы, унифицированные справочники и формы данных.

Все компоненты системы должны обеспечивать единообразную обработку и интерпретацию информации.

Надёжность хранения данных:

Система должна обеспечивать сохранность данных при сбоях и аварийных ситуациях.

Резервное копирование должно выполняться регулярно и обеспечивать возможность полного восстановления данных.

Перечень баз данных и схем хранения определяется на этапе проектирования и согласуется с Заказчиком.

Контроль и валидация данных:

В системе должны быть реализованы механизмы контроля корректности данных, включая:

- проверку типов данных;
- проверку диапазонов допустимых значений;
- контроль обязательности заполнения полей;
- проверку логической согласованности информации.

Классификация и идентификация данных:

Все данные системы должны быть классифицированы по уровню критичности и доступу.

Для обеспечения однозначной идентификации объектов должны использоваться уникальные идентификаторы, исключающие дублирование и обеспечивающие целостность данных.

Актуализация и ведение данных:

Система должна обеспечивать актуальность данных за счёт:

- обновления информации из внутренних и внешних источников;
- синхронизации данных между компонентами системы;
- контроля устаревших и некорректных записей.

Также должны быть предусмотрены процедуры сопровождения данных, включая корректировку, архивирование и удаление в соответствии с регламентами хранения информации.

4.3.3 Требования к лингвистическому обеспечению

ИС должна обеспечивать многоязычную поддержку пользовательского взаимодействия в зависимости от выбранных пользователем настроек.

Поддерживаемые языки:

- Узбекский (латиница)
- Русский (кириллица)
- Английский (латиница)

Особенности работы с данными:

- система должна обеспечивать корректную обработку, хранение, передачу и отображение текстовой информации независимо от языка ввода и языка интерфейса;
- поддержка различных кодировок и символов национальных алфавитов, включая специальные символы и знаки.

Требования к лингвистическому обеспечению:

- в системе должна использоваться единая и согласованная терминология предметной области банковских услуг;
- все элементы интерфейса (сообщения, уведомления, меню, формы и ошибки) должны иметь корректный перевод на все поддерживаемые языки;
- сообщения системы должны быть однозначными, понятными пользователю и при необходимости содержать рекомендации по дальнейшим действиям;
- должна обеспечиваться единообразная стилистика текстов во всех языковых версиях системы;
- интерфейсные и системные сообщения должны быть адаптированы с учётом языковых и культурных особенностей пользователей.

Цель требований:

Обеспечение корректного и унифицированного отображения информации на различных языках, повышение удобства взаимодействия пользователей с системой и снижение вероятности ошибок, связанных с языковыми различиями.

4.3.4 Требования к программному обеспечению

Программное обеспечение системы должно обеспечивать выполнение всех функциональных задач платформы больших языковых моделей (LLM) и связанных сервисов виртуального помощника:

1. **Функциональность и готовность**

- Программное обеспечение должно обеспечивать реализацию всех функций системы в полном объёме.
- Должен быть обеспечен корректный обмен данными между компонентами системы с сохранением целостности информации.
- Должна быть реализована возможность создания, ведения и использования справочников и служебных данных.

2. **Совместимость и интеграция**

- Программное обеспечение должно быть совместимо с используемыми техническими средствами, системным программным обеспечением и инфраструктурой развертывания.
- Должна обеспечиваться информационная совместимость между модулями системы в рамках единых протоколов обмена данными.
- Должен быть обеспечен оперативный доступ к данным с возможностью их представления в виде структурированных форм, таблиц и отчётов (внутренние сервисные представления).

3. Качество программного обеспечения

- Программное обеспечение должно соответствовать требованиям O‘zDSt ISO/IEC 25051:2008 «Требования к качеству и оценка программного продукта».
- Должна обеспечиваться стабильная работа системы при сетевом взаимодействии, высокой нагрузке и параллельной обработке запросов пользователей.

4. Дополнительное программное обеспечение

Для функционирования системы допускается использование системного и прикладного программного обеспечения, включая:

- операционные системы серверного уровня;
- системы управления базами данных;
- веб-серверы и API-шлюзы;
- средства обработки и выполнения моделей искусственного интеллекта.

Конкретный перечень программных средств определяется на этапе проектирования и согласуется с Заказчиком.

