

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ, СОКРАЩЕНИЙ И ТЕРМИНОВ

КРІ	Key Performance Indicator – ключевой показатель эффективности, отражающий реальные количественные показатели достижения целей
ДЗО	Дочерние зависимые организации
ЭДО	Электронный документооборот
Check-in визит	Посещение web-сайта клиентом с прохождением регистрации;
Оmnikanальны е коммуникации	Это использование множества каналов связи с клиентами, объединенных одной системой, с целью создания непрерывности процесса и единой точки сбора и хранения информации о коммуникациях
Ключевой пользователь	Сотрудник Заказчика, обладающий максимальными компетенциями во внутренних процессах Заказчика, имеющий достаточный опыт и знания для последующей передачи знаний и поддержки пользователей
КЦ	Контактный центр Заказчика
SOA	Service Oriented Architecture
IP	Internet Protocol – Маршрутизируемый сетевой протокол
VPN	Virtual Private Network – виртуальная частная сеть
DMZ	Demilitarized Zone - сегмент сети
RH	Руководящий документ
O'zDSt	Государственный стандарт Республики Узбекистан
APM	Автоматизированное рабочее место
АС	Автоматизированная система
АСУ ТП	Автоматизированная система управления технологическим процессом
БД	База данных
ГОСТ	Государственный стандарт
ИКТ	Информационно-коммуникационные технологии
ИСО/МЭК (ISO/IEC)	Международный стандарт
КТС	Комплекс технических средств
ЛВС	Локально-вычислительная сеть
ОС	Операционная система

ПК	Персональный компьютер
ИБ	Информационная безопасность
ИТ	Информационные технологии
ИС	Информационная система
КС	Корпоративная сеть
КСПД	Мультисервисная защищённая корпоративная сеть передачи данных, которая представляет собой определённый состав взаимодействующего сетевого оборудования (маршрутизатор, крипто-шлюз, коммутатор, межсетевой экран), обеспечивающего передачу данных по каналам связи между узлами
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПМИ	Программа и методика испытаний
СПД	Система передачи данных
ТЗ	Техническое задание
ТУ	Технические условия
ТТ	Технические требования

СОДЕРЖАНИЕ

1.	ОБЩИЕ СВЕДЕНИЯ.....	6
1.1.	Полное наименование информационной системы и его условное обозначение.....	6
1.2.	Заказчик	6
1.3.	Исполнитель	6
1.4.	Основание для разработки	6
1.5.	Плановые сроки начала и окончания работ.....	6
1.6.	Источники финансирования.....	6
1.7.	Порядок оформления и предъявления результатов работ.....	6
2.	НАЗНАЧЕНИЕ СИСТЕМЫ И ЦЕЛИ РЕАЛИЗАЦИИ ПРОЕКТА	7
2.1.	Назначение системы	7
2.2.	Цели реализации проекта	7
3.	ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	8
3.1.	Общие сведения	8
4.	ТРЕБОВАНИЯ К СИСТЕМЕ И ИСПОЛНИТЕЛЮ.....	11
4.1.	Требования к системе и исполнителю в целом	11
4.1.1.	Требования к структуре и функционированию системы	11
4.1.2.	Основные функциональные принципы, заложенные в системе	12
4.1.3.	Перечень подсистем, их назначение и основные характеристики	13
4.1.4.	Требования к характеристикам взаимосвязей создаваемой системы со смежными системами, требования к совместимости, способам обмена информацией.....	13
4.1.1.	• И другие.Требования к режимам функционирования системы	13
4.1.2.	Перспективы развития, модернизации системы	14
4.1.3.	Перечень и описание сценариев использования ИС.....	15
4.1.4.	Требования к диагностированию системы	15
4.1.5.	Требования к численности и квалификации персонала системы и режиму его работы	15
4.1.6.	Требования к численности персонала (пользователей) ИС	15
4.1.7.	Требования к квалификации персонала, порядку его подготовки и контроля знаний и навыков..	15
4.1.8.	Требуемый режим работы персонала ИС	15
4.1.9.	Показатели назначения.....	16
4.1.10.	Требования к надежности	18
4.1.11.	Требования к безопасности.....	19
4.1.12.	Требования к защите информации от несанкционированного доступа.....	19
4.1.13.	Требования к разграничению прав доступа.....	20
4.1.14.	Требования по сохранности информации при авариях	20
4.1.15.	Требования защите от влияния внешнего воздействия	21
4.1.16.	Требования к эргономике и технической эстетике	21
4.1.17.	Требования к транспортабельности	23
4.1.18.	Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы	23
4.1.19.	Требования к патентной и лицензионной чистоте.....	23
4.1.20.	Требования по стандартизации и унификации.....	24
4.2.	Требования к функциям (задачам), выполняемым Информационной Системой	25
4.2.1.	Перечень функций, задач или их комплексов, выполняемых подсистемами	25

