«УТВЕРЖДАЮ»
АКБ «БАНК РАЗВИТИЯ БИЗНЕСА»
Заместитель Председателя правления Вохидов О.

«27» сентября 2024 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Автоматизация информационной системы "KYC/AML/CFT/SS" и создание системы управления процессами комплаенс контроля банка.

«СОГЛАСОВАНО»
Директор департамента
Комплаенс контроля
_____Юсупов Ж.
«____»_____ 2024 г.

«СОГЛАСОВАНО»
Директор департамента
Информационные технологии
_____Исломов У.
«____»_____ 2024 г.

Ташкент – 2024 г.

СОДЕРЖАНИЕ

1. Общие сведения

1.1. Полное наименование информационной системы и ее условные обозначения

Полное наименование проекта – автоматизация информационных системы **KYC/AML/CFT и Sanction screening.**

Условный знак информационной системы: «KYC/AML/CFT/SS»

1.2. Наименование организаций-заказчиков и разработчиков информационной системы:

АКБ «Банк развития бизнеса» является Заказчиком данной информационной системы в рамках технической заявки.

Адрес «Заказчика»: 100011, г. Ташкент, Шайхантахурский район, улица А.Навои, дом 18А; тел..: (998-78) 150 00 55 (1254);

МФО: 01037; ИНН: 206 916 313, р/с: 19909 000 6 00001037 001;

Название банка: АТБ "Банк развития бизнеса ", Главное операционное управление

Адрес электронной почты: headoffice@brb.uz.

Организация, разрабатывающая информационную систему, определяется по результатам конкурса.

1.3 Перечень документов, на основании которых создается информационная система:

1) "Правила внутреннего контроля по противодействию легализации доходов, полученных от преступной деятельности, финансированию терроризма и финансированию распространения оружия массового уничтожения в коммерческих банках", зарегистрировано Министерством юстиции Республики Узбекистан 23 мая 2017 г., регистрационный № 2886.

2) Стратегия действий по совершенствованию системы внутреннего контроля в сфере ПОД/ФТ/ФРОМУ в АКБ “Кишлок курилиш банк”, составлена аудиторской компанией Deloitte & Touche и утверждена Наблюдательным советом Банка 27 марта 2022 года.

3) План практических мер по цифровизации банковской деятельности - видеоконференции 23 октября 2023 года (автоматизация системы комплаенса)

1.4 Плановые сроки начала и окончания работы по созданию информационной системы (ИС):

Начало: 15.01.2025 года.

Окончание: 15.04.2026 года.

1.5 Порядок оформления и представления результатов работ

На основании данного технического задания между Заказчиком и Разработчиком информационной системы может быть организована удаленная

работа. С учетом требований Политики информационной безопасности Заказчика, при необходимости, можно обеспечить, чтобы к серверам, расположенным по установленной Заказчиком схеме, имели доступ программисты через удаленный канал защиты.

Объем работ для Разработчика информационной системы должен определяться в соответствии с функциональными требованиями к создаваемой системе (пункт 4).

Разработчик должен организовать работу по созданию информационной системы, сформировав проектную команду. Работа по созданию системы проводится и принимается поэтапно.

По окончании каждого этапа работ стороны подписывают акты по данному этапу.

После получения права на использование программного обеспечения стороны подписывают акты передачи и принятия права на использование программного обеспечения.

Передача результатов работ по созданию информационной системы Заказчику и приемка работ осуществляются на основании актов выполненных работ.

Работы по после(пост)гарантийному обслуживанию выполняются в рамках дополнительного соглашения о техподдержке.

1.6 Исполнитель

Исполнитель по данному проекту будет определен на основе результатов тендерного отбора.

Исполнитель должен:

- иметь опыт работы в данном направлении не менее 3 лет;
- предоставить информацию по реализации аналогичных проектов в течение последних 3 (трех) лет до начала настоящего проекта;
- предоставить информации по персональному составу проектной команды (подтверждение наличия специалистов (инженеров/разработчиков) в штате Исполнителя, подтвердивших свою квалификацию сертификатами от ведущих мировых поставщиков предлагаемого решения).
- представить свое Техническое предложение по поставке решения, удовлетворяющие всем требованиям данного документа.

Для определения критериев технической оценки, Участником (Претендентом) должна быть предоставлена следующая дополнительная информация по:

- Последующей замене специалистов (Осуществляется только на эквивалентных по опыту специалистов. Предварительное согласование с Заказчиком является обязательным).
- Наличие обязательств по решению вопросов «языкового барьера» (в рамках данного Технического Задания) при работе с сотрудниками Заказчика на стороне

Исполнителя является обязательным.

- совокупной стоимости владения ТСО (Total Cost of Ownership) за счет предлагаемого решения (лицензирование, расходы на техподдержку, подписка к сервисам, функционала, уникальных решений производителя и т.п. сроком на не менее 5 лет).

При этом, для расширения круга потенциальных участников в тендерных торгах, в рамках выделенного бюджета заказчиком будут рассматриваться аналогичные решения, в том числе с превосходящими характеристиками, которое выполняет все поставленные цели и задачи, указанные в настоящем техническом задании с учетом целевого назначения и показателей. В этой связи, в случае предоставления аналогичного решения необходимо предоставить:

- технико-экономическую информацию по результативности и эффективности;
- расчет финансовых затрат по взаимоинтеграции с существующей инфраструктурой (миграция, перенос или замена).

Исполнитель должен предоставить информацию по:

- сервисам и подпискам;
- условиям лицензирования при их наличии (объем предоставления, порядок взимания платы, срок действия лицензий и др.);
- перечню осуществляемых работ (услуг) с конкретизацией объема и привлекаемых специалистов (обоснование формирования стоимости оказываемых услуг).

Исполнитель должен предоставить полностью укомплектованное и работоспособное решение, необходимое для обеспечения полноты использования запрашиваемой конфигурации в рамках выделенного бюджета.

2. Назначение и цели создания информационной системы

2.1. Назначение информационной системы

Информационная система «KYC/AML/CFT/SS» выполняет несколько основных функций для управления сложными процессами контроля в банке:

- выявление и оценка рисков, документирование;
- надлежащая проверка и идентификация клиентов, а также регулярное обновление информации о клиентах и их бенефициарных владельцах и её верификация;
- тщательный мониторинг операций, осуществляемых публичными должностными лицами, членами их семей и лицами, близкими к ним;
- ведение национальных, международных и санкционных списков;
- эффективное выявление операций, связанных с лицами, включенными в национальные, международные и санкционные списки;
- безотлагательное приостановление операции, за исключением операций по зачислению денежных средств, поступивших на счет

юридического или физического лица, и (или) замораживание денежных средств или иного имущества лиц, включенных в Перечень, без их предварительного уведомления;

- обеспечение хранения информации об операциях, а также идентификационных данных и материалов по надлежащей проверке клиентов в течение сроков, установленных законодательством;
- выявление сомнительных и подозрительных операций;
- своевременное предоставление в специальный уполномоченный государственный орган информации (документов) о подозрительных операциях, выявленных в ходе осуществления внутреннего контроля;
- выявление по запросам в клиентской базе лиц, связанных с легализацией доходов, полученных от преступной деятельности, финансированием террористической деятельности и (или) финансированием распространения оружия массового уничтожения.

2.2. Цели создания информационной системы

При разработке программного обеспечения ставятся следующие основные цели:

- управление национальными, международными и санкционными списками;
- высокоприоритетными документами;
- выявление операций, связанных с лицами, включенными в национальные, международные и санкционные списки, а также с высокопоставленными должностными лицами;
- проверка операций (скрининг) по запрещенным товарам и товарам двойного назначения;
- мониторинг физического/юридического лица (расчет уровней санкционных и других рисков);
- отслеживание и анализ транзакций;
- отправка обнаруженных подозрительных операций в компетентные государственные органы и формирование отчетов по формам отправленных сообщений;
- единое удобное рабочее место для специалиста: сбор информации, обработка документов, процессов, управление коммуникациями, управление расследованием, управление сроком действия документов.

3. Характеристика объекта информатизации.

Задачи, которые планируется решить с помощью системы: автоматизация ручного труда, снижение операционных издержек, оптимизация процессов комплаенс контроля, работа на единой платформе, централизация функций, контроль за выполнением поставленных задач, автоматизация процессов между Головным офисом и филиалами.

На данный момент большая часть работы по комплаенс контролю в банке выполняется вручную.

4. Требования к информационной системе

4.1. Требования к информационной системе в целом

Требованием настоящего ТЗ определяется построение базового хранилища структурированных/полуструктурированных данных и внедрение системы анализа данных. Проект является частью Дорожной карты построения хранилища данных, систем их анализа и визуализации (утвержден Решением Правления банка № 37 от 11 ноября 2022 г), в рамках которого предусмотрено поэтапное внедрение хранилища данных, моделей расширенной аналитики и озера данных. Следовательно, Исполнитель проекта должен разрабатывать ИС с учётом дальнейшего развития инфраструктуры данных. Подсистемы разрабатываемой ИС в рамках настоящего ТЗ, а именно Подсистема анализа (BI система расширенной аналитики), Подсистема интеграции данных и подсистема хранения данных не должны ограничивать/исключать далнейшее развитие хранилища данных, а именно возможность внедрения инструментов расширенной аналитики, экспорта и импорта данных с систем хранения неструктурированных данных.

