ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на создание
Информационной системы электронного апостиля
и электронного реестра заверенных документов
«E-App» и «E-Register»

Оглавление

Введение

Настоящее Техническое задание предназначено для описания состава требований по созданию Информационной системы электронного апостиля и электронного реестра заверенных документов «E-App» и «E-Register» (далее – ИС).

ИС объединяет в себе функционал «E-App» и «E-Register» и рассматривает их в совокупности. ИС имеет единую базу данных по Республике Узбекистан.

1. Общие сведения

1.1. Полное наименование ИС и ее условное обозначение

Полное наименование ИС: Информационная система электронного апостиля и электронного реестра заверенных документов

Короткое название: «E-App» и «E-Register».

Условное обозначение: ИСЭАЭР (далее по тексту - ИС, Система).

1.2. Наименование организаций заказчика и разработчика ИС

Заказчиком ИС является: ПРООН в Узбекистане.

Бенефициаром ИС является Агентсво государственных услуг при Министерстве Республики Узбекистан

Адрес: г. Ташкент, улица А.Темур - 16 А.

Телефоны: 71 207-00-66

E-mail: info@davxizmat.uz

Исполнитель разработки ИС будет определен по результатам тендерных (конкурсных) торгов.

1.3. Перечень документов, на основании которых создается ИС

Перечень документов, на основании которых создается ИС:

- Указ Президента Республики Узбекистан «О мерах по коренному реформированию национальной системы оказания государственных услуг населению» №УП5278 от 12.12.2017г.
- Постановление Президента Республики Узбекистан «О мерах по реализации положений конвенции, отменяющей требование легализации иностранных официальных документов (ГААГА, 5 октября 1961 года) №ПП1566 от 5 июля 2011 года.
- Постановление Кабинета Министров Республики Узбекистан «О дальнейшем совершенствовании процедуры проставления апостиля на официальных документах».

1.4. Плановые сроки начала и окончания работ

Плановые сроки начала и окончания работы по созданию ИС:

Начало – май 2021;

Окончание – сентябрь 2021.

1.5. Порядок оформления и предъявления результатов работ

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

1. O'z DSt 1985:2018 Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем;
2. O'z DSt 1986:2018 Информационная технология. Информационные системы. Стадии создания;
3. O'z DSt 1987:2018 Информационная технология. Техническое задание на создание информационной системы;
4. O'z DSt 1047:2018 Информационная технология. Термины и определения.

Определен следующий состав работ:

1. Разработка Технического задания на ИС;
2. Прохождение экспертизы Технического задания в ГУП «Центр управления проектами электронного правительства» Министерства информационных технологий и коммуникаций Республики Узбекистан;
3. Прохождение экспертизы Технического задания в ГУП «Центр кибербезопасности» при Службе государственной безопасности Республики Узбекистан;
4. Проведение конкурса и заключение Договора на разработку ИС;
5. Разработка программного обеспечения ИС;
6. Тестирование и при необходимости доработка ИС;
7. Составление эксплуатационной документации на ИС;
8. Экспертиза программного продукта на соответствие Техническому заданию в ГУП «Центр управления проектами электронного правительства» Министерства информационных технологий и коммуникаций Республики Узбекистан;
9. Экспертиза программного продукта на соответствие требованиям безопасности в ГУП «Центр кибербезопасности» при Службе государственной безопасности Республики Узбекистан;
10. Проведение тренингов, включая обеспечение технического сопровождения и поддержки разработанного программного обеспечения ИС;
11. Запуск ИС в эксплуатацию. По результатам данного этапа работ Разработчик представляет Заказчику Акт выполненных работ, и подписывается Акт ввода ИС в эксплуатацию.

Этап разработки программного обеспечения будет разбит на шаги по согласованию Заказчика и Исполнителя. Детальный план-график разработки будет приложением к Договору

между Заказчиком и Исполнителем. По результатам каждого этапа разработки Исполнителем и Заказчиком будет подписываться Акт выполненных работ.

Предпочтительно разбивать разработку на функциональные модули в соответствии с перечнем подсистем, приведенным в Разделе 4.1.1. настоящего Технического задания, с указанием сроков разработки каждого этапа. Этапы разработки (подсистемы) будут приниматься Заказчиком последовательно.

1.6. Термины и сокращения

1.6.1. Сокращения

В настоящем Техническом задании использованы следующие сокращения:

АГУ - Агентство государственных услуг при Министерстве юстиции Республики Узбекистан

БДФЛ – База данных физических лиц

БДЮЛ – База данных юридических лиц

ЕПИГУ – Единый портал интерактивных государственных услуг;

ЕСИ - Единая информационная система идентификации пользователей Республики Узбекистан;

ИС - Информационная Система, в настоящем документе используется как обозначение технических и программных средств для реализации функций «E-App» и «E-Register»;

Конвенция - Гаагская конвенция, отменяющая требование легализации иностранных официальных документов, от 5 октября 1961 года;

ПРООН – Программа развития Организации Объединенных Наций;

ТЗ – Техническое задание;

ЭЦП – электронная цифровая подпись.

1.6.2. Термины

В настоящем ТЗ использованы следующие определения:

Апостиль – специальный штамп, проставляемый на официальный документ для использования за границей в соответствии с Конвенцией, подтверждающий подлинность подписи лица, подписавшего документ, и печати или штампа, удостоверяющего документ;

Компетентный государственный орган - Государственный орган, уполномоченный проставить апостиль в соответствии с Постановлением Президента Республики Узбекистан от 5 июля 2011 г. № ПП-1566 «О мерах по реализации положений конвенции, отменяющей требование легализации иностранных официальных документов (ГААГА, 5 октября 1961

года)»;

Модуль – фрагмент разрабатываемой информационной системы, охватывающий набор логически связанных функций.

Персональный кабинет – ресурс, на котором отображается совокупность данных пользователя, где пользователь может отправлять заявления на получение апостиля;

Подсистема – функциональная часть разрабатываемой ИС, включающая в себя модули и некоторые объекты.

Проставление апостиля - официальная процедура, необходимая для подтверждения подлинности подписи лица, подписавшего документ, и подлинности печати или штампа, подтверждающего документ;

Технологическая инструкция - техническая инструкция, описывающая порядок взаимодействия на уровне API (application programming interface) с внешними по отношению к разрабатываемой ИС информационными системами;

«E-App» - программный продукт, который создает специальный электронный штамп на официальном документе в соответствии с Конвенцией, которая подтверждает подлинность подписи лица, выступающего в качестве подписавшего, и подлинность печати или штампа, удостоверяющего документ;

«E-register» - реестр, содержащий перечень документов, утвержденный компетентным государственным органом в установленном законодательством порядке, используемый для проверки данных апостилей.

2. Назначение и цели создания ИС

2.1. Назначение ИС

Назначением ИС является автоматизация процедуры оказания государственных услуг по проставлению специального штампа «Апостиль» на официальных документах, оформленных на территории Республики Узбекистан.

Заявки на получение электронного апостиля принимаются через ЕПИГУ и центры государственных услуг. ИС позволит ввести совершенно новую процедуру апостилирования официальных документов в стране, а также позволит использовать программное обеспечение «E-App» для подачи документов на получение апостиля и «E-register» для проверки подлинности апостилированных документов, содержащихся в реестре, через сеть Интернет.

Создаваемая информационная система позволит создать инструменты для работы с апостилями, выдаваемыми в Республике Узбекистан, посредством использования информационно-коммуникационных технологий.

ИС будет размещена на ресурсах АГУ.

2.2. Цели создания ИС

Целью реализации проекта является:

- Создание единого реестра министерств и ведомств, занимающихся проставлением апостилей (100% регистрация всех поступающих документов в едином реестре);
- Привлечение физических и юридических лиц к получению апостиля в новом формате;
- Повышение качества государственных услуг, сокращение дублирования документов, устранение бюрократических барьеров при получении услуг;
- Сокращение времени проверки апостилей (до 3х дней);
- Получение статистической информации по выдаваемым апостилям (согласно всей информации в БД);
- Контроль за оказанием государственной услуги проставления апостиля;
- Перевод в электронный вид государственной услуги по проставлению апостиля (возможность получения апостиля как в электронном, так и в бумажном виде, с обязательным внесением в реестр);
- Отмена избыточных административных процедур;
- Создание механизма онлайн оплаты государственной услуги проставления апостиля.

Достижение поставленных целей проекта предполагается при использовании единого подхода и стандартов по внедрению информационно-телекоммуникационных технологий в результате решения следующих задач проекта:

- Формирование единой базы данных апостилей и инструментов работы с ней;
- Создание инструментов для подачи документов на получение электронного апостиля;
- Создание инструментов проверки подлинности электронного апостиля (100% сбор в реестре всех заверяемых подписей, печатей и штампов);
- Создание системы взаимодействия участников процесса предоставления услуги получения электронного апостиля (цифровизация обмена информацией между всеми задействованными органами);

- Создание возможностей получения услуги по получению и проверке апостиля посредством ЕПИГУ;
- Создание инструментов получения статистической информации касательно апостилей, выдаваемых в РУз;
- Создание инструментов проведения оплаты за услуги проставления апостиля.

3. Характеристики объекта информатизации

В настоящее время в Республике Узбекистан отсутствуют информационные системы, выполняющие полностью или частично функции выдачи электронного апостиля.

Для получения государственной услуги по проставлению апостиля заявитель обращается в Центр государственных услуг, либо в ответственную организацию с нотариально заверенными копиями и переводами апостилируемых документов для получения апостиля.

Ведомства, ответственные за проставление апостиля:

- Верховный суд;
- Министерство иностранных дел;
- Инспекция по контролю за качеством образования при Кабинете Министров;
- Территориальные управления юстиции;
- Генеральная прокуратура.

Заявитель должен оплатить государственную пошлину за использование услуги, после чего по истечении указанного срока получить готовый апостиль.

Апостиль оформляется путем размещения штампа на документ (либо на нотариально заверенный перевод документа).

Для проверки подлинности апостиля, заинтересованный субъект должен обратиться в соответствующее ведомство для получения сведений об апостиле.

Данный процесс занимает достаточно длительное время как при оформлении, так и при проверке подлинности апостилей. При этом сведения о проставляемых апостилях хранятся в разрозненных нецифровизированных источниках, что усложняет сбор информации, ее обработку и анализ. Процесс взаимодействия между ведомствами также не автоматизирован, что создает сложности в получении своевременных данных.

Разработка информационной системы осуществляется в целях создания единого виртуального пространства для повышения информационного обеспечения населения и заинтересованных сторон, включая зарубежных заинтересованных субъектов.

Автоматизации посредством ИС подлежат процессы:

- Подача документов на получение электронного апостиля;
- Оплата сбора;
- Проверка идентичности подписи, печати и штампа на представленном документе с подписями, печатями и штампами, которые содержатся в базе данных ИС;
- Проверка статуса рассмотрения документов (ответственное ведомство, статус);
- Формирование уникального QR-кода апостиля;
- Получение уведомлений заявителем по готовности апостиля;
- Подписание апостиля с помощью ЭЦП;
- Проверка подлинности апостиля онлайн с использованием QR-кода;
- Просмотр данных апостиля (в формате pdf, с двумя вложениями: перепроверка подлинности, а также непосредственно документа);
- Формирование статистики по апостилям
- Контроль за оказанием государственной услуги проставления апостиля.

ИС подразумевает доступ пользователей к системе в режиме «клиент-сервер», с использованием Web технологий.

4. Общие требования

4.1. Требования к ИС в целом

4.1.1. Требования к структуре и функционированию ИС

В качестве платформы для построения ИС должно использоваться программное обеспечение с открытым исходным кодом.

Проектирование ИС должно базироваться на сервисно-ориентированной архитектуре:

- уровень представления информации;
- уровень прикладной бизнес логики;
- уровень транспортировки сервисов;
- уровень хранения и обработки данных (сервер базы данных).

В ИС должны быть учтены:

- обеспечение безопасности доступа к данным, хранящимся в базе данных ИС;
- организация персонального кабинета пользователя;
- организация жесткого разграничения доступа пользователей к различным функциям в зависимости от их компетенции, занимаемой должности и назначенных им полномочий;

- обеспечение протоколирования на уровне базы данных всех событий, выполняемых посредством функциональных возможностей ИС (логи).

Функционал ИС должен максимально реализовывать поставленные цели, быть масштабируемым и удобочитаемым. ИС должна включать в себя компоненты, описанные в таблице ниже.

4.1.1.1. Перечень модулей ИС, их назначение и основные характеристики

Таблица 1. Перечень подсистем и их назначение.

№	Название	Описание
1.	Модуль авторизации пользователей	Модуль для идентификации пользователей (заявителей) в системе. Предусмотреть авторизацию посредством One-ID для физических лиц, а также посредством использования ЭЦП для юридических лиц. Авторизация должна быть доступна через ЕПИГУ.
2.	Модуль авторизации ведомств	Авторизация ответственных ведомств предназначается для: • Верховного суда; • Министерства иностранных дел; • Инспекции по контролю за качеством образования; • Территориальных управлений юстиции; • генеральной прокуратуры. Также доступ должен быть организован для сотрудников Агентства государственных услуг для приёма заявок, мониторинга за оказанием государственных услуг и контроля работоспособности системы. Авторизация должна осуществляться с использованием ЭЦП по международному стандарту.
3.	Модуль ЭЦП и хранения сигнатур	ЭЦП в разрабатываемой системе должна полностью соответствовать стандарту ITU-T X.509. ЭЦП предназначается для заверения апостилей.
4.	Модуль хранения сигнатур и печатей	Система должна позволять хранить и использовать цифровые и графические сигнатуры (подписи и печати), вести их учет, позволять контролировать сроки их использования в соответствии с регламентом. Также модуль должен позволять сравнивать сигнатуры апостилируемых документов (сканов) и печати, штампы организаций их выдававших, и определять соответствие.