Требования к Подсистеме «ХАВФСИЗ ЙУЛ»	25
Ошибки на экране S4. Ввод секретного ключа	36
4.3. Требования к видам обеспечения	38
4.3.1. Требования к математическому обеспечению	38
4.3.2. Требования к информационному обеспечению	38
4.3.3. Требования к лингвистическому обеспечению	39
4.3.4. Требования к программному обеспечению	39
4.3.5. Требования к СУБД	39
4.3.6. Требования к техническому обеспечению	39
4.3.7. Требования к метрологическому обеспечению	39
4.3.8. ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННОМУ ОБЕСПЕЧЕНИЮ	40
4.3.9. Требования к гарантийному обеспечению	40
4.3.10. Обучение пользователей	41
4.3.11. Требования к методическому обеспечению	41
5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО ВВОДУ СИСТЕМЫ	43
6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ	45
7 ТРЕБОВАНИЯ ПО СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ДЕЙСТВИЕ	47
8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ	48
8.1. Проектная документация	48
9 ИСТОЧНИКИ РАЗРАБОТКИ	49

1. ОБЩИЕ СВЕДЕНИЯ

1.1. ПОЛНОЕ НАИМЕНОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ЕГО УСЛОВНОЕ ОБОЗНАЧЕНИЕ

Полное наименование информационной системы: «Разработка мобильного приложения «Безопасная дорога» (далее «Система»).

Условное обозначение ИС: ИС «XAFVSIZ YO'L»

1.2. ЗАКАЗЧИК

Академия Генеральной прокуратуры Республики Узбекистан

Г. Ташкент, 100047 ул. Шахрисабз, 42

ИНН 200838518

ОКЭД 92200

ОПЕРУ Казначейство Министерство Финансов Республики Узбекистан

1.3. ИСПОЛНИТЕЛЬ

Согласно Исполнитель по данному проекту будет определен в установленном порядке.

1.4. ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ

1. Указа Президента Республики Узбекистан УП-6079 от 5 октября 2020 года «Об утверждении стратегии «цифровой Узбекистан-2030»

2. Указ Президента Республики Узбекистан 13 декабря 2018 г. № УП-5598 «О дополнительных мерах по внедрению цифровой экономики, электронного правительства, а также информационных систем в государственном управлении Республики Узбекистан»;

3. Постановление Президента Республики Узбекистан от 03 июля 2018 г. №ПП-3832 «О мерах по развитию цифровой экономики в Республике Узбекистан».

4. 5. Постановление Кабинета Министров Республики Узбекистан от 16.10.2015 года № 295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан».

1.5. ПЛАНОВЫЕ СРОКИ НАЧАЛА И ОКОНЧАНИЯ РАБОТ

Система должна быть реализовано в соответствии с установленными Заказчиком сроками.