4.1.1 Требования к функциям (задачам), выполняемым информационной системы

Система работает по следующему принципу:

1. **Сбор данных и анализ**: система собирает данные о клиентах с использованием различных источников, таких как документы клиента, базы данных государственных органов, базы данных международных организаций и т.д. Собранные данные включают личную информацию, финансовую историю, и другие данные, необходимые для проведения KYC (Знай своего клиента), AML (Противодействие отмыванию денег), CFT (Противодействие финансированию терроризма) и SS (Санкционные списки).
2. **Анализ рисков**: система проводит анализ рисков на основе собранных данных, выявляя потенциальные риски по каждому клиенту или транзакции. Это включает оценку вероятности того, что клиент или операция связаны с мошенничеством, отмыванием денег или финансированием терроризма.
3. **Принятие решений**: на основе результатов анализа система генерирует рекомендации или предупреждения о клиентах или транзакциях, которые требуют дополнительного внимания или могут требовать дополнительных проверок. Эти решения могут быть автоматическими (при отсутствии рисков) или требовать вмешательства комплаенс-службы для дальнейшего анализа.
4. **Отчетность и аудит**: система генерирует отчеты о выполнении требований KYC/AML/CFT/SS для органов регулирования и внутренних аудиторов. Эти отчеты включают информацию о проведенных проверках, выявленных рисках, принятых мерах и результатах расследований.
5. **Обновление данных и мониторинг**: система обновляет данные о клиентах в режиме реального времени и непрерывно мониторит активность

клиентов для выявления любых изменений, которые могут потребовать пересмотра рисков.

Целью такой системы является обеспечение соответствия законодательным требованиям в области финансовой безопасности и снижение рисков финансовых преступлений за счет автоматизации процессов и повышения эффективности контроля.

4.1.1.1 Требования к режиму работы (эксплуатации) информационной системы

Информационная система должна работать в режиме 24*7.

Для информационной системы определены следующие режимы работы

- нормальный режим функционирования;
- аварийный режим функционирования.

Основным режимом функционирования Системы является нормальный режим. В нормальном режиме функционирования Системы:

- бесперебойная работа (без перерывов на техническое обслуживание) технических средств пользователей и системных администраторов;
- круглосуточная работа (без перерывов) в обслуживании серверного программного обеспечения и технических средств;
- корректная работа оборудования, составляющего комплекс технических средств;
- корректная работа информационной системы.

Для обеспечения (корректной) нормальной работы системы необходимо соблюдать требования, установленные в соответствующей технической документации (техническая документация, инструкции по эксплуатации и т.д.), и поддерживать условия для эксплуатации аппаратного комплекса программного обеспечения и системы.

Аварийный режим работы системы характеризуется отказом одного или нескольких программных и (или) аппаратных компонентов.

Если система переходит из обычного режима в аварийный, нужно:

- во время сохранения данных выключить все приложения;
- создать резервную копию базы данных.

После этого необходимо провести ряд мероприятий по устранению причин перехода системы в аварийное состояние.

Непрерывная работа информационной системы должна обеспечиваться посредством кластеризации.

4.1.1.2 Перечень подсистем, их задачи и основные характеристики, требования к сегментации

Система должна состоять из отдельных блоков и отчетов, которые интегрированы друг с другом, но работают независимо друг от друга и включать в себя следующие модули и отчеты:

- Подсистема "Авторизация и аутентификация пользователей";

- подсистема "Администрирование" (Administration);

- Подсистема "Запись каждого действия в системе" (Logging);

- Подсистема "Резервное копирование и восстановление данных";

-Подсистема "Управление взаимодействием с внешними информационными системами";

- Подсистема идентификации и повторной идентификации физических/ юридических лиц;

- Подсистема «управление Списками»;

- Блок скрининга транзакций (санкции и товары двойного назначения);

- Мониторинга транзакций (AML сценарии и анализ связей);

- Единое рабочее место для специалиста соответствия.

Список модулей и атрибутов должен обеспечивать полную реализацию всех указанных целей.

4.1.1.3 Требования к диагностике информационной системы

Информационная система должна включать средства диагностики.

Все компоненты информационной системы должны иметь средства диагностики рабочего состояния.

Диагностика работы каждого отдельного компонента создаваемой информационной системы и ее информационной инфраструктуры должна проводиться с использованием самой информационной системы.

Диагностика основных процессов системы, реализация программы должны обеспечивать инструменты для мониторинга процессов.

Компоненты должны обеспечивать удобный интерфейс для просмотра диагностических явлений/событий и мониторинга процесса выполнения программы.

В случае возникновения аварийных ситуаций или ошибок в программном обеспечении средства диагностики должны позволять Разработчику сохранять полный набор информации, необходимой для выявления проблемы (журнал процессов, содержащий информацию о текущем состоянии памяти и текущем состоянии файловой системы).

4.1.1.4 Перспективы развития, модернизации информационной системы

Должна быть возможность модернизации системы. Кроме того, необходимо обеспечить возможность повышения производительности системы за счет ее масштабирования.

В процессе разработки системы она должна быть спроектирована таким образом, чтобы в перспективе можно было увеличить функциональность системы. С целью повышения эффективности системы и удовлетворения потребностей пользователей расширяются функциональные возможности

системы. Модернизация и развитие системы должны осуществляться с учетом факторов, обеспечивающих их экономическую целесообразность.

Система должна позволять переносить программное обеспечение на новое оборудование без изменения программного кода.

4.1.1 Требования к функциям (задачам), выполняемым информационной 4.1.2 Требования к взаимодействию с внешними информационными системами

Для полноценной работы платформы необходимо отправлять запросы во внешние системы.

Список запросов и данных в рамках взаимодействия с системами представлен в таблице:

№	Система	Детализация
1	Сервисное обслуживание шин iABS	Интеграция с системой ABS банка. 1. Модуль ведения клиентов и счетов; 2. Кредитный модуль; 3. Сберегательный/депозитный модуль; 4. Пластиковый модуль; 5. Валютное управление; 6. Ввод платежных документов; 7. Мониторинг; 8. И другие.
2	Внешние веб серверы	- Загрузка и ежедневное автоматическое обновление бесплатных списков (OFAC, EU, UN, UK и так далее) - Загрузка данных из гос услуг (ГЦП -Государственный центр персонализации ЕБП - Единая база предпринимателей и.т.д.) - Загрузка данных из СУГО – (Специально уполномоченный государственный орган)
3	Внешние серверы	*При необходимости*

В будущем должна быть возможность расширить этот список в случае необходимости.

В таблице приведен краткий перечень операций. Состав операций, схема взаимодействия и протоколы запросов будут разработаны позже.

Обмен данными в системе должен поддерживать форматы JSON, xml, csv.

Интеграция с базой данных банка.

Интеграция системы с банковским хранилищем данных осуществляется с целью загрузки данных в систему.

Для автомотический загрузки данных в систему банковский буфер дополняет таблицы схемы. Один раз в день таблицы должны заполняться текущими данными.

Импорт данных

Согласно таблице технологического окна, актуальная информация должна загружаться один раз в день.

Для загрузки новых или измененных данных необходимо заполнить соответствующие поля в таблицах схемы буфера базы данных.

Создание каталогов (для полей, заполненных каталожной информацией) состоит из двух функциональных частей:

Таблицы ссылок в базовой схеме базы данных. Ссылки заполняются администратором программы. Список каталогов будет определен позже.

Если данные не могут быть импортированы из-за отсутствия соответствующих данных при импорте, это регистрируется в журнале импорта. Чтобы устранить ошибку, администратор программы может отредактировать справочную карту через системный интерфейс. Если этой информации нет в каталоге основной схемы базы данных, администратор также включит информацию из этого каталога в основную схему.

4.1.3 Требования к количеству и квалификации пользователей

Система должна поддерживать несколько категорий пользователей, каждая из которых должна обладать своими правами и возможностями.

№	Рол	Власти
1	Администратор	изменить настройки системы; государственная служба (ролики и рухсаты); Готовые настройки системы;
2	Пользователь	удаление изменения раздела данных подтверждение введенной информации формирование отчетов и данных
3	Наблюдатель (просмотр)	просмотр, отслеживание данных; формирование отчетов и данных.

Требования к администратору:

- Профессиональные знания современных методов управления операционными системами, базами данных;
- Знание сетевых и телекоммуникационных технологий;
- Знание технологий информационной безопасности;
- Хорошее знание функционала системы, умение работать с любым компонентом системы.

Требования пользователя:

- Пользователи созданной информационной системы должны обладать знаниями на уровне пользователя персонального компьютера.

Требования к наблюдателю:

- Наблюдатели созданной информационной системы должны обладать знаниями на уровне пользователя персонального компьютера.

Для ее бесперебойной работы система должна поддерживать работу не менее 50 активных внутренних пользователей (сотрудников заказчика) с учетом пользователей, оказывающих помощь и техническое обслуживание (администраторов и специалистов отдела поддержки). Должна быть возможность увеличить количество пользователей как минимум на 20%.

Это должно обеспечить одновременную работу всех сотрудников в процессе работы. Система не должна влиять на сроки выполнения транзакций внешних систем, которые предполагается интегрировать в режиме онлайн.

В процессе обучения пользователей работе с программой оно должно осуществляться с помощью инструкций администратора программы.

При работе с созданной Информационной системой эффективность обучения пользователей контролируется частотой обращений в службу поддержки.

4.1.4 Индикаторы функционирование

Не меняя системного программного обеспечения, необходимо обеспечить возможность расширения работы за счет обновления набора используемых технических средств, в том числе увеличения количества пользователей от расчетного значения.

Система должна обеспечивать следующие функции реагирования для операционных систем:

- навигация по экранным формам не более 10 секунд,
- поиск и фильтрация не более 1 минуты,
- создание отчета за 1 период в месяц (20 атрибутов) не более 1 минуты;
- создание отчета за 1 период в один год (20 атрибутов) не более 5 минут;
- Загрузка подготовленных данных из 15 000 строк и 20 столбцов в Excel не более 2 минут,
- добавление эффектов не более 15 секунд.
- В случае длительных операций система должна выдать пользователю специальное уведомление.

4.1.5 Требования к надежности информационной системы

Показатели надежности системы должны определяться текущими требованиями к надежности автоматизированных информационных систем для государственных органов и управления и определяться в концептуальном проекте.