№	Название	Описание
5.	Кабинет пользователя	Предназначен для предоставления пользователю возможности работы с электронными апостилями, включая функции пп.4.1-4.4.
5.1.	Модуль формирования заявки	Формирование заявки на получение Апостиля (один документ или пакет документов)
5.2.	Модуль добавления сканированных версий документов	Добавление сканированных версий документов, а также нотариально заверенных переводов.
5.3.	Модуль проверки статуса заявок	Пользователю должны быть доступны: • Просмотр заявок, находящихся на рассмотрении; • Проверка статуса заявки; • Получение уведомлений по статусам рассмотрения.
5.4.	Модуль выгрузки Апостиля	Пользователю должны быть доступны: • Выгрузка Апостиля и вывод его на печать в формате .pdf. • Просмотр истории заявок и результатов рассмотрения.
6.	Кабинет ведомств	В каждое ведомство должны поступать заявки согласно регламенту рассмотрения.
6.1.	Модуль очереди документов	Модуль предполагает работу с очередью документов на рассмотрение для получения Апостиля.
6.2.	Модуль Досье	В модуле должна быть организована возможность просмотра Досье всех рассматриваемых документов.
6.3.	Модуль Сток	В модуле должна быть возможность просмотра отклоненных заявок.
6.4.	Модуль подписанных документов	Модуль предполагает работу с подписанными документами, включая просмотр, поиск по ним.
6.5.	Модуль поиска	Расширенный поиск по документам, включая возможность фильтрации документов по типам, по утверждающим сотрудникам, по территориальной принадлежности, по дате проставления Апостиля, по фамилии заявителя, по странам отправления и другим возможным параметрам.
6.6.	Модуль мониторинга за оказанием государственных услуг	Данный модуль позволяет сотрудникам АГУ проводить мониторинг за оказанием государственных услуг
6.7.	Модуль статистики	Предусматривается формирование статистических данных по объему заявок, выданных Апостилей, а также в разрезе ведомств, стран/регионов/районов, физических/юридических лиц и др.
7.	Административный модуль	Администрирование системы и управление системными данными осуществляется

№	Название	Описание
		администратором, авторизовавшемся в системе с помощью специального логина и пароля Администратора. Модуль включает в себя: Управление ролями и доступами пользователей; Формирование матрицы доступа; Управление справочниками и классификаторами; Просмотр логов; Мониторинг сервисов; Модуль «Help» для формирования справочных материалов; Модуль уведомлений (для формирования уведомлений пользователям)
8.	Модуль запроса информации об Апостиле	Модуль предназначен для доступа внешних партнеров, заинтересованных лиц для проверки статуса Апостиля (актуальности и валидности) и основных реквизитов выданного апостиля, а также скан-версии документов.
9.	Модуль интеграции	Для интеграции с внешними системами. На первом этапе подразумевается интеграция с ЕПИГУ, ГЦП, МВД, ГНК, ЕСИ и с СМС-шлюзом для отправки уведомлений пользователям, платежными системами.
10.	Модуль проведения оплаты	Оплаты могут осуществляться путем взаимодействия с функционирующими платежными системами в РУз (Click, Payme, Upay, Paynet). Также предусмотреть возможную оплату картами VISA и MasterCard (Для данного взаимодействия должна быть проработана технологическая инструкция с учетом взаимодействия банков разных стран, включая юридические аспекты. Ответственность за утверждение данной технологической инструкции возлагается на Заказчика).

Структурная схема ИС представлена на рисунке ниже.

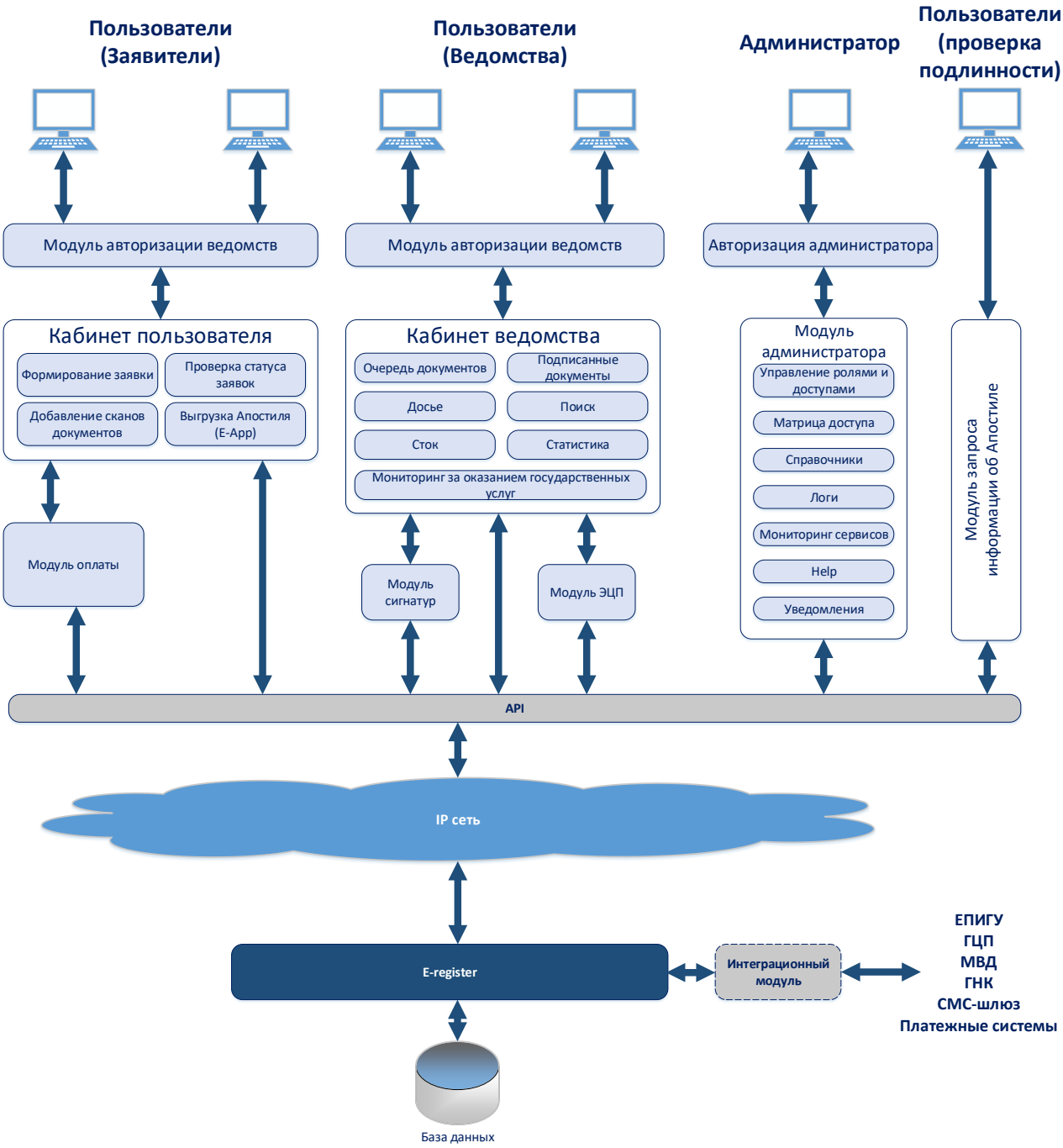
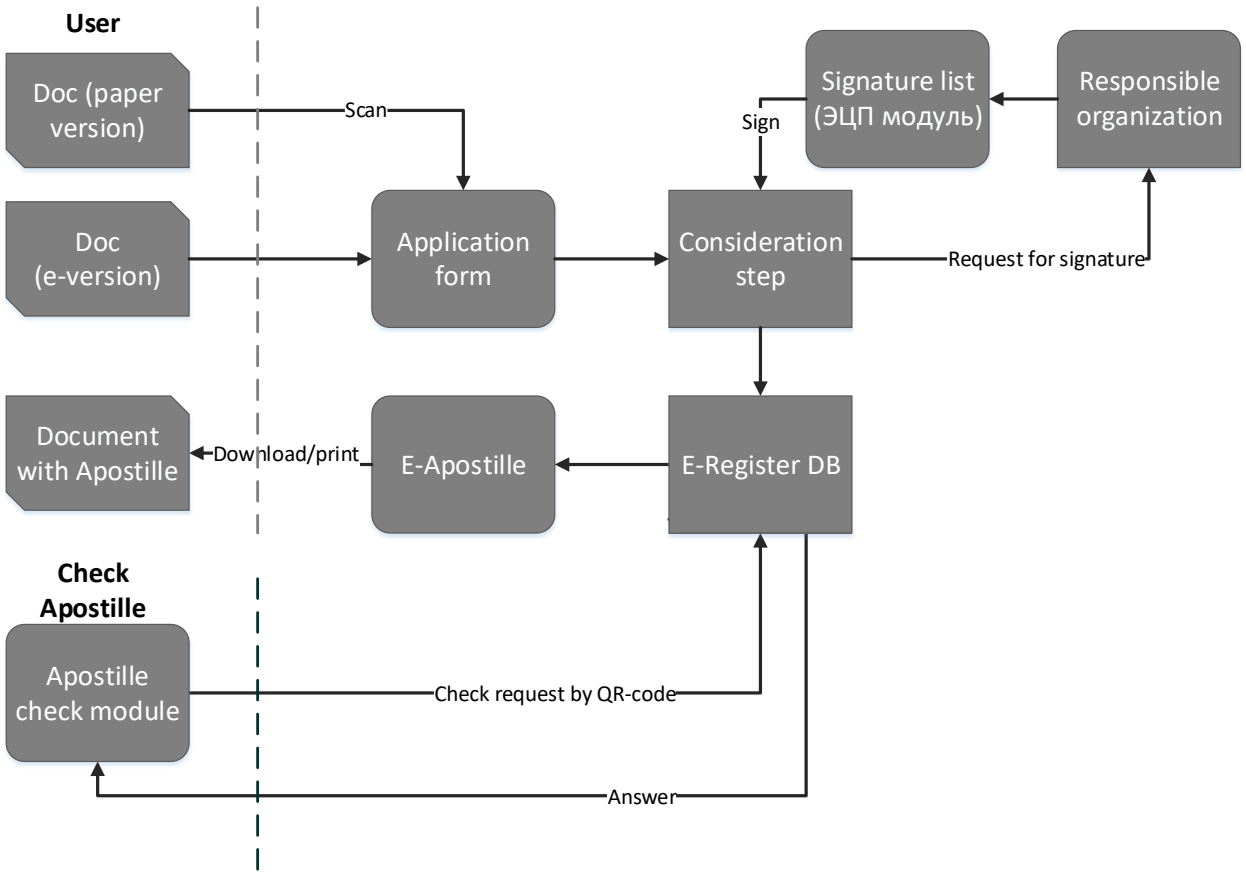


Рисунок 1. Структурная схема ИС.

Логическая схема выдачи электронного апостиля показана на рисунке ниже.



1. Заявитель подает документ (документ в бумажном виде подлежит сканированию, электронный документ будет прикрепляться к заявке и загружаться в систему).
2. Заявитель (физическое или юридическое лицо) заполняет форму заявки в ЕПИГУ.
3. На этапе рассмотрения система отправляет заявку в ответственную организацию согласно Регламенту.
4. Ответственный сотрудник ведомства проверяет документы и ставит утверждающую электронную подпись (сохраненную ранее в реестре сигнатур системы).
5. Документ сохраняется в базе данных «E-register».
6. Организация или любой заинтересованный пользователь, как в РУз, так и за ее пределами, желающий проверить Апостиль по QR-коду, передает запрос через специальную форму Apostille check. Запрос направляется в «E-register», откуда возвращается ответ. При проверке по QR-коду должна выдаваться вся информация и реквизиты запрашиваемого Апостиля. Модуль также должен позволять проверить Апостиль по введенному номеру и дате выдачи.

4.1.1.2. Требования к режимам функционирования ИС

Для ИС определены следующие режимы функционирования:

- нормальный режим функционирования;

- аварийный режим функционирования.

Основным режимом функционирования ИС является нормальный режим.

В нормальном режиме функционирования ИС:

- Портал функционирует круглосуточно семь дней в неделю;
- серверное программное обеспечение и технические средства северов обеспечивают возможность круглосуточного функционирования, с перерывами на обслуживание.

Для обеспечения нормального режима функционирования ИС необходимо выполнять требования и выдерживать условия эксплуатации системы, версионность конечных пользовательских устройств, а также комплекса технических средств ИС, указанные в соответствующих технических документах (техническая документация, инструкции по эксплуатации и т.д.).

Аварийный режим функционирования ИС характеризуется отказом одного или нескольких компонент программного и (или) технического обеспечения.

В случае перехода в аварийный режим ИС должна обеспечивать возможность завершения работы всех пользовательских сессий с сохранением данных.

Действия в аварийном режиме:

- диагностирование инцидентов или проблем, связанных со сбоями или нештатными ситуациями в работе ИС;
- восстановление при необходимости программно-аппаратной конфигурации ИС (сетевого и серверного оборудования);
- восстановление информации при ее утере средствами системы резервного копирования и восстановления;
- расследование причин нештатной ситуации и определение причин инцидента или проблемы.