5. Независимость программных средств

Программное обеспечение системы должно быть максимально независимым от конкретных аппаратных платформ и операционных систем. Архитектура системы должна обеспечивать:

- модульность компонентов;
- переносимость между средами развертывания;
- возможность масштабирования без существенной переработки кода;
- адаптацию к различным инфраструктурным решениям с минимальными изменениями.

4.3.5 Требования к техническому обеспечению

Технические средства системы должны обеспечивать необходимую производительность, отказоустойчивость и масштабируемость для стабильного

функционирования платформы больших языковых моделей (LLM) и связанных сервисов виртуального помощника.

К техническим средствам системы относятся:

- сервер базы данных;
- сервер приложений (backend/API и сервисы обработки запросов);
- серверы обработки моделей искусственного интеллекта (LLM, STT/TTS сервисы);
- терминальные устройства пользователей.

Минимальные требования к серверу базы данных:

- процессор: не менее 8 ядер, частота не ниже 2,40 ГГц, кэш не менее 12 МБ;
- оперативная память: не менее 8 ГБ;
- дисковая подсистема: не менее 200 ГБ SSD/HDD;
- сетевой интерфейс для взаимодействия с другими компонентами системы.

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

- процессор: не менее 8 ядер, частота не ниже 2,40 ГГц, кэш не менее 12 МБ;
- оперативная память: не менее 8 ГБ;
- дисковая подсистема: не менее 200 ГБ SSD/HDD;
- сетевой интерфейс для взаимодействия с другими компонентами системы.

Минимальные требования к серверу приложений ИС:

- процессор: не менее 8 ядер, частота не ниже 2,40 ГГц, кэш не менее 12 МБ;
- оперативная память: не менее 8 ГБ;
- дисковая подсистема: не менее 200 ГБ SSD/HDD;
- сетевой интерфейс для взаимодействия с внутренними и внешними сервисами системы;
- при необходимости — поддержка GPU-ускорения для выполнения задач обработки искусственного интеллекта (в зависимости от архитектуры решения).

Минимальные требования к серверу обработки ИИ-моделей (LLM/STT/TTS)

- процессор: не менее 16 ядер;
- оперативная память: не менее 32 ГБ;
- графический ускоритель (GPU): с объёмом видеопамяти не менее 16 ГБ;
- дисковая подсистема: не менее 500 ГБ SSD;
- высокоскоростной сетевой интерфейс для обмена данными с API и сервисами системы.

Минимальные требования к терминальным устройствам пользователей

- экран: разрешение не ниже Full HD, поддержка сенсорного ввода (при использовании интерактивного терминала);
- камера: не ниже 1080p, поддержка видеопотока для задач распознавания лица (при необходимости);
- микрофон: с поддержкой шумоподавления для работы в офисной среде;
- динамики: достаточное качество и громкость для голосового взаимодействия с системой;
- сенсорный интерфейс: отклик не более 50 мс, поддержка мультитач (при наличии сенсорного управления).

Общие требования

- технические средства должны обеспечивать возможность горизонтального и вертикального масштабирования;
- должна быть обеспечена отказоустойчивость за счёт резервирования ключевых компонентов;
- оборудование должно поддерживать круглосуточный режим эксплуатации;
- архитектура должна исключать единые точки отказа для критически важных компонентов системы.

4.3.6 Требования к метрологическому обеспечению*

Требования не предъявляются.

4.3.7 Требования к организационному обеспечению

Организационное обеспечение ИС должно обеспечивать эффективную эксплуатацию системы и выполнение персоналом своих функциональных обязанностей при использовании платформы больших языковых моделей (LLM) и сервисов виртуального помощника.

Должны быть определены должностные лица, ответственные за следующие направления:

- обработку и сопровождение информации в системе;
- администрирование программно-технических средств системы;
- обеспечение информационной безопасности;
- управление эксплуатацией и поддержкой пользователей системы.

К работе с ИС допускаются сотрудники, обладающие базовыми навыками работы с персональными компьютерами и цифровыми интерфейсами, а также прошедшие обучение по правилам эксплуатации системы и требованиям информационной безопасности.

Пользователи и обслуживающий персонал системы должны проходить обязательный инструктаж, включающий:

- правила работы с системой и взаимодействия с виртуальным помощником;
- требования информационной безопасности и защиты данных;
- правила эксплуатации оборудования и соблюдения регламентов работы;
- действия при возникновении нештатных ситуаций и инцидентов безопасности.