Также в концептуальном проекте должны быть определены методы и средства выполнения работ в случае сбоев системы.

Показатели надежности должны обеспечиваться в соответствии с требованиями к надежности оборудования и электроснабжения, а также за счет выполнения следующих организационных мероприятий:

- предварительное обучение пользователей и обслуживающего персонала;
- своевременное выполнение процессов управления;
- соблюдение правил использования и обслуживания;
- своевременное выполнение процедур резервного копирования данных.

Показатели надежности должны определяться приблизительной частотой возникновения аварийных ситуаций. Для системы показатели надежности регламентированы для следующих типов аварийных ситуаций:

Общесистемный сбой выражается в отсутствии всех или большинства пользовательских интерфейсов системы, независимо от причин, вызвавших этот сбой (аппаратное обеспечение, телекоммуникации, сбои в общем системном программном обеспечении, некорректная работа специализированных программ, ошибки сотрудников, отключение питания). сбои и т.д.), за исключением фатальных причин (форс-мажорных обстоятельств): не более 5% рабочего времени, не чаще 2 раз в месяц.

Частичный отказ характеризуется невозможностью доступа к одному из интерфейсов какого-либо функционального компонента или его неисправностью (отклонение от порядка функционирования, установленного в требованиях технических условий, проектной или рабочей документации на систему): не чаще 4. раз в месяц, не более 10% рабочего времени.

Стабильная работа обеспечивается при локальных отказах компонентов системы:

- отказе автоматизированной рабочей станции;
- отказе линии связи или сегмента локальной сети;
- отказе центрального сервера.

Безопасность информации в системе должна быть обеспечена в следующих чрезвычайных ситуациях:

- перебои в электроснабжении (кратковременное снижение при резком увеличении нагрузки на электрическую сеть, значительное повышение напряжения в краткосрочной перспективе, полное отключение электроэнергии из-за аварий, перегрузок);
- Отключение или выход из строя каналов связи локальной сети заказчика;
- полный или частичный выход из строя технических средств системы, включая сбои и отказоустойчивость
- жесткие диски;
- сбой общих или специальных системных программ;
- ошибки в работе управленческого или технического персонала;
- выход из строя комплекса технических средств в результате техногенных аварий повреждение внешних каналов связи, нарушение работы системы электроснабжения здания;

- отказ элемента сетевой инфраструктуры системы.

Состав и количественные значения показателей надежности для всей системы или ее подсистем

Показатели надежности:

коэффициент доступности 0,99;

время восстановления всей системы составляет 4 часа;

для отдельных подсистем время восстановления не превышает 2 часов.

Требования к надежности оборудование и программного обеспечения

Надежность программного обеспечения подсистемы должна обеспечиваться за счет:

- надежности системного программного обеспечения и программного обеспечения разработчика;
- реализация комплекса мероприятий по исправлению неполадок, поиску и устранению ошибок;
- ведение системных сообщений и журналов ошибок по подсистемам для дальнейшего анализа и внесения изменений в конфигурацию.

4.1.6 Требования к безопасности информационной системы

Все технические решения, используемые в системе, должны соответствовать общим требованиям безопасности программных комплексов при эксплуатации информационных систем, включая требования к настройке, эксплуатации и техническому обслуживанию.

При эксплуатации системы сотрудниками должны соблюдаться общие правила безопасности.

Аутентификация, основанная на современных технологиях, должна обеспечивать безопасность доступа к данным посредством идентификации и ролевых прав пользователей.

Система должна иметь автоматический журнал аудита, который обеспечивает возможность отслеживать наиболее важные (уникальные) данные, хранящиеся в базе данных, и фиксировать все произошедшие события.

Все системы должны работать во внутренней сети банка.

Перед началом разработки системы заказчик представляет требования политики информационной безопасности, применяемые к объекту информационной безопасности. При осуществлении деятельности и обеспечении информационной безопасности необходимо учитывать требования, предъявляемые при разработке системы для предотвращения конфликтных ситуаций.

В экстренных ситуациях необходимо обеспечить возможность аварийного прекращения доступа к системе.

Система должна предусматривать средства защиты данных от несанкционированного доступа неавторизованных пользователей.

Программная платформа должна обеспечивать возможность гибкого распределения полномочий по ее управлению и использованию. Образец необходим для предоставления доступа к определенным разделам графического интерфейса пользователя и для выполнения определенных действий по управлению платформой.

Пакет защиты системы должен включать:

Средства аутентификации пользователей и элементов платформы (рабочие станции, задачи, элементы базы данных и т.д.)

Средства ограничения доступа пользователей на уровне задач и информационных массивов по ролевой матрице (Логин/пароль) логинов.

Удаленный доступ к базе данных должен предоставляться только через разрабатываемую платформу, за исключением случаев, когда сотрудники заказчика имеют прямой доступ к базе данных системы. Разрешение на доступ к базе данных системы предоставляется заказчиком в соответствии с внутренними правилами, и эти разрешения не нарушают требований политики информационной безопасности.

Доступ к сервисным и системным данным должен осуществляться только системным администратором.

Для обеспечения безопасности системы следует определить следующие требования:

1. Требования по валидации полей: - Все входные данные, получаемые от пользователей (например, через веб-формы или API), должны проходить проверку на наличие и корректность разрешенных символов и форматов данных в соответствии с определенными правилами исходя из предполагаемого использования поля. Это включает, но не ограничивается, предотвращением вставки вредоносного кода, такого как SQL-инъекции или скрипты для межсайтового скриптинга (XSS).

2. Требования к периоду бездействия: - Сеанс пользователя должен автоматически завершаться через определенное время бездействия пользователя. Рекомендуемое время бездействия для завершения сеанса составляет **3 минут**, после чего пользователь будет выведен из системы и должен будет выполнить повторный вход. Это мероприятие направлено на предотвращение несанкционированного доступа к аккаунту пользователя в случае, если пользователь оставил сеанс открытым без надлежащей защиты.

3. Требования по ограничению размера прикрепляемых файлов: - Максимально допустимый размер файлов, которые пользователь может загружать в систему, должен быть ограничен до 100 мегабайтах для каждого файла. Все загружаемые файлы должны проверяться на вирусы и другие вредоносные программы перед сохранением в системе. Это помогает предотвратить атаки на переполнение буфера и обеспечивает надлежащую производительность системы при обработке загружаемых данных.

Платформа должна соответствовать требованиям законодательства Узбекистана в области защиты персональных данных в объеме, указанном в настоящем техническом задании.

4.1.6.1 Требования к правам на использование системы

Для управления правами доступа к информации внутри системы система должна соответствовать следующим требованиям:

- возможность пользователей системы ограничивать свой доступ в зависимости от уровня информации и данных, необходимых им для выполнения своих задач, который настраивается только системным администратором;
- Возможность организации доступа к программному обеспечению по защищенному каналу;
- Возможность назначать пользователям определенные роли и ограничивать доступ к информации в зависимости от роли;
- Запретить пользователям доступ к информации, которую они не должны иметь возможности использовать в соответствии с назначенной им ролью или индивидуально назначенным доступом;
- Возможность предоставлять доступ к аналитической информации в соответствии с уровнем роли пользователя;
- Доступ к серверу базы данных должны иметь только ответственное лицо (администратор базы данных) и приложения, отвечающие за функционирование комплекса, взаимодействующего с базой данных.

В системе должен быть реализован механизм безопасности и защиты информации, основанный на следующих основных принципах:

- ограничение доступа к программному обеспечению на основе идентификации пользователя;
- ограничение доступа к программным объектам;
- защита каналов транспортной подсистемы программного обеспечения;
- Защита от внедрения SQL;
- журнал аудита для выявления несанкционированных действий в системе.

4.1.6.2 Требования к защите от несанкционированного доступа к системе

Обеспечение защиты от несанкционированного доступа к системе должно соответствовать следующим требованиям:

- Защита системы должна обеспечиваться комплексом программно-технических средств и поддерживающих их организационных мер;
- разграничение прав доступа пользователей и системных администраторов должно основываться на принципе "не разрешено значит запрещено";
- защита системы должна быть обеспечена на всех технологических этапах обработки информации и во всех режимах работы, в том числе при проведении ремонтных работ и технического обслуживания.;

- меры программной и аппаратной защиты не должны существенно ухудшать основные функциональные характеристики системы (надежность, производительность, возможность изменения конфигурации).

Безопасность в системе обеспечивается перечисленными ниже мерами:

- Все операции в системе выполняются только авторизованными пользователями;
- Система должна обеспечивать на уровне отдельных пользователей разделение доступа к функционалу системы, разделение ролей пользователей в системе (право вызова операторов и набор прав доступа к определенной информации);
- Взаимодействие между удаленными компонентами системы может осуществляться по зашифрованным каналам связи (VPN и/или HTTPS);
- Схема интерфейса должна иметь право только на вызов интерфейсных операторов, без прямого доступа к информации с правами владельца схемы интерфейса.;
- Аудит изменений, внесенных пользователями в важную информацию, для защиты от риска внутреннего мошенничества (просмотр журнала событий системным администратором. В этом случае администратор не должен иметь возможности вносить изменения в журнал событий);
- Запись действий пользователя. Система должна учитывать следующее:
    1) Введение;
    2) вывод;
    3) Удаление объекта;
    4) Добавление объекта;
    5) изменение объекта;

Все пользователи должны получить разрешение от администратора системы безопасности. Доступ пользователя к системе должен осуществляться в соответствии с его ролью.

Для каждого авторизованного пользователя в системе должны сохраняться следующие данные:

1) имя учетной записи/логин;
2) пароль;
3) Группа пользователей;
4) Личная информация полное имя, должность, телефон, отзыв.