Реагирование на нештатные ситуации включает оповещение обслуживающего персонала, принятие мер устранения проблемы, необходимое восстановление информации, выработку и проведение профилактических мероприятий.

4.1.1.3. Перечень и описание сценариев использования

В данном разделе приводятся основные сценарии, используемые в системе. Все возможные вспомогательные сценарии, которые поддерживают логику работы системы, могут быть реализованы по усмотрению Исполнителя в соответствии с функционалом, описанным в разделе 4.2. настоящего Технического задания.

Основными сценариями в системе являются:

- Регистрация заявки на получение апостиля (С-01-01)
- Оплата заявки (С-01-02)
- Рассмотрение апостиля (С-01-03)
- Проверка идентичности подписи, печати и штампа на представленном документе с подписями, печатями и штампами, которые содержатся в базе данных ИС (С-01-04);
- Проверка подлинности апостиля (С-01-05);
- Добавление сканированных документов (С-01-06);
- Авторизация пользователя в системе посредством One-ID (С-01-07);
- Авторизация пользователя в системе посредством ЭЦП (С-01-08);
- Проверка статуса заявки (С-01-09);
- Выгрузка документов апостиля из системы (С-01-10);
- Формирование статистических отчетов (С-01-11).

Регистрация заявки на получение апостиля

Номер сценария: *С-01-01*

Условия запуска: Запуск пользователем функционала заполнения заявки;

Владелец процесса: Заявитель/сотрудник ЦГУ либо ответственного органа;

Порядок выполнения сценария:

1. Запуск функционала заполнения заявки;
2. Заполнение пользователем всех параметров заявки;
3. Добавление к заявке сканированных версий документов (С-01-06);
4. Выполнение сценария проведения оплаты (С-01-02);
5. Сохранение заявки;
6. Отправка на рассмотрение;
7. Завершить сценарий.

Время выполнения сценария: время выполнения данного сценария не регламентируется Системой, зависит от действий пользователей.

Входные данные: Данные заявки.

Выходные данные: Идентификатор заявки, данные для рассмотрения.

Возможные расширения ИС: дополнительные проверки безопасности учетных данных

пользователя.

Оплата заявки

Номер сценария: *С-01-02*

Условия запуска: Сценарий С-01-01;

Владелец процесса: Заявитель;

Порядок выполнения сценария:

1. Запуск функционала проведения оплаты;
2. Формирование суммы государственной пошлины;
3. Выбор платежной системы для оплаты;
4. Переход на сайт платежной системы для совершения оплаты;
5. Получение данных об оплате от платежной системы;
6. Сохранение платежной информации в БД;
7. Возврат к сценарию С-01-01 для завершения работы с заявкой.

Время выполнения сценария: время выполнения данного сценария не регламентируется Системой, зависит от действий пользователей.

Входные данные: Идентификатор заявки, сумма для оплаты, идентификатор платежной системы.

Выходные данные: Данные о платеже.

Расширения ИС: в процессе эксплуатации перечень платежных систем может расширяться.

Рассмотрение апостиля

Номер сценария: *С-01-03*

Условия запуска: завершение сценария С-01-01;

Владелец процесса: ответственный сотрудник

Порядок выполнения сценария:

1. Получение заявки для рассмотрения;
2. Просмотр всех документов и данных заявки (проведение мероприятий по рассмотрению);
3. Проверка идентичности подписи, печати и штампа на представленном документе с подписями, печатями и штампами, которые содержатся в базе данных ИС (С-01-04);
4. В случае идентичности создание апостиля к документу;
5. Подписание документа с помощью ЭЦП;

6. Завершение сценария.

Время выполнения сценария: время выполнения данного сценария не регламентируется Системой, зависит от действий пользователя.

Входные данные: Идентификатор и данные заявки.

Выходные данные: Апостиль.

Проверка идентичности подписи, печати и штампа на представленном документе с подписями, печатями и штампами, которые содержатся в базе данных ИС

Номер сценария: *С-01-04*

Условия запуска: работа сценария С-01-03;

Владелец процесса: ответственный сотрудник

Порядок выполнения сценария:

1. Запуск сценария из С-01-03;
2. Получение скана документа и открытие формы поиска и проверки идентичности подписи, печати и штампа;
3. Выбор способа проверки (автоматическая, с использованием фильтра по организациям и должностным лицам);
4. Ввод параметров для запроса в БД;
5. Формирование запроса в БД для сравнения;
6. Получение ответа от БД и отображение на экране;
7. Предоставление возможности пользователю подтвердить сравнение;
8. Завершение сценария.

Время выполнения сценария: время выполнения данного сценария не регламентируется Системой, зависит от действий пользователя. Время выполнения запроса в БД регламентируется требованиями, описанными в разделе 4.1.4. настоящего ТЗ.

Входные данные: Сканированный документ (данные подписи, печати, штампа).

Выходные данные: Результат сравнения.

Проверка подлинности апостиля

Номер сценария: *С-01-05*

Условия запуска: Функционала проверки апостиля (Check Apostille)

Владелец процесса: Пользователь (любой роли)

Порядок выполнения сценария:

1. Запуск функционала Check Apostille;
2. Использование ссылки для проверки или QR-кода;
3. Отправка запроса в E-register для получения данных апостиля;
4. Возврат ответа с E-register и отображение результатов пользователю;
5. Завершение сценария.

Время выполнения сценария: время выполнения данного сценария регламентируется требованиями, описанными в разделе 4.1.4. настоящего ТЗ.

Входные данные: ссылка для проверки подлинности апостиля.

Выходные данные: перечень параметров апостиля (или сообщение об отсутствии данных).

Добавление сканированных документов

Номер сценария: *C-01-06*

Условия запуска: Выполнение сценария С-01-01, шага добавления сканированных документов

Владелец процесса: Системный процесс

Порядок выполнения сценария:

1. Обращение к сценарию;
2. Открытие формы добавления документов;
3. Выбор документа (-ов) на локальном диске пользовательского устройства;
4. Проверка корректности формата добавляемых документов;
5. Проверка качества добавляемых документов;
6. Отправка запроса на сервер на сохранение добавленных файлов;
7. Завершение сценария.

Время выполнения сценария: время выполнения данного сценария регламентируется требованиями, описанными в разделе 4.1.4. настоящего ТЗ.

Входные данные: документы, добавляемые пользователем.

Выходные данные: сканированные версии документов, сохраненные в системе.

Возможные расширения сценария: возможное расширение количества принимаемых форматов сканированных документов и их проверка.

Авторизация пользователя в системе посредством One-ID

Номер сценария: *C-01-07*

Условия запуска: Запуск пользователем функционала авторизации;

Владелец процесса: Пользователь (физическое лицо);

Порядок выполнения сценария:

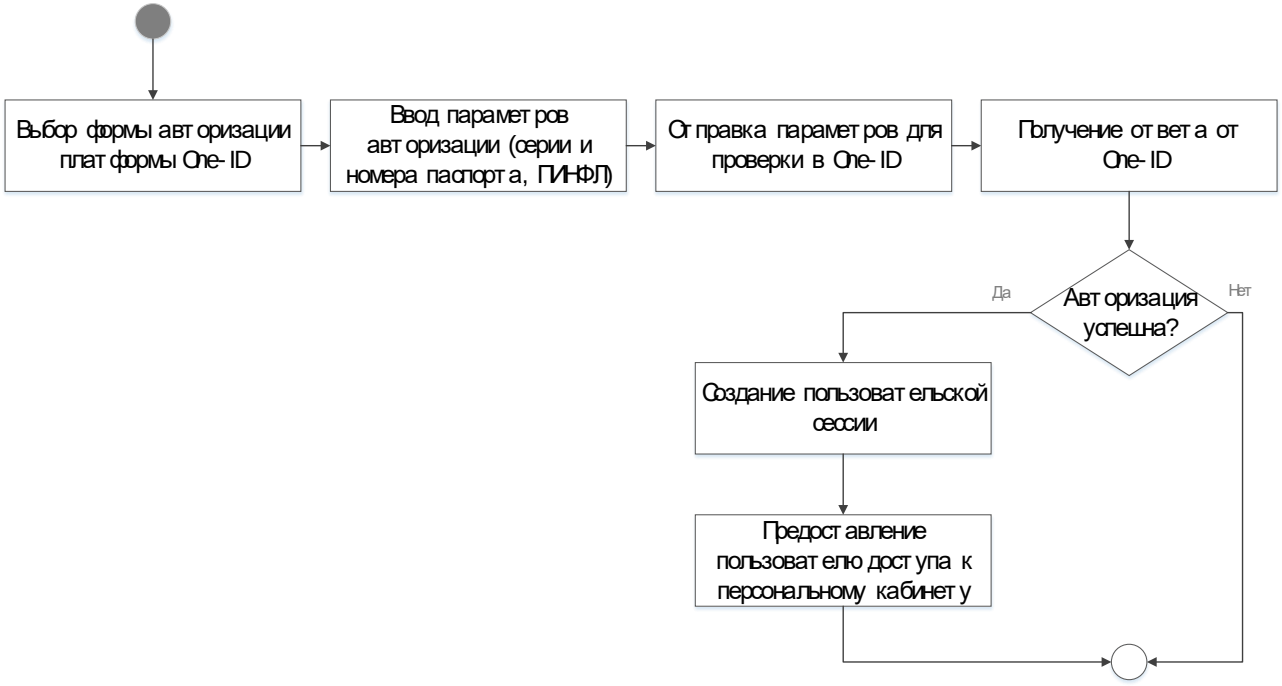
1. Запуск системы;
2. Выбор формы авторизации платформы One-ID;
3. Ввод параметров авторизации (серии и номера паспорта, ПИНФЛ);
4. Отправка параметров для проверки на платформе One-ID;
5. Возвращение ответа от платформы One-ID;
6. В случае отрицательного ответа, переход к п.9;
7. Создание пользовательской сессии;
8. Предоставление пользователю доступа к Персональному кабинету;
9. Завершить сценарий.

Время выполнения сценария: время выполнения данного сценария не регламентируется Системой, зависит от действий пользователей.

Входные данные: Серия и номер паспорта, ПИНФЛ.

Выходные данные: Идентификатор пользовательской сессии.

Схема сценария:



Авторизация пользователей с помощью ЭЦП

Номер сценария: *C-01-08*

Условия запуска: Запуск системы, выбор авторизации

Владелец процесса: Пользователь (юридическое или физическое лицо), сотрудник утверждающего ведомства

Порядок выполнения сценария:

1. Пользователь открывает страницу авторизации и регистрации и выбирает тип авторизации с ЭЦП.
2. Перенаправление на страницу id.egov.uz.
3. Выбор ЭЦП и ввод пароля
4. Подтверждение данных системой ЕСИ
5. Получение ответа от ЕСИ об успешном прохождении авторизации.
6. Предоставление пользователю доступа в систему (создание пользовательской сессии).
7. Завершение сценария.

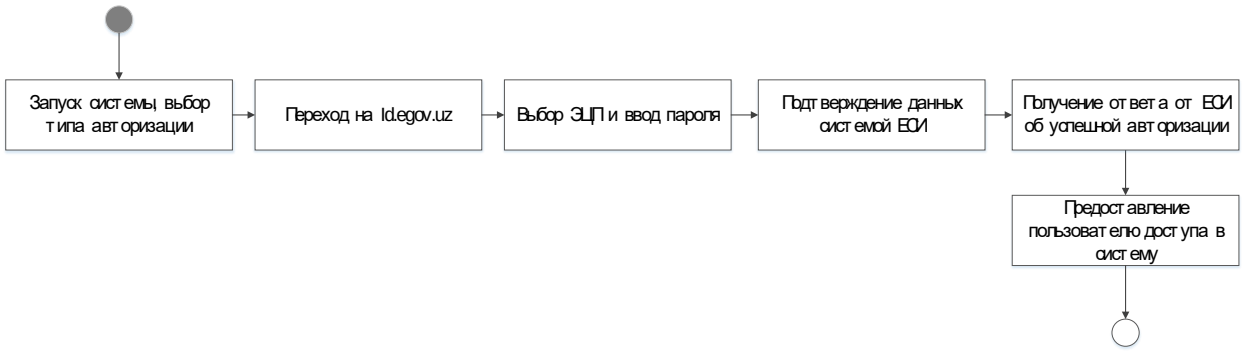
Время выполнения сценария: временной регламент обработки сценария регламентируется временем ответа внешней системы (ЕСИ).

Входные данные: Электронный ключ (при использовании ЭЦП).

Выходные данные: идентификатор пользовательской сессии.

Сценарий С-01-08 не предполагает расширения и направлен только на обеспечение доступа пользователей к ИС, включая доступ юридических лиц и сотрудников ответственных утверждающих ведомств.

Схема сценария:



Проверка статуса заявки

Номер сценария: *С-01-09*

Условия запуска: Запуск раздела отправленных заявок, запрос статуса выбранной заявки

Владелец процесса: Пользователь (юридическое или физическое лицо)

Порядок выполнения сценария:

1. Пользователь открывает страницу со списком заявок, отправленных на

рассмотрение.

2. Выбирает заявку для запроса статуса по ней.
3. Система отправляет запрос на сервер для получения информации о деталях заявки (включая статус)
4. Получение ответа от сервера и формирование страницы деталей заявки для пользователя.
5. Завершение сценария.

Время выполнения сценария: общее время выполнения сценария не регламентируется и зависит от действий пользователя в системе, время выполнения запроса на сервер регламентируется требованиями, описанными в разделе 4.1.4. настоящего ТЗ.