4.3.8 Требования к защите от ошибочных действий пользователей

- Система должна обеспечивать предотвращение критических ошибок пользователей за счёт реализации механизмов валидации и проверки корректности вводимых данных на уровне интерфейса и серверной логики.
- Для потенциально опасных операций (удаление данных, изменение конфигурации, выполнение административных действий, проведение финансовых операций) должны применяться механизмы обязательного подтверждения выполнения действия.
- Пользовательский интерфейс должен минимизировать вероятность ошибочных действий за счёт использования подсказок, контекстной помощи, автозаполнения, а также ограничений на ввод недопустимых значений.
- Должны быть предусмотрены механизмы отката (rollback) или восстановления данных при выполнении ошибочных операций, в пределах допустимых транзакционных сценариев системы.
- Система должна обеспечивать разграничение прав доступа пользователей на основе ролевой модели (RBAC), исключающей возможность выполнения операций, не соответствующих их полномочиям.
- Все действия пользователей и результат их выполнения должны протоколироваться с целью последующего анализа, выявления ошибок и проведения аудита.

4.3.9 Требования к методическому обеспечению

ИС должна разрабатываться с учётом действующих нормативных правовых актов Республики Узбекистан, а также внутренних организационно-распорядительных документов Заказчика.

В процессе проектирования и внедрения системы должны учитываться административные регламенты Заказчика, определяющие:

- процессы банковского обслуживания и взаимодействия с клиентами;
- функции структурных подразделений и сотрудников;
- распределение полномочий, прав и ответственности при использовании ИС.

Должны быть разработаны, согласованы и утверждены в установленном порядке

эксплуатационные и пользовательские инструкции, регламентирующие порядок работы пользователей с системой и взаимодействия с виртуальным помощником.

Состав методического обеспечения уточняется на этапах проектирования и внедрения системы и подлежит согласованию с Заказчиком.

Методическое обеспечение должно включать:

- нормативные правовые и регламентирующие документы;
- инструкции пользователей по работе с функционалом системы;
- должностные инструкции персонала, обеспечивающего эксплуатацию, сопровождение и администрирование системы.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Перечень стадий и этапов работ по созданию ИС должен соответствовать требованиям O‘z DSt 1986:2018 и включать следующие основные стадии:

1 стадия — анализ требований проекта;

2 стадия — подготовка и обработка данных для обучения модели;

3 стадия — создание и обучение большой языковой модели (LLM);

4 стадия — интеграция с внутренними информационными системами и тестирование;

5 стадия — ввод в эксплуатацию и мониторинг функционирования.

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Контроль, испытания и приемка ИС осуществляются в соответствии с требованиями ГОСТ 34.603-92 и включают следующие основные виды испытаний:

1. предварительные испытания;
2. опытная эксплуатация;
3. приемочные испытания (ввод в промышленную эксплуатацию).

Предварительные испытания выполняются после завершения Исполнителем разработки, отладки и внутреннего тестирования системы, а также при условии предоставления документации, подтверждающей готовность системы к испытаниям, и обучения персонала Заказчика по эксплуатации системы.

Опытная эксплуатация проводится с целью проверки соответствия функциональных возможностей системы установленным требованиям, а также оценки стабильности работы ИС в условиях, приближенных к промышленной эксплуатации, с участием пользователей Заказчика.

Приемочные испытания проводятся для подтверждения соответствия системы требованиям настоящего технического задания, оценки результатов опытной эксплуатации и принятия решения о вводе системы в промышленную эксплуатацию.

В ходе испытаний проверяются:

1. корректность и полнота выполнения программно-техническими средствами автоматизированных функций во всех режимах функционирования системы;
2. уровень подготовки персонала и его способность выполнять действия в соответствии с эксплуатационной документацией;
3. полнота и достаточность эксплуатационной документации для выполнения пользователями своих функций;
4. количественные и качественные показатели функционирования системы в соответствии с требованиями технического задания;
5. иные характеристики системы, предусмотренные настоящим техническим заданием.

Приемка выполненных работ и ввод системы в эксплуатацию осуществляются комиссией Заказчика с обязательным участием представителей Исполнителя.

Испытания системы могут проводиться на площадке Исполнителя либо на инфраструктуре Заказчика по согласованию сторон.