1.6. ИСТОЧНИКИ ФИНАНСИРОВАНИЯ

Источником финансирования работ по проекту являются собственные средства Заказчика проекта, средства Бюджетной системы Республики Узбекистан, и другие не запрещенные законодательством финансовые средства.

1.7. ПОРЯДОК ОФОРМЛЕНИЯ И ПРЕДЪЯВЛЕНИЯ РЕЗУЛЬТАТОВ РАБОТ

По завершению отдельных этапов и работы в целом Исполнитель представляет акт сдачи-приемки.

Результаты работ оцениваются приемочной комиссией. Приемочную комиссию в установленном порядке образует Заказчик.

Приемочной комиссии Исполнитель предъявляет документацию, перечень и требования к оформлению которых определяются в соответствии с ГОСТами и иными стандартами, и руководящими документами, действующими на территории Республики Узбекистан, а также по взаимному согласованию Заказчика и Исполнителя.

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

2. НАЗНАЧЕНИЕ СИСТЕМЫ И ЦЕЛИ РЕАЛИЗАЦИИ ПРОЕКТА

2.1. НАЗНАЧЕНИЕ СИСТЕМЫ

Основной целью разрабатываемого мобильного приложения является повышения уровня безопасности дорожного движения, путем

Основными задачами Системы являются:

Регистрация пользователей Системы;

Передача видео данных с пользователей Системы в систему E - Jarima;

Передачи данных из видеорегистраторов в систему E-Jarima;

2.2. ЦЕЛИ РЕАЛИЗАЦИИ ПРОЕКТА

внедрение информационных ресурсов, обеспечивающих:
контроль, в том числе общественный, за формированием и эффективностью использования средств дорожных фондов;
формирование базы данных фото- и видеоматериалов, содержащих зафиксированные гражданами нарушения правил дорожного движения;
общественного мониторинга ситуации на автомобильных дорогах.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1. ОБЩИЕ СВЕДЕНИЯ

В соответствии с задачами, определенными Стратегией действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах, а также в целях создания современной системы подготовки, переподготовки и повышения квалификации кадров органов прокуратуры 8 мая 2018 года Президентом Республики Узбекистан принят Указ «О мерах по коренному совершенствованию системы подготовки, переподготовки и повышения квалификации кадров органов прокуратуры». Согласно Указу, Высшие учебные курсы Генеральной прокуратуры Республики Узбекистан преобразованы в Академию Генеральной прокуратуры Республики Узбекистан.

Академия Генеральной прокуратуры Республики Узбекистан является образовательным и научно-исследовательским учреждением.

Академия в пределах своей компетенции организует деятельность во взаимодействии со структурными подразделениями Генеральной прокуратуры, нижестоящими прокуратурами, Департаментом по борьбе с экономическими преступлениями, Бюро принудительного исполнения, правоохранительными и другими государственными органами, образовательными и научными учреждениями, институтами гражданского общества и общественностью.

Академия осуществляет:

- подготовку, переподготовку и повышение квалификации работников органов прокуратуры, в том числе без отрыва от производства;
- подготовку кадров на бюджетной и платно-контрактной основе, с присвоением степени магистра и выдачей диплома государственного образца;
- профессиональную переподготовку кандидатов на замещение должностей в органах прокуратуры в виде первичной специализации;
- профессиональную переподготовку кадров, состоящих в резерве на замещение руководящих должностей;
- повышение квалификации сотрудников государственных органов и иных организаций по вопросам взаимодействия в сфере профилактики правонарушений и борьбы с преступностью и коррупцией по краткосрочным программам;
- подготовку научных и научно-педагогических кадров высшей квалификации в соответствии с законодательством;
- все виды учебной, методической, научно-исследовательской, информационно-аналитической деятельности, в том числе с привлечением национальных, зарубежных и международных грантов;
- направление профессорско-преподавательского состава, работников и слушателей на стажировку в органы государственной власти, государственного и хозяйственного управления, общественные организации, а также в высшие образовательные и научно-исследовательские учреждения, в том числе зарубежных стран;
- издательскую деятельность.