Входные данные: Электронный ключ (при использовании ЭЦП).

Выходные данные: идентификатор пользовательской сессии.

Примечание: статус заявки может быть также запрошен при формировании страницы списка отправленных заявок, и отображен непосредственно в списке.

Выгрузка документов апостиля из системы

Номер сценария: *С-01-10*

Условия запуска: запуск функционала выгрузки документов апостиля

Владелец процесса: Пользователь (юридическое или физическое лицо)

Порядок выполнения сценария:

1. Для документов в статусе «Готово» инициируется функционал выгрузки документов.
2. Отправка запроса на сервер для выдачи документа.
3. Получение ответа от сервера и открытие документа в формате pdf в новой вкладке браузера (отображение формата pdf подразумевает возможности выгрузки и вывода документа на печать).
4. Завершение сценария.

Время выполнения сценария: время выполнения запроса на сервер регламентируется требованиями, описанными в разделе 4.1.4. настоящего ТЗ.

Входные данные: идентификатор заявки, а также документа.

Выходные данные: документ апостиля в формате pdf.

Формирование статистических отчетов

Номер сценария: *С-01-11*

Условия запуска: Запуск функционала формирования статистики

Владелец процесса: пользователь (администратор, сотрудник ведомства)

Порядок выполнения сценария:

1. Запуск функционала статистики;
2. Выбор параметров статистической выборки (см. п.4.2.6.7);
3. Отправка запроса на сервер для формирования статистических данных;
4. Получение статистической информации от сервера и формирование ее для просмотра пользователя.
5. Завершение сценария.

Время выполнения сценария: время выполнения запроса на сервер регламентируется требованиями, описанными в разделе 4.1.4. настоящего ТЗ.

Входные данные: параметры запроса.

Выходные данные: статистическая выборка, соответствующая параметрам запроса.

Возможные расширения сценария: количество параметров для статистической выборки может со временем увеличиваться в соответствии с требованиями Заказчика.

4.1.1.4. Требования по диагностированию ИС

Для обеспечения высокой надежности функционирования ИС, так и ее отдельных компонентов должно обеспечиваться выполнение требований по диагностированию ее состояния.

Диагностирование ИС должно осуществляться штатными средствами, входящими в комплект поставки программного обеспечения (на стороне бэкенда).

Обязательно ведение журналов инцидентов в электронной форме, а также графиков и журналов проведения ППР. Для всех технических компонентов серверной части необходимо обеспечить регулярный и постоянный контроль состояния и техническое обслуживание.

4.1.1.5. Перспективы развития, модернизации ИС

Основным принципом при разработке ИС является принцип масштабируемости программной части, для того чтобы система могла развиваться и наращиваться дополнительными модулями, выполняющими новые функции, по требованию и в соответствии с условиями Заказчика.

4.1.2. Требования к взаимодействию с информационными системами других организаций

Для интеграции ИС со сторонними системами, с другими государственными ИС

должны быть разработаны интерфейсы (API), в соответствии с требованиями государственного стандарта O’z DSt 2590:2012.

Для получения данных от сторонних информационных систем в ИС будут также формироваться API, отправляемые в бэкенд для дальнейшей обработки.

ИС должна использовать API, разработанные в рамках Технологических инструкций, утвержденных с интегрируемыми ведомствами. Технологические инструкции должны составляться при содействии Исполнителя. Заказчик ответственен за утверждение Технологических инструкций с внешними организациями.

Взаимодействие API должно быть авторизованным, все функциональные методы API должны быть вызваны после процедуры авторизации. Все вызовы API должны быть журналированы на уровне базы данных ИС.

Необходима поддержка форматов JSON, XML, WSDL в качестве формата передаваемых и принимаемых данных в ИС.

Взаимодействие Системы со сторонними ИС должно производится через протокол приема и передачи данных HTTPS.

ИС должна использовать единые справочники и классификаторы, принятые в Республике Узбекистан.

4.1.3. Требования к численности и квалификации пользователей

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

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

Пользовательский интерфейс должен отображать только те инструменты, функции и методы, которые могут быть востребованы пользователем с данным конкретным уровнем доступа.

В работе ИС необходимо предусмотреть следующие роли:

№	Группы пользователей
1	Заявитель – пользователь, желающий получить услугу по проставлению электронного апостиля посредством ЕПИГУ
2	Ответственный сотрудник – пользователь, работающий в соответствующем министерстве или ведомстве, принимающий заявки, а также проверяющий документы и подписывающий апостиль
3	Сотрудник АГУ – пользователь, участвующий в процессах приёма заявок, мониторинга

	и контроля выдачи апостилей
4	Администратор – пользователь, имеющий полный доступ к системным настройкам, справочникам, учетным записям пользователей, журналам событий и другим данным системы.
5	Гость – пользователь, желающий проверить подлинность апостиля по QR-коду.

Предусмотреть минимальный уровень квалификационных требований, которые нужны пользователям для работы в Системе (минимальный уровень компьютерной образованности). Требования к роли Сотрудник АГУ - средний уровень компьютерной образованности, к роли Администратор – высокий уровень компьютерной образованности.

4.1.3.1. Требования к профессиональному образованию, компетенциям и навыкам персонала

Численность персонала со стороны Заказчика должна быть достаточной для информационной и технической поддержки ИС при отсутствии непредвиденных аппаратных сбоев и обстоятельств непреодолимой силы (форс-мажор). Минимальные требования к профессиональному образованию, компетенциям и навыкам персонала определяются должностными инструкциями и с учетом предложений Разработчика.

Предполагаемый перечень категорий персонала и необходимые квалификационные требования представлены в таблице ниже.

Категория персонала	Квалификация персоналу	Порядок подготовки и контроля знаний и навыков
Персонал технического обслуживания	1) Навыки технического обслуживания программных продуктов и аппаратных средств серверного и коммуникационного оборудования; 2) Навыки диагностики отказов средств вычислительной техники.	Специальное образование, специализированные курсы по обслуживанию программных продуктов, администрированию серверного и коммуникационного оборудования.
Группа сопровождения	1) Профессиональные знания применяемых операционных систем, систем управления базами данных и способов их системного администрирования; 2) Знания сетевых и телекоммуникационных технологий;	Специальное образование. Контроль: собеседование, удостоверяющие документы, пробная работа, испытательный срок.

	3) Знание технологий обеспечения информационной безопасности.	

4.1.3.2. Требования к режиму работы персонала

Специальные требования к режиму работы пользователей ИС не предъявляются.

4.1.4. Показатели назначения

ИС должна обеспечивать возможность одновременной работы не менее 5 000 пользователей при следующих характеристиках времени отклика:

- для операций навигации по экранным формам без обращений к базе данных - не более 1 сек;
- для операций, связанных с запросами в БД - не более 10 сек (в зависимости от скорости сети);
- для операций, связанных с взаимодействием с внешними системами - не более 10 сек (в зависимости от скорости сети);
- для других операций - не более 5 сек.

4.1.5. Требования к надежности

ИС должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- при сбоях в аппаратной или программной части оконечного устройства пользователя (рабочей станции), приводящих к перезагрузке операционной системы, восстановление программы должно происходить после перезагрузки устройства;
- при ошибках в работе рабочих станций восстановление функции ИС возлагается на операционную систему устройства;
- при ошибках, связанных с программным обеспечением рабочей станции, восстановление работоспособности возлагается на операционную систему.

ИС должна исключать случайные вызовы процедур, функций, команд, применяемых в функционале. Все вызовы функций, методов, процедур должны быть тщательно проверены, на предмет случайного вызова.

ИС должна быть защищена от неверного использования функций пользователями.

ИС должна обеспечивать корректную обработку ситуаций, вызванных недопустимыми и несогласованными значениями входных данных. В указанных случаях ИС должна выдавать пользователю соответствующие аварийные сообщения, после чего возвращаться в рабочее

состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

ИС, после проведения работ по настоящему Техническому заданию, должна быть устойчива по отношению к программно-аппаратным ошибкам, с возможностью восстановления ее работоспособности и целостности информационного содержимого при возникновении ошибок и отказов рабочих станций пользователей.

ИС должна поддерживать до 10 млн. пользователей к третьему году эксплуатации, 1 млн. активных пользователей.

4.1.6. Требования к безопасности

ИС должна соответствовать общим требованиям безопасности программных средств при работе в составе информационных систем.

Принципы построения решения должны отвечать современным мировым стандартам по степени защищенности и сохранности информации и включать:

- средства шифрования пересылаемой пользователями информации;
- методы для защиты базы данных от несанкционированного доступа;
- протоколирование и аудит, регистрация всех событий и действий пользователей;
- ограничение доступа пользователя к объектам ИС на основе идентификации пользователя в том числе по его роли;
- доступ к данным ограничивается правами доступа, которые определяются ролями пользователей ИС: пользовательский интерфейс отображает только те инструменты, функции и методы, которые могут быть востребованы пользователем с данным конкретным уровнем доступа;
- гибкое управление правами доступа; предоставление возможности Администратору вести учетные записи пользователей;
- защита каналов передачи данных;
- разграничение прав доступа пользователей и Администраторов ИС будет строиться по принципу "что не разрешено, то запрещено";
- защита передаваемой информации посредством шифрования конфиденциальных данных при передаче по каналам связи.

Используемые при разработке технологии должны обеспечить безопасность доступа к данным за счет аутентификации, идентификации и ролевых прав пользователей.

При работе системы на уровне бэкенда ИС должно реализовываться журналирование каждого сеанса пользователя с указанием MAC адреса устройства, с которого был произведен

вход в систему, и времени входа в систему.

Автоматическое ведение журнала аудита должно также предоставлять возможность мониторинга наиболее критичных (уникальных) данных, хранящихся в БД и регистрации всех происходящих событий и изменений любых данных в системе в соответствии с настройкой системы.

Журнал аудита должен создаваться автоматически и вестись постоянно. Каждая операция в журнале аудита должна идентифицироваться по пользователю, дате и времени. Должна быть обеспечена защита журнала аудита от корректировки и удаления записей.

Так как ИС будет работать в связке с Web-сервером все запросы должны передаваться по зашифрованному каналу HTTPS с использованием сертификата SSL, это позволит сохранять стабильную скорость и высокую степень безопасности между приложением и Web-сервером.

Информационная система должна быть размещена в датацентре, отвечающем требованиям информационной безопасности. Заказчик должен обеспечить соответствие серверных комнат и условий их оснащения и оборудования необходимым требованиям для нормального функционирования Системы, а также соответствие требованиям Государственного стандарта O‘z DSt 2875:2014 «Требования к датацентрам. Инфраструктура и обеспечение информационной безопасности».

Хранилище электронных ключей должно быть физически разнесено для обеспечения отсутствия единой точки отказа. Для хранилища электронных ключей (ЭЦП для заверения апостиля) должно дополнительно обеспечиваться резервирование на внешний сервер.

Все внешние элементы технических средств информационной системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь защитное заземление.

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

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

4.1.6.1. Требования к защите информации от несанкционированного доступа

ИС должна соответствовать всем установленным требованиям в действующей нормативной документации Заказчика по защите информации от несанкционированного доступа.

В ИС должно обеспечиваться ограничение физического доступа к элементам системы,

как с целью предотвращения нарушения работы системы, так и с целью получения неавторизованного доступа к информации:

ИС должна реализовывать механизм безопасности и защиты информации на основе следующих основных принципов:

- ограничение доступа к системе на основе идентификации пользователя;
- ограничение доступа к объектам системы;
- ведение журнала аудита для выявления неавторизованных изменений в системе;
- защита каналов передачи данных.

ИС должна обеспечивать функцию контроля доступа к информационным ресурсам Портала.

При разработке перечень персонализированных данных может быть расширен.

ИС должна обеспечивать предоставление информации для ведения журналов (Логи), в которые заносится информация о системных событиях, попытках несанкционированного доступа к информации для всех пользователей ИС.

Защита информации должна включать в себя комплекс организационных мер и программно-аппаратных методов и средств защиты информации, обеспечивающих предотвращение несанкционированного доступа к информационным ресурсам. ИС должна обеспечивать целостность, доступность и конфиденциальность данных при их обработке.

При разработке ИС должны быть учтены требования политики информационной безопасности, действующие у Заказчика, чтобы избежать возникновения конфликтных ситуаций при проведении мероприятий по обеспечению информационной безопасности.

Пароли пользователей должны отвечать требованиям сложности паролей в целях предотвращения попыток взлома методом перебора. Количество неудачных попыток входа в ИС должно быть ограничено и при его превышении ИС должна блокироваться на определенный промежуток времени. Никто не должен иметь права на изменение/удаление записей журналов логов.

4.1.6.2. Требования по сохранности информации при авариях

Сохранность информации на уровне программного обеспечения ИС должна обеспечиваться при:

- аварийных ситуациях в помещении расположения серверов ИС;
- сбоях работы сети, вызванных потерей питания;
- отказах технических средств.

При авариях система обладает возможностью полного восстановления данных за счет

резервного копирования. На уровне программного обеспечения необходимо предотвратить частичную или полную потерю пользовательских данных и нарушение целостности информации, хранящейся в базе данных.

Система должна обеспечивать резервное копирование собственной базы данных, а также настроек системы, которые должны использоваться для восстановления системы. Резервные копии должны хранятся на энергонезависимых носителях и периодически обновляться по мере поступления новых данных и/или не менее чем раз в сутки. Восстановление данных должно осуществляться путем выбора последней неиспорченной копии.

Технические средства системы, должны быть снабжены устройствами бесперебойного питания (UPS) для предохранения от перепадов напряжения и непредвиденного отключения электричества.