По результатам испытаний Исполнитель оформляет акт приемки выполненных работ, подписываемый Заказчиком. В случае выявления замечаний оформляется протокол испытаний с указанием выявленных недостатков, сроков их устранения и ответственных исполнителей.

Дополнительные требования Заказчика, выявленные в процессе испытаний и опытной эксплуатации и не предусмотренные настоящим техническим заданием, не являются основанием для отказа в приемке системы и подлежат реализации в рамках отдельных соглашений и согласованных сроков выполнения.

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

7.1. Технические мероприятия

В ходе реализации проекта на объекте автоматизации выполняются работы по подготовке к вводу в эксплуатацию ИС «Платформы больших языковых моделей (LLM)».

При подготовке к вводу в эксплуатацию должно быть обеспечено выполнение следующих работ:

- определить ответственных должностных лиц Заказчика за внедрение системы и

проведение опытной эксплуатации;

- обеспечить участие специалистов Заказчика в обучении работе с платформой, проводимом Исполнителем;
- обеспечить готовность программно-технической инфраструктуры (серверы, сети, контейнерная среда, API-шлюзы) для развертывания LLM-платформы;
- совместно с Исполнителем подготовить план развертывания платформы в целевой инфраструктуре Заказчика;
- провести опытную эксплуатацию системы и проверку интеграционных сценариев (API, сервисы, внешние модели и т.д.).

Состав и содержание работ уточняются на стадии рабочей документации и по результатам опытной эксплуатации.

7.2. Обучение персонала

До передачи системы в промышленную эксплуатацию Исполнитель должен подготовить комплект эксплуатационной документации, включающий:

- Руководство пользователя;
- Руководство администратора;
- Руководство по интеграции и использованию API платформы (при необходимости).

Также Исполнитель обязан провести обучение персонала Заказчика по использованию системы и её техническому сопровождению на основе разработанной документации.

Программа обучения должна быть дифференцирована по категориям пользователей в зависимости от их роли и уровня технической подготовки (например: администраторы системы, разработчики/интеграторы, специалисты по сопровождению, конечные пользователи API).

Практическая часть обучения должна включать работу в тестовой (песочнице) среде платформы для отработки навыков взаимодействия с функциональностью системы, API-интерфейсами, инструментами мониторинга и средствами управления моделью.

По завершении обучения для каждой категории пользователей должно проводиться контрольное тестирование с целью оценки уровня усвоения материала и готовности к работе в продуктивной среде.

Для обеспечения доступности информации должны быть разработаны текстовые и видеоматериалы (инструкции, гайды, демонстрации сценариев использования). Указанные материалы должны размещаться во внутреннем корпоративном контуре Заказчика и охватывать ключевые сценарии использования платформы, включая работу с API, моделями и сервисами.

Особое внимание должно уделяться обучению пользователей с различным уровнем технической подготовки, включая специалистов без опыта работы с LLM-платформами.

В течение первых шести месяцев после ввода системы в эксплуатацию должна обеспечиваться постпусковая поддержка пользователей, включая консультации, разбор инцидентов и оперативное решение возникающих вопросов.

По результатам промышленной эксплуатации допускается актуализация учебных материалов с учетом фактических сценариев использования системы и выявленных потребностей пользователей.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Перечень документации технического и рабочего проектирования должен соответствовать номенклатуре, установленной O‘zDSt 1985:2018. Исполнитель по результатам выполнения работ обязан предоставить полный комплект документации, необходимой для эксплуатации Платформы больших языковых моделей (LLM) и отражающей её текущее состояние на момент передачи в промышленную эксплуатацию.

Комплект документации технического проекта передается Заказчику в двух экземплярах на бумажном носителе, а также в электронном виде (на электронных носителях или через согласованные средства передачи данных Заказчика).

Проектная документация подлежит обязательному согласованию и утверждению Заказчиком.

Перечень документации, предоставляемой Заказчику на этапах тестирования системы и при подписании акта о вводе в опытную эксплуатацию, включает:

- общее описание разработанной Информационной системы «Платформа больших языковых моделей (LLM)»;
- программу и методику испытаний платформы;
- руководство пользователя платформы;
- руководство администратора платформы;
- документацию по API;
- описание архитектуры системы и компонентов развертывания.