Требования к составу пароля: пароль должен состоять минимум из 8 символов, состоять из заглавных и прописных букв, в дополнение к буквам, состоять из цифр и символов. Символы, введенные при доступе, не должны четко отображаться на экране и храниться в зашифрованном виде.

Количество неудачных попыток доступа к системе должно быть ограничено, и если оно будет превышено, система должна быть заблокирована на определенное время.

4.1.6.3 Требования к защите данных

В целях обновления существующего у заказчика комплекса и защиты информации и программного обеспечения от несанкционированного доступа и воздействия вредоносных программ (компьютерных вирусов и вредоносных скриптов) при запуске системы заказчик должен принять организационные, правовые, технические и технологические меры, направленные на предотвращение возможных нарушений. Несанкционированные действия программного обеспечения и те действия, которые были предприняты службой информационной безопасности банка, должны устранить последствия.

Для предотвращения несанкционированного доступа к информационным ресурсам автоматизированной банковской системы должны быть обеспечены следующие требования:

- Защита информации от внешних атак;
- Защита информации от несанкционированного доступа пользователей;
- Обеспечение целостности информации (в процессе хранения, передачи и обработки информации);
- Обеспечение защиты информации, передаваемой между узлами участников системы (Главным банком, региональными и районными филиалами), путем создания закрытого и зашифрованного канала;
- Обеспечение передачи файлов между узлами участников системы путем создания закрытого файлообмена (главный банк, региональные и районные отделения);
- Регистрация и проверка систем безопасности;
- Работа с логами (мейсетевыми экранами (Firewall), обрабатывающими защищенные данные во всех областях) должна осуществляться в удобочитаемом виде;
- Отрасль использование базовых приложений и сервисов в режиме реального времени (онлайн) во время деятельности Республики.

Все системы безопасности должны разрабатываться с учетом требований действующих стандартов и нормативных документов Республики Узбекистан, которые были согласованы между заказчиком и исполнителем до начала разработки.

Информационная безопасность в системе должна достигаться за счет комплексного использования:

- средства защиты информации от несанкционированного доступа к рабочим станциям, серверам и сетевому телекоммуникационному оборудованию;
- мейсетевой экран (брандмауэр);
- средства анализа безопасности, обнаружения и предотвращения атак;
- средства защиты информации от вирусов.
- средства аутентификации и контроля доступа, а также записи действий пользователя.

4.1.6.4 Требования к резервному копированию и восстановлению

Программа резервного копирования должна соответствовать следующим требованиям:

- Обеспечивать возможность копирования только измененных блоков для уменьшения размера передаваемых данных;
- Эффективное использование ресурсов хранилища за счет уменьшения избытка хранимых данных;
- Обеспечение возможности повышения производительности Резервного комплекса за счет масштабирования;
- Поддержка передачи резервных копий через сеть передачи и сеть хранения данных;
- Установка специального программного обеспечения для резервного копирования внутри операционной системы, защищенной физической системой;
- Резервное копирование должно быть настроено администратором базы данных клиента в соответствии с внутренними правилами и вышеуказанными требованиями.

4.1.7 Требования к эргономике и технической эстетике

Платформа должна обеспечивать удобный и понятный интерфейс для работы со всеми представленными функциями, разработанный с учетом современной эргономики и дизайна:

- экранные формы и меню должны иметь простое логическое расположение, пункты меню должны быть сгруппированы в соответствии с их функциональными функциями и информационной тематикой, каждый пункт меню должен соответствовать только одной функции;
- дизайн экранных форм должен быть стандартным и может быть изменен, если проблему невозможно решить с помощью стандартной формы;
- эргономические решения должны быть одинаковыми для всех компонентов и модулей системы;
- пользовательский интерфейс должен способствовать снижению вероятности случайных некорректных действий;
- все каталоги в отдельной подсистеме должны открываться стандартным способом во время работы пользователя;
- системный интерфейс должен обеспечивать отображение на экране только функций, доступных конкретному пользователю;
- системный интерфейс должен обеспечивать визуальное отображение на экране хода длительных процессов обработки.

Система должна запрашивать подтверждение для важных операций, таких как изменение и удаление данных. Пользовательский интерфейс должен содержать информативные описания ошибок. Система должна обеспечивать удобные механизмы, которые устанавливаются для контроля того, когда

пользователь вводит значения полей в соответствии со справочниками/классификаторами:

совместимость с допустимыми значениями;

соответствие значениям справочников и классификаторов.

Все записи в экранных формах, а также сообщения, предоставляемые пользователю (за исключением системных сообщений), должны быть на русском и узбекском языках.

4.1.8 Требования к чистоте патентов и лицензий

Внедрение системы должно осуществляться в соответствии с действующим законодательством.

Для каждой части информационной системы необходимо обеспечить, чтобы не было нарушения существующих документов об исключительном праве третьих лиц.

4.1.9 Требования к стандартизации и унификации

При разработке системы необходимо придерживаться принципа унификации.

Информация, загружаемая, вводимая и обрабатываемая в систему, должна соответствовать основным принципам единообразия, непротиворечивости, одноразового включения, полноты и достоверности информации.

Все сервисы должны работать в инфраструктуре TCP/IP;

Взаимодействие клиентских устройств с серверной частью системы должно осуществляться с использованием стандартных протоколов обмена.

Текущее решение должно обеспечивать функционирование задач, операций и интерфейсов в следующих операционных системах: Windows, mas-OS. Система должна обеспечивать интеграцию с другими системами с необходимыми решениями.

Разрабатываемые документы должны быть представлены в строгом соответствии с нормативными документами Республики Узбекистан.

4.2. Функциональные требования информационной системой

Она характеризуется следующими подсистемами и модулями требований к функциям и задачам, выполняемым информационной системой.

4.2.1 Подсистема "Авторизация и аутентификация пользователей"

Подсистема "аутентификация и авторизация" всех пользователей системы должна выполняться администратором безопасности. Доступ пользователя к системе должен осуществляться в соответствии с его ролью.

Для каждого авторизованного пользователя в системе должно поддерживаться следующее:

1) имя учетной записи/логин;

2) пароль;

3) Группа пользователей;

4) Личная информация полное имя, должность, телефон, отзыв.

Требования к составу пароля: пароль должен состоять минимум из 8 символов, состоять из заглавных и прописных букв, в дополнение к буквам, состоять из цифр и знаков препинания. Символы, введенные при доступе, не должны четко отображаться на экране и храниться в зашифрованном виде.

Количество неудачных попыток доступа к системе должно быть ограничено, и если оно будет превышено, система должна быть заблокирована на определенное время.

4.2.2 Подсистема Администрирование.

Подсистема "администрирование" предназначена для управления пользователями.

Подсистема администрирования включает в себя следующие функции:

- управление учетными записями, контроль персонала, включая удаление из системы сотрудников, покинувших организацию;
- управление ролями пользователей для гибкой настройки информации, которую должны видеть сотрудники на разных должностях;
- мониторинг активности пользователей для отслеживания перемещений сотрудников и определения эффективности;
- управление разрешениями пользователей на определенные функции системы для руководителей.

4.2.3 Подсистема "Запись каждого отдельного действия в системе" (Logging).

В аварийных ситуациях или в программном обеспечении, при возникновении ошибок в средствах диагностики, подсистема "запись действий" должна позволять разработчику хранить полный набор информации, необходимой для выявления проблемы (журнал процессов, содержащий информацию о текущем состоянии памяти и о состоянии оперативной). текущее состояние файловой системы), автоматическое ведение журнала аудита, который позволяет отслеживать наиболее важные (уникальные) данные, хранящиеся в базе данных, и записывать все произошедшие события. Оптимально использовать дополнительные программы для регистрации. В этом случае разработчик дает заказчику рекомендации по установке программного обеспечения, самостоятельной установке и эксплуатации заказчиком.

4.2.4. Подсистема «резервное копирование и восстановление данных»

Работа подсистемы "Резервирование" осуществляется в соответствии с установленным графиком резервирования. Описание процедуры резервного копирования и восстановления данных, а также политики восстановления

системы (количество резервных копий, их тип) должны быть в эксплуатационных документах. Подсистема настроена в соответствии с правилами резервирования, принятыми клиентом.

4.2.5. Подсистема «управление взаимодействием с внешними информационными системами»

Подсистема "Интеграция" для осуществления интеграции со сторонними системами.

Подсистема "интеграция" включает в себя следующие функции:

настройка параметров интеграции для взаимодействия со сторонними ресурсами.

Должна быть предусмотрена возможность внесения дополнений в информационную систему в режиме постоянной наглядности. Кроме того, необходимо обеспечить возможность повышения производительности системы за счет ее масштабирования.

Она должна быть спроектирована таким образом, чтобы можно было увеличить функциональность информационной системы. Для повышения эффективности платформы и удовлетворения потребностей пользователей функциональность системы расширена. Модернизация и развитие системы должны осуществляться с учетом факторов, обеспечивающих их экономическую целесообразность.

Должна быть предусмотрена возможность переноса системы на новый сервер без изменения программного кода.

4.2.6 Подсистема идентификации и аутентификации клиентов: физических/ юридических лиц

Подсистема идентификации и аутентификации клиентов: физических и юридических лиц обеспечаеть онлайн идентификации клиентов или субъектов. С этим выполняются различных технологий и методов и берёт данных из разлицних государственных серверов (Государственного центра персонализации-ГЦП, единая база предпринимателей Узбекистан-ЕБП, и т.д.). Эти данные отражается в анкетах клиентов и предотвращает мошенничества.

4.2.7 Подсистема «управление Списками»

Этот модуль обеспечивает ежедневное формирование и обновление списка. Список формируется и обновляется следующим образом:

Загрузка и ежедневное автоматическое обновление бесплатных списков (OFAC, EU, UN, UK и так далее)

Возможность загружать и ежедневно автоматически обновлять платные списки (Dow Jones, LexisNexis, Refinitiv и прочие)

Возможность загружать и ежедневно автоматически обновлять региональные (локальные) и собственные списки.