Информационная безопасность должна соответствовать требованиям, установленным в действующих редакциях стандартов: O‘z DSt ISO/IEC 13335-1, O‘z DSt ISO/IEC 15408-1, O‘z DSt ISO/IEC 15408-2, O‘z DSt ISO/IEC 15408-3, O‘z DSt ISO/IEC 27001, O‘z DSt ISO/IEC 27002, O‘z DSt 2814.

Информация, отображаемая в ИС, не должна терять свое качество (актуальность, полноту, достоверность), разрушаться, повреждаться, искажаться и теряться при возникновении любых аварийных ситуаций: отказа технических средств, потери питания в электросети и т.п.

4.1.6.3. Требования к защите от влияния внешних воздействий

Необходимо применение экранированных кабелей, экранирование помещений, где должно размещаться оборудование, учесть условия совместного использования радиоэлектронных средств (радиосвязи, телевизионных и радиовещательных передатчиков, сотовых и пейджинговых систем связи и др.) при которых взаимные помехи не влияют на работоспособность оборудования.

Оборудование, предназначенное для работы ИС, должно быть устойчиво к внешним воздействующим факторам.

Оборудование, предназначенное для работы ИС, в упакованном виде должно выдерживать хранение в течение года (включая транспортирование) в складских помещениях при температуре от -50 °С до +40 °С, при среднемесячном значении относительной влажности 80 % при температуре +20 С (допускается кратковременное повышение влажности до 98% не более 1 месяца в год).

В случае потери работоспособности при сбоях, ошибках или отказах программно-

технических средств ИС должна обеспечивать 100% гарантию сохранности информации.

Регламент работы ИС должен предусматривать создание резервных копий баз данных и сопутствующей информации.

4.1.7. Требования к эргономике и технической эстетике

ИС должна обеспечивать удобные для пользователей интерфейсы, отвечающие следующим требованиям:

- При создании ИС должен быть разработан удобный и интуитивно понятный интерфейс для пользователя, который хорошо знает свою предметную область и не является специалистом в области информационных технологий.
- Пользовательские интерфейсы ИС должны быть спроектированы и разработаны с применением единых принципов графического представления информации и организации доступа к функциональным возможностям и сервисам.
- Должен быть разработан графический дизайн пользовательских интерфейсов, цветовые, шрифтовые и композиционные решения для отображения текстов, изображений, таблиц, гиперссылок, управляющих и навигационных элементов (меню, кнопок, форм и т.п.), поля для заполнения должны иметь примечания о данных, которые требуется ввести.
- ИС должна обеспечивать качественное взаимодействие пользователя (человека) с системой.
- Основным требованием по эргономике и технической эстетике является адекватность времени реакции компонентов ИС на сложность запроса пользователя к базам данных:
  - при выполнении стандартных запросов пользователь должен работать с ИС в реальном режиме времени (до 1 секунды на ответ);
  - пользователь должен получать ответ от системы в течении 5 секунд после отправления стандартных запросов (при максимально хорошем качестве сигнала сети);
  - при выполнении сложных запросов, требующих длительного времени на выполнение, пользователь должен получать предупреждение о процессе ожидания.
- Дизайн компонентов презентационного уровня ИС должен быть разработан с учетом стандартных эргономических требований на пользовательский

графический интерфейс, обеспечивающий комфорт и продуктивность работы его пользователей, а также быструю загрузку выбранных пользователем страниц.

- При разработке дизайна интерфейса должны ставиться в приоритет удобство и простота понимания интерфейса. Дизайн элементов пользовательского интерфейса должен вызывать минимальное понимание действий, которое совершит пользователь при взаимодействии с одним из элементов. Элементы интерфейса не должны ассоциироваться с функциями, которые они не выполняют. Дизайнерские решения должны соответствовать действующим санитарным и эргономическим стандартам и наиболее эффективно создавать положительную эмоциональную реакцию у пользователей ИС.
- Дизайн пользовательского интерфейса системы должен быть адаптивным под разрешения большинства экранов.

Необходимо применить следующий минимальный перечень требований:

- ИС должна иметь удобную систему навигации, то есть возможность перехода к интересующей информации за 1-3 клика.
- Вся информация должна быть разбита на блоки и выделяться деталями оформления для удобства работы с ней.
- Структура ИС должна быть спроектирована таким образом, чтобы, находясь на любой странице, пользователь понимал, где он находится, и как перейти к интересующей его информации.
- Навигация осуществляется при помощи ссылок на тип отображения информации в ИС, а также ссылок на объекты данных.
- Элементы интерфейса не должны ассоциироваться с функциями, которые они не выполняют.
- В разработке дизайна должны учитываться самые современные дизайнерские решения UI (user interface) и UX (user experience) для удобства пользователей.

4.1.8. Требования к транспортабельности

Требования к транспортабельности не предъявляются.

4.1.9. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов ИС

Минимальный срок эксплуатации ИС:

- в целом - не менее 10 лет;
- отдельных функциональных модулей - не менее 3 лет;

Требования к жизненному циклу ИС на стадиях промышленной эксплуатации должны быть уточнены в процессе разработки.

Периодическое техническое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации производителя оборудования.

Эксплуатация технических средств ИС и безопасность помещений, в которых они расположены, должны обеспечиваться с соблюдением требований руководящего документа RH 45-201:2011 «Технические требования к зданиям и сооружениям для установки средств вычислительной техники» и государственного стандарта 0‘z DSt 2875:2014 «Требования к датацентрам. Инфраструктура и обеспечение информационной безопасности».

4.1.10. Требования к патентной и лицензионной чистоте

Исполнитель должен использовать только объекты интеллектуальной собственности, права на которые приобретены (получены) и используются без нарушений прав на интеллектуальную собственность третьих лиц или предоставлены Заказчиком. Это требование должно обеспечивать соблюдение авторских, смежных, патентных и иных прав разработчиков используемых сторонних компонент. Исполнитель обязуется безвозмездно передать ему права на использование охраняемых результатов интеллектуальной деятельности, права на которые принадлежат Исполнителю и (или) третьим лицам, и которые использовались Исполнителем.

4.1.11. Требования по стандартизации и унификации

На всех стадиях разработки проекта должна обеспечиваться унификация проектных решений, что должно обеспечиваться единообразным подходом к решению однотипных задач, унификацией технического, информационного, лингвистического, математического, информационного и организационного обеспечения. Единообразный подход к решению однотипных задач должен достигаться:

- унификацией функциональной структуры в части реализации автоматизированных функций и информационных связей между ними;
- одинаковым программно-техническим способом реализации подобных функций системы и единым интерфейсом с пользователем, соответствующим международным стандартам.

Унификация технических средств должна достигаться за счет:

- применения серийных технических средств, соответствующих международным стандартам;
- минимизации применяемых типов вычислительных машин и других компонентов;
- использования типовых автоматизированных рабочих мест, компонентов и комплексов.

Унификация информационного обеспечения должна достигаться за счет:

- использования единой системы классификации и кодирования объектов и входящих в состав подсистем;
- использования национальных, отраслевых и других стандартных классификаторов, применяемых в практике функционирования объекта;
- использования типовых форм документов (отчетов) и рационального ограничения их видового состава (по согласованию с Заказчиком);
- применения единых методов и средств сбора, подготовки, контроля и хранения информационных массивов системы.

Унификация математического обеспечения должна достигаться за счет модульного принципа построения алгоритмов и типизации алгоритмических модулей.

Унификация ПО должна достигаться:

- максимально возможным применением стандартных программных средств;
- использованием унифицированных программных модулей при разработке прикладных программ.

Показатели, устанавливающие требуемую степень использования стандартных, унифицированных методов реализации функций Системы, поставляемых программных средств, типовых математических методов и моделей, типовых проектных решений:

- поддержка современных транспортных протоколов: **TCP/IP, HTTP(S);**
- поддержка Internet-стандартов: **RESTfulAPI**;
- поддержка стандартов реализации поисковых механизмов;
- поддержка наиболее распространенных форматов документов: **Json, Json-rpc, XML, HTML, Javascript;**
- поддержка кластерных решений с балансировкой нагрузки;
- поддержка распределенного поиска информации;
- поддержка распределенного доступа к информации;
- возможность функционирования на различных аппаратных платформах.

Система кодирования и классификации, используемая для формирования

нормативно-справочной информации, должна отвечать требованиям классификации и атрибутирования документов, принятым на территории Республики Узбекистан, а также учитывать мировой опыт создания подобных систем1.

Разрабатываемое решение должно обеспечивать унификацию функциональных задач, операций и пользовательских интерфейсов.

4.2. Требования к функциям (задачам), выполняемым ИС

4.2.1. Модуль авторизации пользователей

Модуль авторизации пользователей предназначен для обеспечения доступа заявителей к функционалу системы.

ИС должна позволять авторизоваться посредством One-ID, а также с использованием ЭЦП. Юридические лица будут иметь возможность авторизоваться с использованием ЭЦП.

Авторизация должна быть доступна через ЕПИГУ.

4.2.2. Модуль авторизации ведомств

В проставлении апостиля может участвовать одно из пяти ответственных ведомств:

- Верховный суд;
- Министерство иностранных дел;
- Инспекция по контролю за качеством образования;
- Территориальные управления юстиции;
- Генеральная прокуратура.

Для каждого ответственного сотрудника должна быть создана учетная запись в системе. Авторизация должна происходить с использованием ЭЦП при взаимодействии с ЕСИ, согласно электронным ключам внутреннего модуля системы (см. раздел 4.2.3 настоящего ТЗ).

Также доступ к ИС должен быть организован для сотрудников Агентства государственных услуг с целью использования функций отправления заявок, мониторинга процессов обработки запросов на получение апостиля и контроля работоспособности системы.

4.2.3. Модуль ЭЦП и хранения сигнатур

Формирование и проверка ЭЦП в разрабатываемой системе должны полностью соответствовать стандартам ITU-T X.509.

В ИС должно быть реализовано единое хранилище ключей ЭЦП для проверки наличия сертификата и выпуска доверенного сертификата.

---

[1] Единая система классификации и кодирования технико-экономической и социальной информации Республики Узбекистан.
https://new.standart.uz/upload/file/stand-text/OzDSt/ozdst_6.01.1-2007.pdf

ЭЦП данного формата будут использоваться для авторизации сотрудников ответственных ведомств, а также для проставления подписи при заверении апостиля.

4.2.4. Модуль хранения сигнатур и печатей

Система должна позволять хранить и использовать цифровые и графические сигнатуры (подписи и печати), вести их учет, позволять контролировать сроки их использования в соответствии с регламентом.

Данный модуль должен позволять проводить графический анализ соответствия сигнатуры апостилируемых документов (сканов) и печатей организаций их выдававших.

При формировании сигнатур необходимы следующие сведения о должностном лице:

- ФИО;
- Должность;
- Ведомство;
- E-mail;
- Комментарий;
- Активна ли учетная запись;
- С какого по какое число учетная запись активна;
- Фото подписи;
- Фото печати и штампа в хорошем качестве.

Для функционирования данного модуля будут собраны образцы всех подписей и печатей, штампов ответственных органов, документы которых попадают для рассмотрения и получения апостиля.

4.2.5. Кабинет пользователя

В кабинете пользователя заявитель получает возможность работы с электронными апостилями, включая:

- Формирование заявки для получения апостиля;
- Добавление сканированных версий документов для рассмотрения;
- Проверку статуса заявок;
- Выгрузку готового документа апостиля.

4.2.5.1. Модуль формирования заявки

Формирование заявки на получение Апостиля (один документ или пакет документов) осуществляется заявителем.

В данном модуле должны заполняться данные (не ограничиваясь):

- Данные физического лица Ф,И,О:
    - Серия и номер паспорта;
    - ПИНФЛ;
    - Дата рождения;
    - Адрес;
    - Номер телефона;
    - Электронный адрес;
- Данные юридического лица (Наименование ю/л):
    - ИНН организации;
    - Наименование организации;
    - Юридический адрес организации;
    - Электронный адрес;
- Количество апостилируемых документов;
- Тип апостилируемых документов (должен быть единый тип по одному делу);
- Скан апостилируемого документа (каждого);
- Дата заполнения заявки (формируется автоматически).
    - Реквизиты апостилируемого документа (дата, номер, город);
    - Страна отправления;
    - Язык заполнения (англ/узб/рус).

При выборе типа первого подаваемого документа пользователь должен видеть весь список подаваемых документов. При добавлении следующих документов список типов документов должен отсортировываться согласно ведомству назначения. Данный пункт позволит исключить добавление в заявку документов, относящихся к разным ведомствам для рассмотрения.

При заполнении заявки предусмотреть поле, определяющее, в каком виде будет выдан апостиль, в бумажном или электронном. На первом этапе внедрения системы необходимо использовать любой из вариантов (бумажный или электронный) как при подаче заявки, так и при получении апостиля.

Примечание: в одной заявке могут подаваться несколько документов, однако все они должны направляться только в одно ведомство. Оплата в этом случае производится за подачу одной заявки. В случае возможной ошибки, когда документ попадет в другое ведомство не по назначению, то необходимо предусмотреть в системе возможность перенаправления заявки в другое ведомство без возврата заявки заявителю. Сотрудники

АГУ либо ответственных органов должны рассмотреть заявку и правильно перенаправить запрос.

4.2.5.2. Модуль добавления сканированных версий документов

В данном модуле пользователь добавляет в систему сканированные документы в формате .pdf. Система должна автоматически проверять качество добавляемого документа и при невозможности распознать документ, выдавать ошибку.