Программы по подготовке, переподготовке и повышению квалификации кадров в Академии осуществляются в установленном порядке на бюджетной и платно-контрактной основе.

Основной целью Академии является организация эффективной системы подготовки, переподготовки и повышения квалификации работников органов прокуратуры и других кадров, а также проведение фундаментальных и прикладных научных исследований.

Основной целью Академии является организация эффективной системы подготовки, переподготовки и повышения квалификации работников органов прокуратуры и других кадров, а также проведение фундаментальных и прикладных научных исследований.

Основные задачи и направления деятельности:

- организация единой системы подготовки, переподготовки и повышения квалификации работников органов прокуратуры, обеспечивающей развитие и совершенствование их знаний и навыков, в том числе по системному анализу и критическому мышлению, личных и деловых качеств, формирование и укрепление высокого чувства справедливости и ответственности за неукоснительное соблюдение законов, прав и свобод граждан;

- широкое внедрение современных педагогических и информационно-коммуникационных технологий, дистанционного обучения, интерактивных и проблемно-ситуационных методов обучения и тренингов;

- научно-методическое обеспечение деятельности органов прокуратуры, проведение фундаментальных, прикладных и инновационных исследований, реализация на системной основе научно-исследовательских программ и проектов по наиболее актуальным проблемам обеспечения верховенства закона, укрепления законности, защиты прав и свобод граждан, а также субъектов предпринимательства, охраняемых законом интересов общества и государства, профилактики правонарушений, в том числе с привлечением национальных, зарубежных и международных грантов;

- разработка научно обоснованных выводов и рекомендаций по совершенствованию законодательства и формированию единообразной правоприменительной практики;

- подготовка кадров по специальностям магистратуры, основанная на прикладном характере обучения и тесной взаимосвязи с профессиональной деятельностью органов прокуратуры;

- подготовка научных и научно-педагогических кадров высшей квалификации по направлениям деятельности органов прокуратуры;

- повышение квалификации сотрудников государственных органов и иных организаций по вопросам взаимодействия в сфере профилактики правонарушений и борьбы с преступностью и коррупцией;

- обеспечение психологического сопровождения деятельности органов прокуратуры, проведение профессионального психологического отбора кандидатов на службу, изучение морально-психологического климата в органах прокуратуры с выработкой рекомендаций по его улучшению;

- осуществление международного сотрудничества в области проведения совместных научных исследований, обмена информацией нормативно-правового, методического и аналитического характера, привлечения в образовательный процесс зарубежных специалистов, организации на системной основе стажировок педагогических, научных сотрудников и слушателей;

- углубление эффективного межведомственного взаимодействия с образовательными и научно-исследовательскими учреждениями, в том числе зарубежных стран, осуществляющими подготовку, переподготовку и повышение квалификации юридических кадров, в целях обмена опытом, консолидации усилий по повышению качества образовательного процесса;

- привлечение зарубежных высококвалифицированных специалистов для учебной и научно-методической работы, проведение консультаций на контрактной основе, а также заключение договоров и сотрудничество с иностранными образовательными, научно-

исследовательскими организациями в сфере подготовки, переподготовки и повышения квалификации управленческих кадров.

4. ТРЕБОВАНИЯ К СИСТЕМЕ И ИСПОЛНИТЕЛЮ

4.1. ТРЕБОВАНИЯ К СИСТЕМЕ И ИСПОЛНИТЕЛЮ В ЦЕЛОМ

Создаваемая информационная система будет представлять из себя мобильного приложение, разрабатываемая собственными силами.

К целевой Системе предъявляется ряд основополагающих требований:

Система должна иметь интуитивно-понятный пользовательский интерфейс.

Система должна обеспечивать защиту данных и разграничивать данные по уровню доступа пользователей.

Система должна иметь модуль согласования данных и уведомления пользователей.