4.2.8 Блок скрининга транзакций (санкции и товары двойного назначения)

С помощью этого модуля предусмотрено сопоставление операций клиентов банка с санкциями и товаром двойного назначения и установление контроля над ними как мониторинг и проверка физических и юридических лиц и их операции с списками санкций и расчет уровня риска. В этом:

- Возможность работать с разными стандартными форматами (MT, MX, ISO20022)
- Целевая скорость проверки и ответа – 1 секунда
- Наличие собственного пользовательского интерфейса для обработки алертов
- Лицензирование блока предусматривает неограниченное количество пользователей
- Возможность интеграции с внешней системой
- Наличие встроенного интерфейса с почтовым сервером (нотификация по ошибкам, алертам, отправка информации о принятом решении по алерту)
- Гибкая система настройки параметров проверки без необходимости программирования (NO CODE/LOW CODE), включая fuzzy логику Дамерау-Левенштейна, различные настройки проверки для минимизации ложных срабатываний
- Наличие примеров работы блока не менее, чем в 20 банках из разных стран
- Наличие примера работы блока при ежедневном скрининге 1 млн транзакций
- Наличие примера работы блока при скрининге транзакций в процессе обработке моментального платежа (instant payment).

4.2.9 Мониторинга транзакций (AML сценарии и анализ связей)

Из этого модуля следует, что банк будет в значительной степени сравнивать стандарты сомнительных транзакций клиентов и определять их. Так как с помышу с этой модуля можно будет составыть отчетов по формам сообщений, отправляемых в компетентные государственные органы. Этот модуль должен включать:

- Наличие собственного пользовательского интерфейса для обработки алертов
- Лицензирование блока предусматривает неограниченное количество пользователей
- Возможность интеграции с внешней системой – передача алертов на обработку (на выбор – всех или частично, только для случаев расследования)
- Наличие встроенного интерфейса с почтовым сервером (нотификация по ошибкам, алертам, отправка информации о принятом решении по алерту)
- Наличие механизма ежедневного пересчета уровня риска клиентов (вся база клиентов ежедневно)

- Возможность настройки нескольких моделей риск-скоринга в зависимости от типа/категории клиента
- Гибкая система настройки сценариев поведенческого анализа и моделей риск-скоринга без необходимости программирования (NO CODE/LOW CODE)
- Возможность в производственной среде настроить новый сценарий, не включать алерт, а только видеть статистику возможных алертов на реальных данных
- Линк – анализ: на основании всего массива транзакций за устанавливаемый период времени видеть связи между клиентами с возможностью фильтрации (установка периода времени, сумм и т.п.) – графическая визуализация с указанием направлений денежного потока, сумм, наименований корреспондентов, с возможностью погрузиться в детали
- Наличие примеров работы блока не менее, чем в 20 банках из разных стран
- Наличие примеров работы блока при ежедневном анализе 200 млн. транзакций (объем всех транзакций последних 12 месяцев).

4.2.10 Единое рабочее место для специалиста соответствия

Единое рабочее место для специалиста соответствия это сбор информации, обработка документов, процессы, управление коммуникациями, управление расследованиями, управление достоверностью документов и включает в себя следующее:

1. Коммуникационная панель
2. Панель уведомлений
3. Панель помощи
4. Панель настроек
5. Регистры
6. Управление профилем юридических и физических лиц
7. Управление процессами (риск-кейсами)
8. Управление документами
9. Управление связями владельцев и выгодополучателей
10. Управление связями между лицами, холдинги
11. Управление инцидентами
12. Управление анкетами
13. Управление заданиями
14. Управление расчетами уровня риска
15. Управление моделями риск
16. Управление регистром товаров двойного назначения
17. Управление справочником TARIC
18. Управление списками
19. Проверка по санкционным спискам
20. Управление бизнес правилами
21. Встроенная почта

22. Внутренние публикации
23. Управление правами пользователей
24. Управление замещениями
25. Управление оповещениями
26. Управление изменениями, в том числе ошибками
27. Функция поиска
28. Изменения процессов, форм

4.2.10.1. Коммуникационная панель

Коммуникационная панель – дополнительная область, доступная в любом режиме работы пользователя (например, пользователь работает с карточкой клиента или с расследованием, или с регистром), с возможностью легко скрыть/минимизировать панель с целью расширения основной рабочей области пользователя:

- Лента опубликованных внутренних оперативных публикаций, с возможностью оставить комментарий и отметить как понравившееся.
- Лента телефонных звонков с возможностью инициировать новый звонок (при наличии интеграции с телефонной станцией), с возможностью сохранить звонок при выбранном объекте системы (например, при клиенте, персоне, при отдельном расследовании)
- Лента электронных писем (входящих, исходящих, черновики), с возможностью фильтрации, с возможностью связать выделенное письмо с любым объектом системы (например, с другим письмом, с клиентом, с персоной, с расследованием, с заданием, с документом и т.д.), с возможностью инициировать новое письмо в интерфейсе самой системы.

4.2.10.2. Панель уведомлений

Панель уведомлений – дополнительная область, доступная в любом режиме работы пользователя (например, пользователь работает с карточкой клиента или с расследованием или с регистром), с возможностью легко скрыть/минимизировать с целью расширения основной рабочей области пользователя:

- Оперативные напоминания
- Уведомления ленты (внутренние публикации)
- Ожидание визирования/авторизации
- События календаря (например, день рождение персоны)
- Служебные сообщения
- Задачи по бизнес-процессам (индивидуальные и групповые)

4.2.10.3. Панель помощи

Панель помощи – возможность перейти в базу знаний и возможность написать обращение в службу поддержки

4.2.10.4. Панель настроек

Панель настроек – возможность перейти в режим настроек.

4.2.10.5. Регистры

Регистры – наличие отдельных регистров с возможностью средствами настройки (без программирования) создавать новые регистры, менять содержание регистра (добавлять колонки, менять порядок и размерность колонок).

- Регистр юридических лиц (клиенты и не клиенты)
- Регистр физических лиц (клиенты и не клиенты)
- Регистр связей владельцев и выгодополучателей
- Регистр анкет клиентов
- Регистр документов (ID, доверенности, договоры, уставы)
- Регистр инцидентов
- Регистр процессов (риск-кейсов)
- Регистр заданий
- Регистр осуществленных расчетов уровня риска
- Регистр моделей риск-скоринга
- Регистр товаров двойного назначения
- Регистр TARIC номенклатуры
- Регистр применяемых списков санкций
- Регистр настроенных бизнес правил, оповещений
- В рамках каждого отдельного регистра иметь возможность средствами настройки (без программирования, NO CODE/LOW CODE) обеспечить индивидуальные для каждого пользователя динамические группы регистра (например, в регистре лиц сделать группы резидентов и нерезидентов, группы по типу, по статусу, по возрасту и т.д.). При изменении какого-либо признака объекта регистра, формирующего группу (например, возраст лица), объект автоматически должен перейти в соответствующую группу (соответствующую возрастную группу)
- Возможность сортировки по каждой колонке регистра
- Возможность создания пользователем фильтра в рамках отдельного регистра по одному или нескольким параметрам на выбор пользователя.

4.2.10.6. Управление профилем юридических и физических лиц

Управление профилем юридических и физических лиц – возможность из регистра юридических или физических лиц, посредством установленного фильтра или средствами поиска найти лицо и открыть его карточку/досье,

Карточка/досье должна содержать 360°-профиль соответствия лица, всю необходимую информацию, анкеты, документы и оценки уровней рисков и т.д., включая историю изменения информации и оценок

Иметь возможность нажатием кнопки сформировать отчет, который должен содержать структурированный 360°-профиль соответствия отдельного лица

Карточка лица должна содержать всю необходимую информацию (набор информации должен быть параметризирован в зависимости от типа и статуса лица, например набор требуемой информации может отличаться для юридического и физического лица, является ли лицо клиентом или нет):

- Синхронизированные данные с мастер-системой – наименование, регистрационный номер, адрес
- альтернативные адреса
- налоговая резиденция
- сегментация
- классификация деятельности
- установленные запреты
- риск факторы
- связанные страны
- связанные персоны и предприятия
- анкета, включая историю ее изменений
- владельцы и выгодополучатели (в случае юридического лица)
- уровень риска, включая его изменение
- связанные документы
- связанные расследования
- финансовые показатели (полученные из учетной системы)
- связанные задания, письма, чаты, заявления
- и т.д.

Карточка лица должна содержать раздел истории, где есть возможность просмотреть или добавить действия, связанные с лицом, например, задания, электронные письма, заявки, предложения.

Карточка лица должна содержать раздел вложений и примечаний, где видны уже сохраненные вложения и примечания, а также есть возможность добавить вложение к профилю в неструктурированном виде или добавить примечания в формате html-поля.