Все сканированные версии документов могут быть добавлены с локального диска персонального компьютера пользователя в хранилище документов персонального кабинета пользователя. Далее документы из хранилища могут прикрепляться к заявке.

Также возможен вариант прикрепления документа с локального диска непосредственно к заявке и автоматическое сохранение документа в хранилище.

4.2.5.3. Модуль проверки статуса заявок

Пользователь должен иметь возможность видеть список своих направленных заявок для получения апостиля и видеть статусы по каждой заявке.

В случае, если пользователь направил для получения апостиля несколько документов, относящихся к разным ведомствам, то каждый из документов может иметь свой статус, при этом общий статус заявки формируется из статуса наиболее запоздалого документа. В случае частичного положительного рассмотрения (на часть документов проставлен апостиль, а на оставшиеся – не проставлен), то пользователь увидит статусы рассмотрения непосредственно на документах.

Возможные статусы заявки для пользователя:

- На рассмотрении;
- Рассмотрена;
- Отказана.

Возможные статусы документов, входящих в состав заявки:

- На рассмотрении;
- Готово;
- Отказано.

Предоставить возможность пользователю просмотреть любую из заявок, направленных им. В том числе необходимо создать сортировку по документам, на которые получен апостиль.

Пользователь должен иметь возможность получать уведомления касательно изменения статуса заявок или документов в составе заявок.

4.2.5.4. Модуль выгрузки Апостиля

Пользователю должны быть доступны:

- Выгрузка Апостиля и вывод его на печать в формате .pdf.
- Просмотр истории заявок и результатов рассмотрения (с применением фильтров по дате, типу документа, результату рассмотрения каждого документа и др.).

Документ апостиля формируется согласно утвержденному шаблону.

Апостиль имеет два приложения:

1. Перепроверка подлинности утверждения;
2. Непосредственно апостилируемый документ.

Параметры апостиля:

1. Ф.И.О должностное лицо, подписавшего официальный документ, поданный на апостиль.

Официальное наименование государственного органа, выдавшего официальный документ.

Когда апостиль проставляется на нотариально заверенной копии официального документа, слова «нотариально заверенная копия» после слов «этот публичный документ» в строке 1 апостиля, а также фамилия и должность нотариуса и название нотариальной конторы соответственно.

2. Должность лица, подписавшего официальный документ. Если официальный документ подписан более чем одним лицом, указывается должность самого высокого в их должности (например, председательствующий судья).
3. Официальное название организации, выдавшей официальный документ.
4. Город, страна в котором был проставлен апостиль.
5. Дата проставления апостиля цифрами.
6. Ф.И.О. и должность лица, апостилизировавшего официальный документ.
7. Порядковый номер, соответствующий порядковому номеру в E-register.
8. Вид выданного апостиля (в электронной или бумажной форме)
9. QR-код апостиля (уникальный в мировом масштабе);
10. символ/печать выдавшего гос органа;
11. сведения об электронной подписи.

На каждом апостиле внизу документа, должна быть приписка, что настоящий документ можно проверить по указанному (обозначенному) веб-адресу.

4.2.6. Кабинет ведомств

Кабинет ведомства предназначен для получения заявок, относящихся непосредственно к данному ведомству, рассмотрения документов, внесения дополнительных сведений в систему, подписания апостиля или отказа в выдаче апостиля по данному документу.

В каждое ведомство должны поступать заявки согласно регламенту рассмотрения.

4.2.6.1. Модуль очереди документов

Модуль предполагает работу с очередью документов (заявок) на рассмотрение для получения Апостиля.

Модуль подразумевает использование возможности редактирования заявки, проверки заверяющей подписи в модуле сигнатур и печатей, заверения, изменения статуса.

Параметры каждой заявки аналогичны тем, которые описаны в разделе 4.2.4.1. настоящего ТЗ.

4.2.6.2. Модуль Досье

В модуле Досье должна быть организована возможность просмотра Досье всех рассматриваемых документов/заявок вне зависимости от того, был ли проставлен апостиль на документ.

4.2.6.3. Модуль Сток

В модуле должна быть возможность просмотра отклоненных заявок. При рассмотрении документов обязательно должна быть возможность внесения комментария ответственным сотрудником по результатам рассмотрения. Данный комментарий необходим для внутреннего пользования.

4.2.6.4. Модуль подписанных документов

Модуль предполагает работу с подписанными документами, включая просмотр, поиск по ним. Также должна быть предоставлена возможность просмотра всех сканированных версий документов.

Поиск должен быть организован в соответствии с требованиями раздела 4.2.5.5. настоящего ТЗ.

Параметры апостиля описаны в разделе 4.2.4.4. настоящего ТЗ.

4.2.6.5. Модуль поиска

ИС должна предоставлять сотрудникам ведомств функцию расширенного поиска по всем документам/заявка в БД.

Расширенный поиск по документам должен включать в себя в том числе параметры

фильтрации документов по типам, по утверждающим сотрудникам, по территориальной принадлежности, по дате проставления Апостиля, по фамилии заявителя и другим возможным параметрам.

4.2.6.6. Модуль мониторинга оказания государственных услуг

Данный модуль позволяет сотрудникам АГУ проводить мониторинг за оказанием государственных услуг, в частности, контролировать сроки исполнения заявок, передавать по назначению ошибочно переданные заявки.

Сотрудник АГУ в любой момент должен иметь доступ к информации касательно:

- Полного перечня рассматриваемых заявок;
- Перечня заявок с истекающим сроком рассмотрения (для формирования уведомлений);
- Заявок, переданных в АГУ для передачи по назначению в другое ведомство;
- Заявок, по которым вынесено решение, за выбранный период;
- Заявок, по которым не был выдан Апостиль (отказы);
- Заявок, относящихся к определенному ведомству;
- Заявок, относящихся к определенному должностному лицу, проставляющему Апостиль.

На этапе разработки могут быть предусмотрены другие параметры для контроля со стороны АГУ.

4.2.6.7. Модуль статистики

ИС должна предусматривать формирование статистических данных по объему заявок, выданных Апостилей, а также в разрезе ведомств, стран/регионов/районов, физических/юридических лиц и др.

Полный перечень статистических параметров для выборки будет определен на этапе разработки системы.

4.2.7. Административный модуль

Административный модуль предназначен главным образом для сотрудников Агентства государственных услуг, которые будут осуществлять функции мониторинга работоспособности системы, формирования листа сигнатур, а также им должны быть доступны:

- Dashboard по всем основным показателям выдачи Апостилей;
- Лист поступающих заявок и возможность направления заявок согласно

регламенту, в ответственные ведомства (в случае, если не произошло автоматического распределения);

- Лист досье по рассматриваемым заявкам;
- Функционал формирования сигнатур (см. раздел 4.2.3 настоящего ТЗ);
- Просмотр статистики по различным показателям;
- Функционал формирования реестра/базы данных подписей, печатей и штампов должностных лиц, которые могут подписывать официальные документы, для дальнейшей их идентификации с подписями, печатями и штампами на представленном документе с подписями, печатями и штампами, которые содержатся в базе данных ИС;
- Лист отклоненных дел (сток);
- Функционал расширенного поиска (аналогично описанному в разделе 4.2.5.5. настоящего ТЗ);
- Раздел формирования доступов (ролей и доступов для пользователей-сотрудников ведомств);
- Раздел просмотра системных логов;
- Раздел управления справочниками и классификаторами.

4.2.7.1. Управление ролями и доступами пользователей

В данном модуле администратору доступны все учетные записи пользователей с возможностью сортировки по типу.

Администратор должен иметь доступ заблокировать учетную запись пользователя, а также создавать учетные записи, включая отправку учетных данных пользователям, изменять типы учетных записей пользователей.

4.2.7.2. Формирование матрицы доступа

Администратору должен быть доступен функционал управления доступами в привязке к пользовательским ролям.

Доступы должны формироваться в привязке к функциональным элементам и разделам как пользовательского интерфейса, так и административного модуля.

Регулирование таблицы доступов должно позволять создавать новые пользовательские роли без нарушения логики функционирования ИС.

4.2.7.3. Управление справочниками и классификаторами

Системный модуль, который предназначен для формирования справочных данных для работы ИС. В виде справочников могут быть оформлены все вспомогательные данные для

заполнения списков. Справочники и классификаторы должны быть доступны в модуле администрирования.

4.2.7.4. Просмотр логов

ИС должна сохранять логи всех системных событий, включая:

- события по всем межсистемным взаимодействиям;
- все действия пользователей в ИС.

При просмотре логов должна быть возможность сортировать информацию по дате, имени пользователя, типу событий и другим возможным параметрам для удобства поиска нужного события. Данный функционал должен быть доступен Администратору системы.

4.2.7.5. Мониторинг сервисов

Мониторинг сервисов должен позволять администратору системы контролировать работоспособность всех программных модулей и интерфейсов ИС, а также использовать минимальный тестовый набор инструментов для проверки.

4.2.7.6. Модуль «Help»

Модуль предназначен для размещения подсказок и справочных разделов помощи при работе с системой. Пользователь должен в любой момент иметь возможность получить исчерпывающую информацию о том, какие данные вносить, какие требования предъявляются к вводимым данным, какие регламенты проставления апостиля и другое.

4.2.7.7. Модуль уведомлений

В модуле уведомлений генерируются все основные типы уведомлений пользователям.

Для заявителей:

- Изменение статуса заявки/документа в процессе рассмотрения;
- Завершение рассмотрения заявки.

Для ведомств:

- Поступление заявок;
- По приближению завершения срока истечения используемой сигнатуры.

4.2.8. Модуль запроса информации об Апостиле

Модуль предназначен для доступа внешних партнеров, заинтересованных лиц для проверки статуса Апостиля (актуальности и подлинности) и основных реквизитов выданного апостиля, а также скан-версии документов.

Организация или любой заинтересованный пользователь, как в РУз, так и за ее пределами, желающий проверить Апостиль по QR-коду, передает запрос через специальную

форму Apostille check. Запрос направляется в «E-register», откуда возвращается ответ. При проверке по QR-коду должна выдаваться вся информация и реквизиты запрашиваемого Апостиля. Модуль также должен позволять проверить Апостиль по введенному номеру и дате выдачи.

Параметры апостиля, необходимые для отображения при проверке подлинности, приведены в разделе 4.2.4.4. настоящего Технического задания.

4.2.9. Модуль интеграции

Модуль предусматривает организацию взаимодействия с внешними системами согласно утвержденным технологическим инструкциям.

Предусмотреть возможность расширения системы в дальнейшем для взаимодействия с другими информационными системами в части получения/обмена информацией.

На первом этапе подразумевается интеграция с ЕПИГУ для авторизации в системе через Единый портал, а также возможность выгрузки и просмотра готовых апостилированных документов в Едином портале.

Интеграция с внешними системами подразумевает получение персональных данных юридических и физических лиц. На первом этапе подразумевается интеграция с ЕПИГУ, ГЦП (БДФЛ, БДЮЛ, получение персональных данных), МВД (данные о регистрации физических лиц), ГНК (получение данных юридических лиц), с СМС-шлюзом для отправки уведомлений пользователям, платежными системами.

4.2.10. Модуль проведения оплаты

Для подачи заявки на получение услуги проставления электронного апостиля, пользователь должен оплатить государственную пошлину за рассмотрение. Для этого необходимо организовать интеграцию с платежными сервисами, чтобы пользователь смог оплатить заявку онлайн.

Стоимость заявки формируется исходя из тарифа за услугу рассмотрения. Заявка может включать в себя несколько документов, направляемых в одно ведомство.

ИС должна взаимодействовать с платежными системами и получать от них информацию во внутренний биллинг.

Биллинг должен сопоставлять проведенные оплаты с учетными записями, по которым они проводились, а также заявками, за которые оплаты были внесены, фиксировать даты оплаты и выдавать данные по запросу для персонального кабинета пользователя и контролирующих ведомств.

Интеграция с платежными системами осуществляется по согласованным

технологическим инструкциям и выделяемым API.

Предполагается получение следующих данных:

- Дата оплаты;
- Учетная запись для оплаты;
- Оплаченная сумма.

Аналитика данных об оплате должна производиться на стороне ИС в модуле оплат.

4.3. Требования к видам обеспечения

4.3.1. Требования к математическому обеспечению

Описание и содержание алгоритмов, исполняемых в ИС, определяется в процессе разработки программного обеспечения.

4.3.2. Требования к информационному обеспечению

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

Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД. Средства СУБД, а также средства используемых операционных систем должны обеспечивать документирование и протоколирование обрабатываемой в системе информации. Структура базы данных должна поддерживать кодирование хранимой и обрабатываемой информации. Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации.

Средства СУБД, а также средства используемых операционных систем, сервера приложений и веб-сервера должны обеспечивать документирование и протоколирование (логирование) циркулирующей в Системе информации, защиту данных от разрушений при авариях и сбоях в электропитании Системы, контроль, хранение, обновление и восстановление данных. Информационное наполнение Системы (данные E-register) создается в процессе ее эксплуатации, за исключением ограниченного количества первоначальных данных, загружаемых при подготовке Системы к опытной эксплуатации.

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

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

Резервное копирование данных должно осуществляться на регулярной основе, в

объёмах, достаточных для восстановления информации в подсистеме хранения данных.

4.3.3. Требования к лингвистическому обеспечению

При разработке ИС должны быть использованы языки программирования высокого уровня, применяющиеся для разработки информационных систем.

Пользовательский интерфейс должен взаимодействовать с конечным пользователем ИС на трех языках: узбекском (латиница и кириллица), русском и английском.