Система должна интегрироваться с внешними системами.

Система должна иметь модуль отчетности и модуль анализа.

Система должна быть построена в соответствии со следующими основными принципами:

Безопасность;

Стандартизация;

Наблюдаемость;

Достоверность;

Масштабируемость;

4.1.1. ТРЕБОВАНИЯ К СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ

Система должна быть реализована как современное программно-техническое решение.

В техническую структуру проекта входят следующие компоненты:

- Мобильное приложение для Android, iOS;

Мобильное приложение должно быть разработано для платформы Android 4+, iOS15 с применением языков программирования высокого уровня.

Дизайн приложения должен быть адаптивный и работать корректно во всех устройствах Android 4+, iOS 15. В связи с тем, что пользователи определенное время использовали первую версию приложения, интерфейс новой версии приложения должен быть привычно-ассоциируемым.

Интерфейс подключаемых модулей должен быть выполнен в едином стиле с интерфейсом ядра системы и должен обеспечивать возможность прозрачного перемещения администратора между модулями системы и использование одинаковых процедур управления и навигационных элементов для выполнения однотипных операций.

При определении стиля оформления приложения и основного направления, следует использовать концепцию Material design с рекомендациями размеров, отступов, визуальных эффектов, анимации.

Мобильное приложение должно:

- поддерживать возможность работы в портретной ориентации экрана.
- Локализация приложения предусматривать узбекскую (кириллица и латиница) и русскую версию пользовательского интерфейса.
- Версия поддерживаемых Android, iOS
- Разрешения экранов Android, iOS: mdpi (320x480 px), hdpi (480x800px), xhdpi (720x1280px), xxhdpi (768x1280px).

Мобильные приложения для Android и iOS должно реализовываться нативными средствами, либо на основе платформы, обеспечивающей компиляцию в нативные приложения для обеспечения максимальной производительности.

- Версия поддерживаемая iOS 15

В приложении необходимо использовать сервисы геолокации для определения маршрута Серверное приложение:

Необходимо реализовать серверное приложение, обеспечивающее работу мобильных приложений системы. Серверное приложение должно реализовывать REST API для взаимодействия с мобильными приложениями. Формат сериализации данных JSON.

4.1.2. ОСНОВНЫЕ ФУНКЦИОНАЛЬНЫЕ ПРИНЦИПЫ, ЗАЛОЖЕННЫЕ В СИСТЕМЕ

Основные принципы, которыми должен руководствоваться Исполнитель при выборе/проектировании Системы, следующие:

- Данные должны быть доступны сотрудникам в объеме, необходимом и достаточном для выполнения своих функциональных обязанностей;
- Аналитические вычисления должны быть отделены от оперативной обработки данных;
- Необходимо следовать эволюционному подходу, позволяющему обеспечить непрерывность бизнеса и сохранить инвестиции в ИТ;
- Необходимо обеспечить защиту данных и их надежное хранение. Меры по защите информации должны быть адекватны ценности данных.