Карточка лица должна содержать раздел аудита, который содержит информацию обо всех изменениях, внесенных в профиль лица

Карточка лица должна содержать раздел оперативных публикаций (feed), в котором видна история проведенных внутренних публикаций (обсуждений) по данному лицу, а также есть возможность организовать новую публикацию (новое внутреннее обсуждение)

Возможность менять карточку лица средствами настройки (без программирования, NO CODE/LOW CODE) – внешний вид, порядок полей, названия полей, добавлять новые поля

Желательно, чтобы адрес лица можно было верифицировать и визуализировать на карте через интерфейс системы

Иметь возможность заблокировать клиента в интерфейсе системы (требуется соответствующая интеграция с учетной системой)

4.2.10.7. Управление процессами (риск-кейсами)

Управление процессами (риск-кейсами) – возможность из регистра риск-кейсов, посредством установленного фильтра или средствами поиска найти процесс и открыть его

В системе должны уже содержаться модельные процессы (риск-кейсы):

- онбординг клиента
- проверка клиента (CDD)
- расширенная проверка (EDD)
- согласование изменения клиентского файла (структуры, выгодополучателя, представителя, доверенности, анкеты)
- расследование алерта (скрининг имен)
- расследование алерта (скрининг транзакций)
- расследование алерта (мониторинг транзакций)
- проверка сделки (товары двойного назначения)
- запрос третьей стороны (контрагент)
- запрос третьей стороны (надзорная институция)
- блокирование клиента

Иметь возможность вручную инициировать процесс из предложенного списка процессов (риск-кейсов)

Возможность инициации нового процесса автоматически при срабатывании настроенного бизнес-правила (условия, отслеживаемого системой), например, оборот клиента достиг 1 млн. евро – инициировать процесс проверки клиенте, или у клиента изменился риск рейтинг на «очень высокий» инициировать процесс расширенной проверки

Возможность инициации нового процесса расследования алерта автоматически при поступлении информации об алерте из внешних систем

Возможность на каждом шаге процесса сформировать задание отдельному исполнителю, с автоматическим оповещением исполнителя, чтобы информация об этом задании и его исполнении сохранилась в процессе

Возможность исполнителя шага процесса вернуть процесс на предыдущий шаг с указанием причины возврата

Возможность добавлять новый тип процесса или менять текущий процесс средствами настройки (без программирования, NO CODE/LOW CODE) – добавление шага, изменение шага, исполнитель шага, дополнительные действия при шаге (например, автоматическое оповещение исполнителя по электронной почте)

Возможность настройки предопределенных решений, заданий на определенном шаге процесса (когда пользователь не может сам выдумать задание и исполнителя, но выбрать из настроенного списка)

Возможность настроить время исполнения отдельного шага и время исполнения всего процесса и иметь возможность видеть просроченные шаги и процессы

Возможность настроить чек-листы на шаге процесса и установить обязательность прохождения чек-листа (например, не позволять переходить на следующий шаг процесса, пока не пройден чек-лист данного шага).

4.2.10.8. Управление документами

Управление документами – возможность из регистра документов, посредством установленного фильтра или средствами поиска найти карточку документа и сам документ и открыть его

Иметь возможность зарегистрировать документ (создать карточку с метаданными документа)

Иметь возможность к карточке документа присоединить имидж документа

Иметь возможность контролировать ключевые метаданные документа и настраивать бизнес правила по формированию напоминания либо по инициации процесса или задания (например, оповещение о всех идентификационных документах, срок действия которых заканчивается в течение ближайших 30 дней, или создать задание по получению нового идентификационного документа)

Иметь возможность поиска документа в системе по метаданным карточки документа

Иметь возможность поиска документа в системе по содержанию документа

Иметь возможность установить связь одного отдельного документа с различными объектами системы (клиентом, другим документом, расследованием). Тогда информация об этом документе и ссылка на этот документ должна быть видна у всех связанных объектов (например, один и тот же договор относится к двум клиентам, т.к. это договор между ними, документ зарегистрирован один, но он через установленную связь виден у обоих клиентов)

Возможность менять карточку документа средствами настройки (без программирования, NO CODE/LOW CODE) – внешний вид, порядок полей, названия полей, добавлять новые поля.

4.2.10.9. Управление связями владельцев и выгодополучателей

Управление связями владельцев и выгодополучателей – возможность из регистра связей владельцев и выгодополучателей посредством установленного фильтра или средствами поиска найти карточку связи и открыть ее:

- Возможность указания типа выгодополучателя с указанием доли владения и основания владения
- Возможность деактивации связи с фиксацией времени и исполнителя (в том числе по причине ошибочно созданной связи)

- Возможность менять карточку связи средствами настройки (без программирования, NO CODE/LOW CODE) – внешний вид, порядок полей, названия полей, добавлять новые поля.

4.2.10.10. Управление связями между лицами, холдинги

Управление связями между лицами, холдинги – возможность зарегистрировать связь между лицами заранее предопределенного типа

- Возможность деактивации связи с фиксацией времени и исполнителя (в том числе по причине ошибочно созданной связи)
- Возможность добавлять новый тип связи средствами настройки (без программирования, NO CODE/LOW CODE), а также посредством настройки определять, влияет данный тип связи на образование холдинга или нет
- Связи между лицами должны быть видны в соответствующих карточках/профилях лиц и должны формировать холдинг (по связям, влияющим на построение холдинга)
- Должно быть видно, через сколько уровней связей связаны лица (например, лицо А связано с лицом В, которое связано с лицом С, которое связано с лицом D, таким образом лицо А связано с лицом D связями третьего уровня)
- Можно предопределить и настроить (без программирования), сколько уровней связей образуют холдинг связанных лиц
- Если два лица входят в два независимых холдинга, то при регистрации связи между этими двумя лицами, у всех участников двух холдингов должна автоматически изменится информация о связях и они должны сформировать единый холдинг. При деактивации этой связи автоматически изменится информация о связях и холдинг должен разделиться на два.

4.2.10.11. Управление инцидентами

Управление инцидентами – возможность из регистра инцидентов посредством установленного фильтра или средствами поиска найти инциденг и открыть его:

- Возможность ручной регистрации инцидента
- Возможность инициации нового инцидента автоматически при поступлении информации об алерте из внешних систем
- Иметь возможность автоматической регистрации нового инцидента на основе письма, присланного на специально выделенный для этого адрес электронной почты
- Возможность загрузки инцидентов из внешних источников
- Возможность менять карточку инцидента средствами настройки (без программирования, NO CODE/LOW CODE) – внешний вид, порядок полей, названия полей, добавлять новые поля

4.2.10.12. Управление анкетами

Управление анкетами – возможность из регистра анкет посредством установленного фильтра или средствами поиска найти определенную анкету и открыть ее:

- Возможность создания различных типов анкет для разного типа клиентов
- Контроль версионности анкет, возможность определить, какие версии анкет были актуальными на определенную дату
- История обновления анкет для каждого клиента
- Обеспечение механизма напоминания о необходимости обновления анкеты для каждого отдельного клиента
- Возможность создания новой версии анкеты средствами настройки (без программирования, NO CODE/LOW CODE) – внешний вид, порядок полей, названия полей, добавлять новые поля.

4.2.10.13. Управление заданиями

Управление заданиями – возможность из регистра заданий посредством установленного фильтра или средствами поиска найти определенное задание и открыть его

- Возможность инициации нового задания из любого шага процесса, из любого объекта системы (клиент, документ, анкета и т.д.). Помимо автоматического попадания в регистр заданий, данное задание должно сохраниться при шаге процесса или объекте, при котором оно было инициировано
- Возможность инициации задания на группу исполнителей
- Возможность автоматической нотификации исполнителя задания посредством электронной почты с линком на само задание
- Возможность конфигурации карточки задания средствами настройки (без программирования, NO CODE/LOW CODE) – внешний вид, порядок полей, названия полей, добавлять новые поля.

4.2.10.14. Управление расчетами уровня риска

Управление расчетами уровня риска – возможность из регистра расчетов уровня рисков посредством установленного фильтра или средствами поиска найти определенный расчет или серию расчетов по определенному клиенту и открыть отдельный расчет

Обеспечивать начальный расчет уровня риска клиента в процессе онбординга нового клиента

Возможность конфигурации карточки расчета уровня риска средствами настройки (без программирования, NO CODE/LOW CODE) – внешний вид, порядок полей, названия полей, добавлять новые поля.

4.2.10.15. Управление моделями риск скоринга

Управление моделями риск скоринга – возможность из регистра моделей риск скоринга посредством установленного фильтра или средствами поиска найти определенную модель и открыть ее. Возможность конфигурации создания новой модели или модернизации текущей модели средствами настройки (без программирования, NO CODE/LOW CODE).

4.2.10.16. Управление регистром товаров двойного назначения

Управление регистром товаров двойного назначения – возможность ввести (загрузить) список товаров двойного назначения, иметь возможность проверки в ручном режиме по коду товара или по наименованию товара выявить, входит ли товар в список товаров двойного назначения.

4.2.10.17. Управление справочником TARIC

Управление справочником TARIC – возможность ввести (загрузить) справочник TARIC кодов, иметь возможность проверки в ручном режиме по TARIC коду товара выявить, входит ли товар в список товаров двойного назначения.

4.2.10.18. Управление списками

Управление списками – иметь возможность видеть полный регистр применяемых списков (санкционных, региональных и собственных), обеспечить обновление списков в соответствии с разделом 4.2.6.

4.2.10.19. Проверка по санкционным спискам

Проверка по санкционным спискам – обеспечить возможность начальной проверки нового клиента по спискам, в дополнении к разделу 4.2.7, который регулирует регулярную ежедневную проверку всей базы клиентов и связанных с ними персон

Иметь возможность вручную проверить отдельное лицо (физическое или юридическое лицо) на наличие его в списках

Начальная проверка нового клиента по спискам должна быть автоматической частью электронного процесса онбординга нового клиента, упомянутого в разделе 4.2.10.7.

Гибкая система настройки параметров проверки без необходимости программирования (NO CODE/LOW CODE), включая fuzzy логику Дамерау-Левенштейна, различные настройки проверки для минимизации ложных срабатываний.

4.2.10.20. Управление бизнес правилами

Управление бизнес правилами – возможность из регистра бизнес правил посредством установленного фильтра или средствами поиска найти определенное правило и открыть его

Возможность настройки бизнес правила средствами настройки (без программирования, NO CODE/LOW CODE) по определенному условию или комбинации условий, содержащихся в системе автоматически инициировать какое-либо оповещение, задание, действие или процесс (например, оповещение о всех идентификационных документах, срок действия которых заканчивается в течение ближайших 30 дней, или создать задание по получению нового идентификационного документа), другой пример: оборот клиента в месяц составил 100 тыс. Доллар США – автоматически инициировать процесс (риск-кейс) EDD по данному клиенту).