При смене языковой версии ИС, пользователь должен остаться на исходной странице, автоматически не перемещаясь на главную.

4.3.4. Требования к программному обеспечению

Прикладное программное обеспечение должно отвечать следующим требованиям:

- высокая степень готовности для решения поставленных задач;
- совместимость программных продуктов в части используемых технических средств, системного ПО и общесистемной инфраструктуры в пределах требований к техническому обеспечению, а также их информационная совместимость в пределах требований к информационному обмену.

ПО должно быть разработано с учетом технологии, обеспечивать реализацию всех функций системы и решение всех поставленных задач для каждого АРМ.

Пользовательский интерфейс «человек—машина» для данной ИС должен осуществляться при помощи АРМ оператора.

АРМ оператора должно предлагать оператору стандартную операционную оболочку пользователя. Оператору должен быть обеспечен быстрый доступ к необходимой информации. В случае возникновения ошибки при обработке данных, система должна известить об этом оператора немедленно.

ПО должно быть построено в виде программных модулей, унифицированных для каждого рабочего места. При этом задачи, которые не нужны для данного АРМ должны быть неактивны, либо добавляться в оболочку ПО. Все модули должны обмениваться информацией в полном объеме без ущерба для всей системы.

Доступ к информации должен осуществляться своевременно, представляться в виде таблиц, отчетов, форм, соответствующих главных и контекстных меню. Данные должны передаваться по сети без ущерба для функционирования всей системы. ПО системы должно иметь возможность создания, ведения, использования справочников.

4.3.5. Требования к техническому обеспечению

Состав оборудования и минимальные требования к параметрам оборудования для

реализации данного проекта, предоставлены ниже.

№ п/п	Сведения о необходимых функциональных характеристиках	Требуемое значение
1	**2**	**3**
1.	Сервер приложения - 1 шт.	
1.1.	Комплект с направляющими для монтажа в 19" стойку	Наличие обязательно
1.2.	Количество поддерживаемых процессоров, не менее	2
1.3.	Количество установленных процессоров, не менее	2
1.4.	Тактовая частота процессора, не менее	2.5 GHz
1.5.	Общий объем L3 памяти процессора, не менее	27,5 Mb
1.6.	Количество физических ядер не менее	20
1.7.	Количество логических ядер: не менее	40
1.8.	Динамическое высвобождение сбойных модулей памяти (ECC)	Наличие обязательно
1.9.	Количество DIMM слотов не менее	24
1.10.	Тип оперативной памяти	DDR4-2933
1.11.	Объем оперативной памяти, не менее	512 GB
1.12.	Максимальный объем наращивания оперативной памяти, не менее	6144 GB
1.13.	Использование технологии для коррекции ошибок	Наличие обязательно
1.14.	Тип шины ввода/вывода	PCIe
1.15.	Количество слотов ввода/вывода PCIe, до	6
1.16.	Сетевой адаптер 10 Гбит/с 2-портами SFP+, не менее	1
1.17.	Сетевой адаптер 1 Гбит/с, не менее	4
1.18.	Сетевой адаптер FC 16 Гбит/с 2-портами, не менее	1
1.19.	Поддержка технологии Infiniband	Наличие обязательно
1.20.	USB 3.0 не менее	5
1.21.	Serial порт не менее	1
1.22.	Micro SD slot не менее	1
1.23.	Тип внутренних HDD дисков	HDD SAS 10K 12Gbps 2.5in
1.24.	Количество внутренних HDD дисков с объемом не менее 1.2TB не менее	2
1.25.	«Горячая» замена дисков	Наличие обязательно
1.26.	RAID контроллер	PCI-E 3.0 Raid controller с поддержкой SAS 12 Гбит/с на линию
1.27.	RAID контроллер должен поддерживать RAID	0, 1, 5, 6, 10, 50, 60
1.28.	Количество блоков питания не менее 500 Вт не менее	2
1.29.	Резервирование блоков питания и вентиляторов	N + 1
1.30.	«Горячая» замена блоков питания и вентиляторов	Наличие обязательно
2.	Сервер базы данных - шт.	
2.1.	Комплект с направляющими для монтажа в 19" стойку	Наличие обязательно

№ п/п	Сведения о необходимых функциональных характеристиках	Требуемое значение
1	2	3
2.2.	Количество процессоров, не менее	2
2.3.	Тактовая частота процессора, не менее	3.6 GHz
2.4.	Общий объем L3 памяти процессора, не менее	24,75 Mb
2.5.	Количество физических ядер не менее	20
2.6.	Количество логических ядер: не менее	40
2.7.	Динамическое высвобождение сбойных модулей памяти (ECC)	Наличие обязательно
2.8.	Количество DIMM слотов не менее	24
2.9.	Тип оперативной памяти	DDR4-2933
2.10.	Объем оперативной памяти, не менее	512 GB
2.11.	Максимальный объем наращивания оперативной памяти, не менее	6144 GB
2.12.	Использование технологии для коррекции ошибок	Наличие обязательно
2.13.	Тип шины ввода/вывода	PCIe
2.14.	Количество слотов ввода/вывода PCIe, до	6
2.15.	Сетевой адаптер 10 Гбит/с 2-портами SFP+, не менее	1
2.16.	Сетевой адаптер 1 Гбит/с, не менее	4
2.17.	Сетевой адаптер FC 16 Гбит/с 2-портами, не менее	1
2.18.	Поддержка технологии Infiniband	Наличие обязательно
2.19.	USB 3.0 не менее	5
2.20.	Serial порт не менее	1
2.21.	Micro SD slot не менее	1
2.22.	Тип внутренних SSD дисков	SSD SAS Mixed Use 12Gbps 2.5in
2.23.	Количество внутренних SSD дисков с объемом не менее 400 ГБ не менее	2
2.24.	RAID контроллер	PCI-E 3.0 Raid controller с поддержкой SAS 12 Гбит/с на линию
2.25.	RAID контроллер должен поддерживать RAID	0, 1, 5, 6, 10, 50, 60
2.26.	«Горячая» замена дисков	Наличие обязательно
2.27.	Количество блоков питания не менее 800 Вт не менее	2
2.28.	Резервирование блоков питания и вентиляторов	N + 1
2.29.	«Горячая» замена блоков питания и вентиляторов	Наличие обязательно

Требования к системе хранения данных

Кэш память должна быть задействована под контроль информации и хранение критически важных данных.

Аппаратная платформа должна поддерживать носители SSD с объемом

920/1920/3840/7680/15360 Гбайт, жесткие диски с объемом 2/4/6/8 Тбайт. Платформа должна поддерживать функционал репликации zero PRO встроенный контролер iSCSI/FCoE (SAS).

Необходима поддержка функционала SAN, функционала дедупликации, функционала автоматической настройки SAN, функционала зонирования SAN хранилища, функционала переноса данных между несколькими массивами, поддержка двух типов SAS хранилища (SFF, LFF), функционала миграции данных.

Должно быть предусмотрено наличие не менее двух контроллеров для повышенной надежности RAID 1, RAID5 и RAID6. Поддержка интеллектуального размещения данных по средствам анализа узких мест в системе хранения данных.

Требования к аппаратной части:

№ п/п	**Сведения о необходимых функциональных характеристиках**	**Требуемое значение**
1	**2**	**3**
1.	Система хранения данных - шт.	
1.1.	Тип устройства	Монтируемый в серверный шкаф
1.2.	Унифицированное хранилище	Предлагаемый СХД должен быть унифицированным хранилищем с одним микрокодом / операционной системой;
1.3.	Поддерживаемые операционные системы	СХД должно поддерживать следующие операционные системы: Windows Server 2016, Windows Server 2019, VMware, Solaris, HPE-UX, IBM-AIX и Linux
1.4.	Дисковое пространство	СХД должен иметь емкость не менее 288ТБ с использованием дисков не более 8ТБ (не менее 7,2 тыс. об/мин) и емкость не менее 7,36ТБ SSD с использованием дисков не более 920ГБ; Предлагаемый СХД должен поддерживать не менее 240 дисков SAS и 120 накопителей SSD.
1.5.	Поддерживаемые жесткие диски	Предлагаемый СХД должен поддерживать двухпортовые жесткие диски Enterprise SAS на 300/600/1200/1800 ГБ с возможностью горячей замены, а также жесткие диски SATA на 2ТБ / 4ТБ / 6ТБ / 8ТБ; Предлагаемый СХД должен поддерживать SSD-накопители емкостью более 6 ТБ.
1.6.	Кэш	СХД должен быть предоставлен с минимальным объемом 64 ГБ в одном блоке; Кэш должен использоваться только для данных и управления. Накладные расходы ОС не должны выполняться

№ п/п	Сведения о необходимых функциональных характеристиках	Требуемое значение
1	2	3
		внутри кеша; Предлагаемый СХД также должен иметь возможность с дополнительной поддержкой Flash Cache с использованием накопителей SSD. Обе файловые службы, а также операции Блока должны иметь возможность использовать флэш-кеш. Рекомендуемая поддержка не менее 800 ГБ флэш-кеша; Если Flash-кеш не поддерживается внутри СХД, поставщик должен гарантировать, что предлагаемый СХД может быть масштабирован до минимума 128 ГБ DRAM без замены или обновления контроллеров.
1.7.	Вычислительная мощность	Предлагаемая архитектура хранения должна основываться на специально построенном двигателе ASIC, XOR, чтобы не было нагрузки на процессор хранения во время расчетов Raid Parity; В случае, если поставщик не имеет функциональных возможностей ASIC, тогда для каждой контрольной пары должен быть предоставлен дополнительный кеш чтения и записи на 16 ГБ, чтобы сбалансировать производительность.
1.8.	Архитектура	Контроллеры должны работать в режиме Active-Active, чтобы один логический блок можно было распределять между всеми контроллерами симметричным образом, с поддержкой всех основных функций, таких как Thin Provisioning, Data Tiering и т.д.
1.9.	Точки отказа	Предлагаемая СХД должен быть сконфигурирован в конфигурации No Single Point (нет точек отказа), включая плату контроллера, кэш, вентиляторов, источник питания и т.д.
1.10.	Поддержка RAID и виртуализация	Предлагаемая СХД должна поддерживать уровни RAID 1, 5 и 6; Предлагаемая СХД должна иметь встроенную поддержку виртуализации, чтобы RAID 1, 5 и 6 можно было вырезать из логического пространства, а не выделять отдельные физические диски для каждого приложения; Каждый поставляемый диск должен иметь возможность одновременно участвовать в нескольких и разных RAID.
1.11.	Защита данных	В случае сбоя питания, СХД должен иметь функцию de-stage, чтобы избежать потери данных.

№ п/п	Сведения о необходимых функциональных характеристиках	Требуемое значение
1	2	3
1.12.	Протоколы	Предлагаемая СХД должна поддерживать все известные протоколы, такие как FC, ISCSI, FCOE, SMB 3.0, NFS V4, FTP / FTPS и т.д.
1.13.	Host порты и Backend порты	Предлагаемая СХД должна иметь не менее 12 хост-портов для подключения к серверам со скоростью 16 Гбит/сек; Предлагаемая СХД должна поддерживать дополнительные IP- порты не менее 4 портов 10 Гбит/сек или не менее 8 х 1 Гбит/сек для операций файловых служб; Предлагаемая СХД должна иметь не менее 2 дополнительных IP-порта для репликации на между СХД; Предлагаемая СХД должна иметь не менее 16 SAS Back-end линий, работающих на скорости не менее 12 Гбит/сек на каждую линию.
1.14.	Производительность и QoS (качество обслуживания)	Предлагаемая СХД должна иметь возможность объединять в группу или RAID не менее 30 жестких дисков для лучшей производительности; Предлагаемая СХД должна поддерживать качество обслуживания для критически важных приложений, чтобы для логических единиц приложения в хранилище можно было определить соответствующее время отклика. Должна быть предусмотрена возможность определения разного времени обслуживания / ответа для различных логических единиц приложения; Механизм качества обслуживания должен позволять определять минимальную и максимальную пропускную способность для требуемых IOPS / пропускной способности для заданных логических единиц приложения, работающих в СХД; Должно быть возможно изменить качество обслуживания. Время отклика (как в миллисекундах, так и в субмиллисекундах), IOPS, спецификация пропускной способности в реальном времени.
1.15.	Provisioning и распределение пространства	Предлагаемая СХД должна поддерживать режимы использования ресурсов «Thin Provisioning» и «Thin Reclamation» для поддержания виртуального диска «тонким» в течение продолжительного периода времени в процессе функционирования;

№ п/п	Сведения о необходимых функциональных характеристиках	Требуемое значение
1	2	3
		Режим «Thin Reclamation», возвращение удаляемых (обнуляемых, как принято в индустрии) блоков в пул свободного пространства, в пределах подсистемы хранения данных должен быть автоматизированным; Операции «Thin Reclamation» не должны приводить к значительной загрузке центрального процессора системы хранения данных и должны обеспечивать возвращение блоков в пул свободного пространства даже в момент пиковых нагрузок на массив без значительного влияния на его производительность; Для простоты управления, функционал «Thin Provisioning» должен быть изначально интегрирован в архитектуру массива, без необходимости выделения отдельных пулов емкости для этого функционала. Система должна поддерживать возможность миграции с толстых томов извне массива на тонкие тома на массиве. Система должна поддерживать конвертирование толстых томов в тонкие и обратно на массиве.
1.16.	Техническое обслуживание	Предлагаемая СХД должна поддерживать онлайн (без прерывания) обновление прошивки, как для контроллера, так и для «жестких» дисков.
1.17.	Снимок (snapshot), копирование, клонирование (clone)	Предлагаемая СХД должна обладать функционалом «мгновенных снимков» (Snapshot) а также поддерживать возможность «полных копий» (Clone); СХД должна поддерживать на базе контроллеров функционал мгновенных снимков на основе указателей (как минимум 512 копий с поддержкой чтения и записи); Массив должен поддерживать возврат в пул свободного пространства емкости удаленных мгновенных снимков с тонким выделением ресурсов. Производитель должен обеспечить 20% дополнительного дискового пространства в случае, если указанный функционал не поддерживается.
1.18.	Управляющее программное обеспечение	Предлагаемая СХД должна поставляться с программным обеспечением для мониторинга производительности массива в режиме реального времени через графический интерфейс пользователя.