4.2.10.21. Встроенная почта

Обеспечить не замену почтового клиента, но дублирование писем (входящие, исходящие, черновики) из подключенных почтовых ящиков (может быть несколько).

- отображение писем в ленте (смотреть требование 4.2.10.1.).
- удаление письма из ленты не должно вести к удалению письма на почтовом сервере (т.е. не предусматривается управление почтовым сервером).
- возможность связать выделенное письмо из ленты с любым объектом системы (например, с другим письмом, с клиентом, с персоной, с расследованием, с заданием, с документом и т.д.). При открытии объекта должны быть видны связанные с ним электронные письма
- возможность отправить письмо из любого объекта системы (например, из карточки клиента, персоны, расследования, задания, документа и т.д.). Тогда письмо должно быть автоматически связано с объектом и должно быть видно при объекте.

4.2.10.22. Внутренние публикации

Внутренние публикации – иметь возможность пользователю системы сделать публикацию или открыть обсуждение по любому объекту в системе (клиент, документ, процесс), с линком на данный объект, определить круг участников, автоматически данная публикация (обсуждение) должна сохранится при данном объекте, если публикация (обсуждение) была инициирована из ленты публикаций, иметь возможность сохранить эту публикацию (обсуждение) при определенном объекте.

4.2.10.23. Управление правами пользователей

Управление правами пользователей – иметь возможность настройки профилей пользователей с конфигурацией доступа в рамках отдельного профиля вплоть до отдельного поля системы.

4.2.10.24. Управление замещениями

Управление замещениями – иметь возможность ручного перенаправления заданий и процессов одного работника – другому работнику. В случае интеграции с системой учета персонала, иметь возможность автоматически направлять

задания и процессы его заместителю в первый день начала отсутствия (согласно данным системы учета персонала) и автоматически возвращать невыполненное по завершению отсутствия (согласно данным системы учета персонала).

4.2.10.25. Управление оповещениями

Управление оповещениями – иметь возможность посредством настройки системы (без программирования, NO CODE/LOW CODE) настраивать оповещения на как самому себе, так и другим исполнителям шага процесса или задания как внутри системы (панель оповещений), так и посредством отправки электронного письма.

4.2.10.26. Управление изменениями, в том числе ошибками

Управление изменениями, в том числе ошибками – предусмотреть три основных режима работы с объектами (чтение, редактирование, удаление). Для некоторых объектов предусмотреть невозможность удаления (например, связи между клиентами или персонами, влияющие на расчет уровня риска, поведенческий анализ и принятие решения в момент времени) – для таких критически важных объектов предусмотреть возможность деактивации с указанием причины (в том числе причиной может быть «ошибочно создано»).

4.2.10.27. Функция поиска

Функция поиска – иметь возможность глобального поиска по метаданным, содержащимся в системе, и по содержанию вложений (например, поиск фразы в текстах по всей базе приложенных документов).

4.2.10.28. Изменения процессов, форм

Изменения процессов, форм иметь возможность посредством настройки системы (без программирования, NO CODE/LOW CODE) настраивать новые процессы и формы ввода, менять текущие процессы и формы ввода.

4.3. Требования к обеспечениям

4.3.1 Требования к обеспечению достоверности данных

Состав, структура и методы организации информации в системе должны быть определены на этапе изучения проекта.

Уровень хранения данных в системе должен быть построен на основе системы управления базами данных (СУБД).

Для обеспечения целостности системных данных необходимо использовать встроенные механизмы СУБД.

Атрибутивный состав основных информационных объектов системы, являющихся предметом обмена данными между системой и объединенными системами, должен включать идентификаторы, позволяющие идентифицировать соответствующие информационные объекты в Объединенных системах. Правила кодирования записей в системных каталогах должны соответствовать

действующим формализованным правилам соответствующих каталогов заказчика.

Связанные программные компоненты должны использовать общую объектную модель.

Взаимодействие между уровнем хранения данных (реализованным с помощью СУБД) и уровнем обработки данных в компоненте обработки и хранения данных должно осуществляться с использованием сетевых протоколов стека TSP/IP.

Взаимодействие между клиентским приложением (веб-браузером) и сервером приложений (веб-сервером) должно осуществляться с использованием стандартных протоколов. Требования к характеристикам взаимодействия создаваемой системы с соответствующими информационными системами и требования к взаимодействию с другими связанными информационными системами должны быть определены на этапе предпроектного запроса.

Для обеспечения сохранности информации в аварийных случаях должны быть разработаны правила организации автоматического и ручного резервного копирования данных с использованием инструментов СУБД. Правила разрабатываются администраторами СУБД в соответствии с внутренними правилами заказчика.

Аппаратные возможности для хранения резервных копий предоставляются заказчиком.

Резервное копирование должно выполняться в соответствии с установленным графиком резервного копирования. Описание процедуры резервного копирования и восстановления данных, а также политики восстановления системы (количество резервных копий, их тип) должны содержаться в эксплуатационных документах, подготовленных заказчиком.

4.3.2 Требования к лингвистическому обеспечению

Лингвистическое обеспечение системы должно включать использование единого логического и концептуального интерфейса для пользователей и разработчиков. Включая:

- лингвистическое обеспечение должно быть достаточным для общения пользователей разных категорий с помощью средств автоматизации в удобной для них форме, а также для осуществления процессов преобразования обрабатываемой в системе информации и отображения ее пользователю;
- включать серверное устройство для полной регистрации журналов;
- при разработке и проектировании системы следует использовать инструменты проектирования;
- взаимодействие пользователя с системой должно осуществляться на узбекском или русском языках. Исключения могут включать системные сообщения, которые не зависят от локализации.

Языки управления данными должны соответствовать требованиям стандарта ANSI 1992 (realism SQL) и поддерживать реляционную и объектно-реляционную модели баз данных, а также стандарт jdbs.

4.3.3 Требования к программному обеспечению

Сервер СУБД	
Операцион тизим	Orasle Linux
СУБД	Postgresql ва Adminer
Сервер приложений	
Операцион тизим	Orasle Linux
Сервер приложений	Nginx
Жава	Orasle Java SE 8U202+, OpenJDK 1.8.0_282

Требования к рабочему столу пользователя:

Клиентское рабочее место	
Операцион тизим	Windows 10 и выше
Браузер	Google Chrome x64* Firefox x64* Яндекс Браузер x64* * последние версии

4.3.4 Требования к технической поддержке

Оборудование, необходимое для работы системы, приобретается заказчиком в соответствии с рекомендациями по вычислительной инфраструктуре, предоставленными разработчиком системы.

Набор технических средств системы должен быть достаточным для выполнения всех предусмотренных в ней автоматизированных функций.

Для полноценной работы системы разработчик/подрядчик обязан обеспечить необходимые расчеты вычислительных ресурсов программного обеспечения, в то время как поставка программного обеспечения осуществляется заказчиком.

По результатам обследования разработчик/исполнитель должен предоставить заказчику заключение о требованиях к техническим характеристикам серверов, сетевых и других оборудований. Данные оборудование не может привязана к конкретному производителю, что необходимо для корректной работы программного обеспечение системы, а также должно соответствовать оборудованию заказчика.

Кроме того, разработчик/руководитель должен указать рекомендации по процессам интеграции с существующими информационными системами

(внутренними и внешними), чтобы оптимально интегрировать систему, представленную в завершении, с существующими бизнес-процессами.

Необходимые серверы:

- Промышленный сервер;
- Резервный сервер (рекомендуется);
- Тестовый сервер (рекомендуется);

Промышленный сервер является основным сервером для запуска приложения.

Для соблюдения политики отказоустойчивости рекомендуется иметь резервный сервер с конфигурацией, аналогичной промышленному серверу.

Если настроена отказоустойчивая конфигурация, то в случае сбоев в работе основного сервера приложений сервер приложений переносится на резервный сервер. В режиме ожидания (бездействие системы) принудительная синхронизация между рабочим и резервным серверами происходит каждый час. Переход на резервный сервер осуществляется администратором приложения при возникновении сбоев в работе системы. Однако система не должна гарантировать сохранность незавершенных операций. Система может работать как в обычном режиме с использованием одного сервера приложений, так и в режиме высокой доступности с использованием основного и резервного серверов приложений ("горячий резерв"), что позволяет пользователю продолжать работу без перезапуска приложения. Таким образом, если основной сервер приложений выходит из строя и переключается в режим резервного копирования, возможно потерять часть данных, переданных на сервер, но еще не сохраненных, в то время как данные, не переданные на сервер, сохраняются. Чтобы предотвратить частичную потерю данных, пользователь может подтвердить повторную отправку данных формы.

При установке защищенной от ошибок конфигурации все компоненты информационной системы и конфигурации бизнес-приложений (клиентская часть, серверная часть, базы данных) синхронизируются.

Сервер и тестовый сервер для разработки — это сервер приложений и СУБД, установленные на одном физическом сервере. Сервер программиста используется для улучшения функциональности приложения.

Тестовый сервер предназначен для тестирования программы перед окончательным тестированием поставки на сервер предварительной подготовки. Сервер предварительной подготовки предназначен для окончательного тестирования поставки в конфигурации, аналогичной промышленному стенду. Перед тестированием процесса обновления база данных переносится с рабочего сервера на предварительный сервер и размещается конфигурация приложения, полученная с рабочего сервера. После установки новой версии приложения проверяется корректная работа всех модулей, а также корректность обновления конфигурации (потеря данных после обновления, отсутствие ошибок в конфигурации).

На первом этапе реализации минимальная конфигурация сервера, которая должна быть предоставлена перед началом тестирования системы, приведена в таблице:

Среда	Сервер	Кол-во процессорных ядер, вСПУ	РАМ, Гб	Диски, Гб	ОС
Промышленная	Сервер приложений	4	16	500	SentOS 7
Промышленная	Сервер СУБД	16	128	2048	Orasle Linux

4.3.5 Требования к организационной поддержке

Организационная поддержка системы должна быть достаточной для того, чтобы сотрудники могли эффективно выполнять возложенные на них задачи при выполнении автоматизированных и связанных с ними неавтоматизированных функций. Заказчик обязан определить лиц, ответственных за:

Заказчик утверждает лиц, выполняющих следующие задачи:

- обработка данных в системе;
- управление системой;
- обеспечение информационной безопасности в системе;
- управление персоналом обслуживающих систему.

К работе с системой должны быть допущены сотрудники, обладающие навыками работы на персональном компьютере, знакомые с правилами пользования и прошедшие обучение работе с системой.

Порядок организации деятельности ИС и взаимодействия сотрудников с ИС должен регулироваться инструкциями пользователя и инструкциями по обслуживанию и управлению ИС.

К работе с системой должны быть допущены сотрудники, прошедшие обучение и обладающие навыками работы с системой.

Защита от некорректных действий пользователя достигается за счет изоляции доступа к системе, отображения предупреждающих сообщений и использования обязательных и неотредактированных полей.

4.3.6 Требования к методическому обеспечению

При использовании информационной системы разрабатываются технические инструкции для пользователя в произвольной форме.

5. Состав и содержание работ по созданию информационной системы

Перечень стадий и этапов работ по созданию ИС

№ Этапа	Наименование работ	Срок исполнения		Исполнитель	Результат
		начало	окончание		

1.	Получение требованные параметры сервера и выделить места для “KYC/AML/CFT/SS”.	15.01.2025	01.02.2025	Заказчик	Готовность места для установки ПО
2.	Установка программы “KYC/AML/CFT/SS”	01.02.2025	01.10.2025	Разработчик	Готовность для испытательние ПО
3.	Проведение испытательных работ программы.	01.10.2025	01.12.2025	Заказчик и Разработчик	Выявление и устранение ошибок и недостатки
4.	Установка программ в боявом режиме.	01.12.2025	01.01.2026	Разработчик	Готовность для использование и изучение
5.	Проведение обучения ПО для сотрудников.	01.01.2026	01.03.2026	Разработчик	Готовность сотрудников для использование ПО
6.	Оформления акта о запуске программы.	01.03.2026	15.03.2026	Заказчик	Акт выпольненных работ
7.	Подготовка заключительного отчета по завершению проекта	15.03.2026	31.03.2026	Разработчик	Отчет о завершение проекта
8.	Осуществление окончательной оплаты в соответствии с условиями договора.	01.04.2026	15.04.2026	Заказчик	Окончательная оплата

6. Порядок контроля и приемки информационной системы

Контроль, тестирование и приемка системы должны проводиться на основе O‘z DSt 1987:2018, согласно которому предписываются следующие основные виды испытаний:

1) предварительный;

2) испытательные операции;

3) приемочный.

Предварительные эксплуатации должны проводиться после исправления и тестирования программного обеспечение разработчиком, в том числе получение и ознакомления заказчиком необходымых перечень соответствующих документов о готовности ИС к тестированию предварительной эксплуатации.

Тестирование ИС проводится для определения соответствие функциянирование системы поставленным задачам со стороны заказчика.

Приемо-сдаточные испытания системы проводятся с целью определения ее соответствия техническим условиям, оценки качества тестирования и принятия решения о возможности ее допуска к постоянной эксплуатации.

При тестировании системы проверяется следующее:

1) качество выполнения автоматических функций комплексом программных и технических средств во всех режимах работы системы в соответствии с техническими условиями;

2) осведомленность сотрудников с документами по пользованию ИС и наличие навыков необходимых для выполнения функций, установленных во всех режимах работы системы в соответствии с техническими условиями;

3) полнота инструкций в документах по руководству ИС с целью использование сотрудников во всех режимах работы системы в соответствии с техническими условиями для выполнения ими своих функций;

4) количественные и (или) качественные описания реализации автоматических и неавтоматизированных функций системы в соответствии с техническими условиями;

5) другие возможности системы в соответствии с техническим заданием.

Критерии оценки достижения целей создания системы определяются функциональностью системы, реализованной в рамках данного проекта.

В результате предварительных испытаний, испытательных операций и приемочных испытаний состовляются подробный отчет о проведенных испытаний. В случае получение положительных результаттов от испытательных операций, так же при экспуатации ИС отсутствуют отклонения или их нефункциональный характер, допускается не проводить приемочные испытания или проводить их в сокращенном объеме в соответствии с параметрами, выбранными на усмотрение специалистов. Вышеуказанные отчеты о положительных результатах проведение предварительных испытаний и испытательных операций являются основанием для удтверждение актов приема обращений на соответствующем этапе внедрения системы.

Приемка выполненных работ и запуск системы должны осуществляться специальной комиссией заказчика с обязательным участием исполнителя.

Для того, чтобы система была принята комиссией, необходимо сформировать и провести тестовое исвытание системы.

Проводятся приемочные испытания, чтобы определить, соответствие системы данной спецификации.

Тестирование системы проводится на объекте создателя системы.

По результатам своей работы комиссия составляет акт приемки выполненных работ, который подписывается всеми членами комиссии и передается заказчику на удтверждение, в противном случае должны быть составлены протоколы испытаний, в которых указаны замечания и сроки их устранения.

Перед полным развертыванием необходимо оценить соответствие системы требованиям информационной и кибербезопасности.

7. Требования к содержанию работ по подготовке к запуску информационной системы

В процессе реализации проекта на объекте автоматизации необходимо подготовиться к запуску системы. При подготовке к запуску заказчик должен обеспечить выполнение следующих работ:

- удтвердить список подразделений и ответственных лиц, ответственного за внедрение и проведение тестовой эксплуатации;
- обеспечение доступности пользователей для обучения работе с системой;
- обеспечение соответствия помещений и рабочих мест пользователей к системы требованиям;
- обеспечение выполнения требований к программному обеспечению и техническим средствам, на которые должна быть размещена/установлена данная информационная система;
- подготовка плана размещения/установка системы на своих технических средствах совместно с разработчиком системы;
- проведение тестовых операций.

Требования к составу и содержанию работ по подготовке объекта автоматизации к запуску системы, включая основные виды деятельности и перечень персонала тех, кто их выполняет, должны быть определены на этапе подготовки рабочих документов и по результатам тестирования.

В течение периода запуска системы должен подготовить инструкции по руководству системы и провести обучение персонала заказчика работе с системой.

Разработчик/подрядчик должен провести обучение персонала заказчика.

Проектная группа должна подготовить подробный план перехода к коммерческому использованию на стадии предпроектных исследований.

7.1. Требования к гарантированной системной поддержке

Срок гарантийного обслуживания должен составлять не менее 12 (3) месяцев с даты ввода в эксплуатацию.

В течение гарантийного срока разработчик/подрядчик несет ответственность за:

- качество работ, выполняемых в рамках внедрения информационной системы;
- сохранение текущей версии программного обеспечение;
- техническая помощь/поддержка на узбекском и русском языках;
- консультирование персонала пользователей по использованию и управлению данной информационной системы;
- непрерывная работа информационной системы, за исключением аппаратных сбсев.

В течение гарантийного срока обслуживания разработчик/подрядчик обязан ответить на все вопросы, поставленные ответственнымы сотрудниками заказчика, прошедших обучение, в случве ответы вышеуказанные вопросы непредусмотрены в сопроводительных документах. Список ответственных сотрудников заказчика согласовывается сторонами при заключении договора на техническое обслуживание.

Скорость реагирования на запросы заказчика о технической поддержке системы не должна превышать 48 часов с момента поступления заявки по электронной почте исполнителю и/или подтверждения получения по телефону. В случае возникновения аварийной ситуации в системе разработчик/исполнитель обязан реагировать на запросы заказчика в течение 24 часов с момента получения сообщения от заказчика.

Консультационная помощь ответственного специалиста заказчика осуществляется по телефону или онлайн.

Все дополнительные требования к функционированию, архитектуре базы данных, дизайну, обучению новых пользователей и другие вопросы, не предусмотренные данной технической задачей, могут быть реализованы в рамках данного документа, в случае эти требования не противоречат данной технической спецификации.

8. Требования к оформлению документов

Все документы данного проекта оформляются в соответствие с действующим законодательством Республики Узбекистан. При разработке проектной, рабочей и эксплуатационной документации подрядчик обязан строго руководствоваться нижеследующими государственными стандартами и рекомендациями:

O‘zDSt 1987:2018 Информационные технологии. Типы, полнота и определение документов при создании информационных систем;

Разработчик обязан предоставить полные инструкции по руководству информационной системой для пользователя и технического персонала, а также технологические инструкции по взаимодействию и интеграцию с другими информационными системами;

Содержание всех инструкцией по данной системы должны охватывать подробной информации по конфигурацию и техническому обслуживанию;

В соответствии с O‘zDSt 1987:2018, программа и эксплуатационные документы должны включать в себя:

1) спецификация;

2) характерисика программы;

3) инструкции по установке системы;

4) руководство пользователя;

5) руководство администратора;

6) технологические рекомендации по взаимодействию со сторонними информационными системами;

Все документы должны быть представлены в электронном виде, а также при необходимости на бумажном носителе;

Для проведения испытаний подрядчик обязан предоставить программу и методологию испытаний;

Подготовка этих документов должна быть проведена и согласована с заказчиком;

Подготовленные документы представляются в двух экземплярах на бумажном и электронном носителях.

Представили:

Руководители проекта **Н.Мавланов**

М.Муминова

Ж.Амиров

Э.Джураев

А.Бабаханов

Р.Эргашев

Г.Ражабова

Д. Джуманиязов