№ п/п	Сведения о необходимых функциональных характеристиках	Требуемое значение
1	2	3
1.19.	Storage Tiering	Предлагаемая СХД должна поддерживать фоновую миграцию виртуального тома с одного типа набора RAID на другой тип без прерывания обслуживания приложения, использующего указанный ресурс; Для эффективного многоуровневого хранения данных система хранения должна поддерживать автоматическую миграцию данных на основе политик с одного уровня на другой, включая перемещение блоков данных по типам дисков (уровням) в пределах одного логического тома, между тремя уровнями. В качестве уровней хранения заказчик должен иметь возможность использовать не только носители разного типа, но и одного типа с разными уровнями RAID и размером.
1.20.	Удаленная репликация	Система хранения данных должна поддерживать функционал репликации данных на уровне контроллеров в пределах всего модельного ряда семейства предлагаемого массива; Система хранения данных должна поддерживаться схема одновременной синхронной и асинхронной репликации, для поддержки одного резерва в пределах города (до 10 км), а второго на значительном удалении (более 100км).

Закупка, поставка, настройка данного оборудования не входят в состав настоящего Технического задания и предоставляются Заказчиком.

4.3.6. Требования к метрологическому обеспечению

Требования к метрологическому обеспечению будут определяться в зависимости от используемого оборудования, и предъявляться к оборудованию и прочим техническим средствам.

4.3.7. Требования к организационному обеспечению

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

Должны быть определены должностные лица, ответственные за:

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

К работе с ИС должны допускаться работники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации, техники безопасности и прошедшие обучение работе с ИС.

Необходимы обязательные инструктажи пользователей, в том числе по технике безопасности, перед началом работы с ИС (и/или) подсистемами.

4.3.8. Требования к методическому обеспечению

ИС должна разрабатываться на основании действующих нормативных правовых актов и организационно-распорядительных документов заказчика. Следовательно, в рамках разработки данной ИС, должны быть учтены соответствующие административные регламенты заказчика, в которых должны быть определены процессы деятельности и функции подразделений, а также сотрудников объектов заказчика, их права, обязанности и ответственности по использованию данной системы. Также, должны быть утверждены в установленном порядке инструкции выполнения пользователями операций в работе с Системой. Состав методического обеспечения будет уточняться в процессе разработки ПО и согласовывается с Заказчиком. Методическое обеспечение предоставляется по требованию Разработчика и состоит из:

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

5. Состав и содержание работ по созданию ИС

Этапы создания ИС представлены в Таблице ниже.

№ этапа	Наименование работ и их содержание	Сроки выполнения		Разработчик (организация, предприятие)	Результат завершения этапа
		начало	окончание		
1.	Разработка Технического задания	03.21	05.21	ПРООН	Разработано Техническое задание

№ этапа	Наименование работ и их содержание	Сроки выполнения		Разработчик (организация, предприятие)	Результат завершения этапа
		начало	окончание		
2.	Прохождение экспертизы Технического задания в ГУП «Центр управления проектами электронного правительства» Министерства информационных технологий и коммуникаций Республики Узбекистан	05.21.	05.21	Заказчик, ГУП «Центр управления проектами электронного правительства» Министерства информационных технологий и коммуникаций Республики Узбекистан	Экспертные заключения получены. ТЗ утверждено
3.	Прохождение экспертизы Технического задания в ГУП «Центр кибербезопасности» при Службе национальной безопасности РУз	05.21.	06.21.	Заказчик, ГУП «Центр кибербезопасности»	Экспертные заключения получены. ТЗ утверждено
4.	Заключение Договора	07.21	07.21	ПРООН, Разработчик	Заключен договор на разработку ИС
5.	Разработка	07.21	09.21	Разработчик	Демонстрация функционала ИС в соответствии с Техническим заданием
6.	Тестирование	10.21	10.21	Разработчик, Заказчик	
7.	Составление эксплуатационной документации	10.21	10.21	Разработчик	Подготовлена эксплуатационная

№ этапа	Наименование работ и их содержание	Сроки выполнения		Разработчик (организация, предприятие)	Результат завершения этапа
		начало	окончание		
					документация
8.	Экспертиза программного продукта на соответствие Техническому заданию в ГУП «Центр управления проектами электронного правительства» Министерства информационных технологий и коммуникаций Республики Узбекистан	10.21	10.21	Заказчик, ГУП «Центр управления проектами электронного правительства» Министерства информационных технологий и коммуникаций Республики Узбекистан	Экспертные заключения получены.
9.	Экспертиза программного продукта на соответствие требованиям безопасности в ГУП «Центр кибербезопасности» при Службе государственной безопасности Республики Узбекистан	10.21	10.21	Заказчик, ГУП «Центр кибербезопасности» при Службе государственной безопасности Республики Узбекистан	Экспертные заключения получены.
10.	Проведение тренингов	10.21	10.21	Заказчик, Разработчик	Проведено обучение
11.	Введение программного обеспечения в эксплуатацию	11.21	11.21	Заказчик, Разработчик	Акт выполненных работ, Акт ввода ИС в эксплуатацию

Заказчик должен обеспечить создание условий функционирования объекта

автоматизации, при которых гарантируется соответствие создаваемой ИС требованиям, содержащимся в ТЗ, а именно:

- приведение поступающей в ИС информации к виду, пригодному для обработки с помощью программно-технических средств (в соответствии с требованиями к информационному и лингвистическому обеспечению);
- проведение необходимых изменений в объекте автоматизации;
- создание условий функционирования объекта автоматизации, при которых гарантируется соответствие создаваемой ИС требованиям, содержащимся в настоящем Техническом задании;
- создание необходимых для функционирования ИС подразделений и служб в организационной структуре Заказчика;
- сроки и порядок комплектования штата и обучения персонала.

При внесении изменений в ИС должны выполняться следующие требования:

- все изменения должны документироваться;
- должна поддерживаться совместимость версий.

6. Порядок контроля и приемки ИС

В ходе сдачи-приемки проекта, проводятся следующие виды работ:

- Заключительные испытания ИС;
- устранение недостатков;
- приемочные испытания ИС.

Проверка и приемка информационной ИС проводятся на территории нахождения объектов использования продукта. Условие проведения приемки системы – ИС должна быть подготовлена на условиях «под ключ».

Испытания ИС проводятся с целью проверки соответствия реализации требований ТЗ, работоспособности ПО, а также проверки комплектности ПО и документации к техническим и программным средствам. Приемочная комиссия формируется из числа представителей организаций, вовлеченных в реализацию проекта. Работы по реализации проекта считаются завершенными после подписания сторонами акта приемки в эксплуатацию.

7. Требования к составу и содержанию работ по подготовке ИС к вводу в действие

7.1. Технические мероприятия

В процессе создания ИС необходимо выполнить следующий комплекс работ по подготовке систем к вводу в действие:

- разработать ПО, необходимое для запуска ИС в опытную эксплуатацию, а также эксплуатационную документацию;
- провести обучение персонала работе с ИС;
- обеспечить подготовку производственных площадей для размещения комплекса технических средств;
- определить ответственных лиц за внедрение ИС на объектах;
- подготовить необходимые организационно-распорядительные документы, регламентирующие порядок работы персонала в условиях функционирования ИС.

Комплектование штатов и подразделений, необходимых для функционирования системы, а также подготовка их сотрудников должны быть завершены до начала опытной эксплуатации систем.

7.2. Приведение поступающей в ИС информации к виду, пригодному для обработки

Информация в Систему вводится пользователем через заполнение интерактивных web- форм, каждое поле которых предназначено для ввода данных в конкретном формате, правильность заполнения при этом должна проверятся перед сохранением данных в ИС.

7.3. Изменения, которые необходимо осуществить в объекте автоматизации

В рамках внедрения ИС Заказчику требуется создание (либо соответствующее изменение) специализированного структурного подразделения (отдела) объекта автоматизации, отвечающего за администрирование и техническую поддержку ИС. В состав изменений в объекте автоматизации должны быть включены:

- выделение и подготовка специального помещения для размещения аппаратных компонентов ИС, отвечающего требованиям, приводимым в настоящем Техническом задании;
- установка и настройка лицензионного ПО, необходимого для функционирования ИС, в соответствии с требованиями к программному обеспечению, приводимыми в настоящем Техническом задании;
- установка и настройка разработанных компонентов ИС;
- подбор персонала для вновь создаваемого подразделения объекта автоматизации, отвечающего за администрирование и техническую поддержку ИС;
- обучение пользователей ИС.

7.4. Создание условий функционирования объекта автоматизации

Необходимо обеспечить выполнение требований к условиям эксплуатации объекта автоматизации и характеристикам окружающей среды, указанным в настоящем подразделе.

Помимо этого, для обеспечения соответствия создаваемой ИС требованиям к моменту сдачи в эксплуатацию Заказчиком должны быть выполнены требования к техническому обеспечению ИС, а пользователи системы должны пройти обучение по работе с ней.

7.5. Создание необходимых для функционирования ИС подразделений и служб

К моменту передачи ИС в эксплуатацию должна быть создана служба эксплуатации системы, в которую входят системные Администраторы и информационные Администраторы. Сотрудники службы эксплуатации должны пройти необходимое обучение.

7.6. Обучение персонала

До сдачи ПО в эксплуатацию Разработчик обязан подготовить Руководство пользователя и Руководство Администратора, а также провести обучение (тренинг) сотрудников Заказчика по работе в Системе и техническому сопровождению на основе данной документации.

7.7. Гарантийное обслуживание

Перевод ИС на гарантийное обслуживание происходит после подписания акта выполненных работ по настоящему Техническому заданию. Предусматривается гарантийное обслуживание ИС сроком на 12 (двенадцать) месяцев.

Гарантийное обслуживание включает в себя:

- Исправление ошибок, возникших при работе ИС, в рамках разработанного функционала, утвержденного настоящим Техническим заданием,
- Консультации технических специалистов Заказчика по настройке ИС, по вопросам, не освещенным в технической документации, предоставленной по текущему проекту,
- Консультации операторов по вопросам работы в ИС, если ответы на эти вопросы отсутствуют в разработанной и предоставленной документации по текущему вопросу.

Гарантийное обслуживание не включает в себя:

- Выполнение работ по совершенствованию функционала ИС не предусмотренное настоящим Техническим заданием,
- Все дополнительные требования по функциональным возможностям, архитектуре базы данных, дизайну, обучению новых пользователей, и прочим вопросам не

предусмотренные текущим Техническим Заданием, реализуются в рамках новых Договоров.

Для создания условий функционирования ИС, при которых гарантируется соответствие создаваемой системы требованиям, содержащимся в настоящем техническом задании, и возможность её эффективного использования, в организации Заказчика должен быть проведен комплекс мероприятий.

8. Требования к документированию

В состав технической документации, разрабатываемой при доработке компонентов ИС, должны входить следующие документы:

- Спецификация;
- Текст программного кода ИС (в электронном виде);
- Инструкция по установке ИС (в составе Руководства Администратора ИС);
- Общее описание разработанной ИС;
- Программа и методика испытаний разработанной ИС;
- Руководство пользователя разработанной ИС;
- Руководство Администратора разработанной ИС.

Руководство пользователя должно содержать описание принципов и функций ИС, а также способов работы на автоматизированных рабочих местах оператора.

Руководство Администратора должно включать:

1. Инструкции по разворачиванию системы;
2. Описание принципов организации системы (на уровне Администратора);
3. Описание способов работы;
4. Описание способов ведения справочников в базе данных системы.

По соглашению сторон и в связи с проведением обучения специалистов Заказчика специалистами Разработчика для эксплуатации системы в различных режимах ее функционирования, а также в случае заключения договора сопровождения системы, состав документации может быть ограничен настоящим Техническим заданием (определить Договором на создание ИС).

Вся документация должна предоставляться Заказчику в 2-х экземплярах на бумажном и электронном (компакт-диск, флеш) носителях. Документы на электронном носителе должны предоставляться в формате MicrosoftWord 97-2016. ИС должна передаваться Заказчику на электронных носителях (компакт-диск и флеш) в двух копиях.

Комплекты документации должны быть предоставлены на русском языке (допускается

использование английского языка в тех местах, где его присутствие необходимо).

9. Источники

1. O'zDSt 1985:2018 «Информационные технологии. 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».

Приложение А

Информационной системы электронного апостиля и электронного реестра заверенных документов «E-App» и «E-Register».

Наименование предприятия	Адрес
ГУП «Центр управления проектами электронного правительства» Министерства информационных технологий и коммуникаций Республики Узбекистан	г. Ташкент, ул. Амир Темур шоҳ, 4 Телефон: (+998 71) 238-41-07
ГУП «Центр кибербезопасности»	г. Ташкент, ул. Кирк-киз, 10а Телефон: (+998 71) 203-55-11