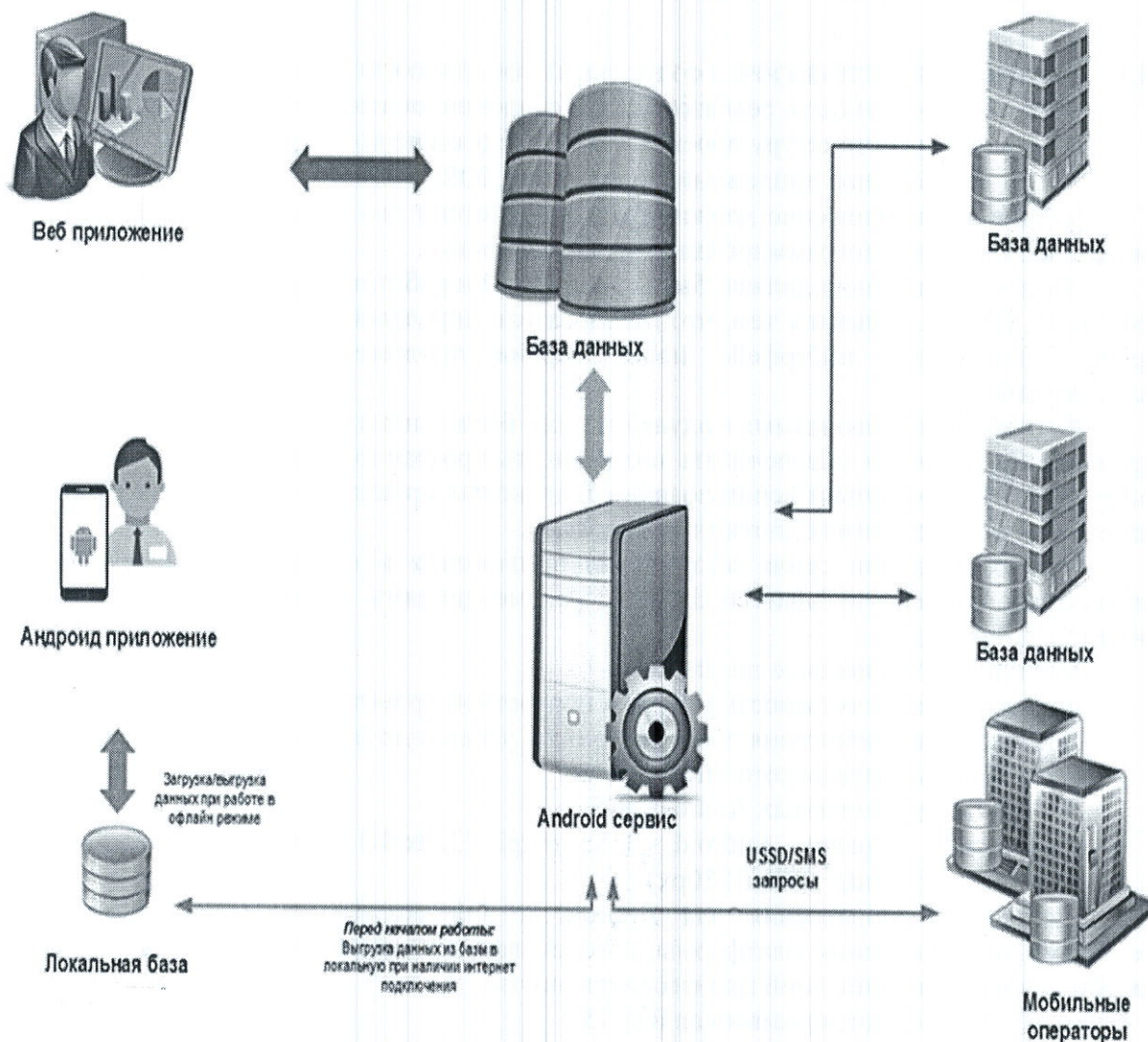


Рис. Архитектура ИС

4.1.3. ПЕРЕЧЕНЬ ПОДСИСТЕМ, ИХ НАЗНАЧЕНИЕ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Функциональные подсистемы:

- ❖ Подсистемы «Хавфсиз йул»

4.1.4. ТРЕБОВАНИЯ К ХАРАКТЕРИСТИКАМ ВЗАИМОСВЯЗЕЙ СОЗДАВАЕМОЙ СИСТЕМЫ СО СМЕЖНЫМИ СИСТЕМАМИ, ТРЕБОВАНИЯ К СОВМЕСТИМОСТИ, СПОСОБАМ ОБМЕНА ИНФОРМАЦИЕЙ

Исполнитель в ходе разработки системы должен предусмотреть интеграцию с внешними аналитическими порталами по общедоступным протоколам таким как:

Интеграционный адаптер рекомендуется реализовывать с использованием следующих технологий:

- файловый обмен – напрямую или через протоколы FTP/SFTP;
- SOAP – Simple Object Access Protocol, протокол обмена структурированными сообщениями в распределённой вычислительной среде;
- ODBC – Open Database Connectivity, программный интерфейс (API) доступа к базам данных;
- JDBC – Java Database Connectivity, платформенно-независимый промышленный стандарт взаимодействия Java-приложений с различными СУБД;
- RPC – Remote Procedure Call, вызов удаленной процедуры;
- RMI – Java Remote Method Invocation, протокол вызова удаленного метода на языке Java для распределенных объектных Java-приложений;
- COM, DCOM – Distributed Component Object Model, распределенная компонентная объектная модель;
- MOM – Messaging Oriented Middleware

4.1.1. • И ДРУГИЕ ТРЕБОВАНИЯ К РЕЖИМАМ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

Система должна функционировать в круглосуточном режиме и обеспечивать возможность работы в следующих режимах:

1. Штатный режим (непрерывная круглосуточная работа):

Штатный режим обеспечивает выполнение функций системы. Это основной режим работы. В штатном режиме функционирования системы:

- клиентское программное обеспечение на рабочих местах пользователей обеспечивает возможность круглосуточного функционирования с регламентированными перерывами на техническое обслуживание и обновление программного обеспечения;
- серверное программное обеспечение, предоставляет возможность круглосуточного функционирования с регламентированными перерывами на техническое обслуживание и обновление программного обеспечения.

Для обеспечения штатного режима функционирования системы необходимо соблюдать требования и выдерживать условия эксплуатации программного обеспечения, указанные в соответствующих технических документах (техническая документация, инструкции по эксплуатации и т.д.).

2. Сервисный режим (для проведения обслуживания, реконфигурации и пополнения новыми компонентами).

Сервисный режим предназначен для обновления и профилактического обслуживания программно-аппаратных средств, изменения конфигурации компонентов.

Сервисный режим функционирования используется для выполнения операций подготовки и проведения регламентов, испытаний или значительной перестройки системы.

В данном режиме система недоступна для пользователей.

В данном режиме также осуществляется техническое обслуживание, реконфигурация, модернизация и совершенствование системы.

Режим позволяет проводить диагностирование инцидентов или проблем, связанных со сбоями или авариями в работе системы.

Сервисный режим предназначен, прежде всего, для проведения регламентных работ и профилактики системы:

- проведение обслуживания комплекса технических средств системы;
- установка обновлений общесистемного и специального программного обеспечения;
- контроль работоспособности компонентов системы;
- выполнение «холодного» резервного копирования базы данных; реконфигурации и замены компонент системы и т.д.).

4.1.2. ПЕРСПЕКТИВЫ РАЗВИТИЯ, МОДЕРНИЗАЦИИ СИСТЕМЫ

Система должна обеспечивать возможность модернизации и развития при необходимости изменения состава требований к выполняемым функциям и видам обеспечения.

Модернизация Системы должна проводиться экспертами в предметной области и прикладными программистами.

Система должна реализовывать возможность дальнейшей модернизации программного обеспечения. Также необходимо предусмотреть возможность увеличения производительности системы путем её масштабирования.

4.1.3. ПЕРЕЧЕНЬ И ОПИСАНИЕ СЦЕНАРИЕВ ИСПОЛЬЗОВАНИЯ ИС

Бизнес-процессы и основные действия пользователей и сторонних ИС (в пределах рассматриваемой ИС), позволяющих достигнуть целей создания Системы предусматривается описать в виде сценариев использования

4.1.4. ТРЕБОВАНИЯ К ДИАГНОСТИРОВАНИЮ СИСТЕМЫ

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

Диагностика программных и технических средств должна быть осуществлена с помощью стандартных режимов системных операционных систем, операционных систем отдельных рабочих станций, а также путем прогона контрольного примера.

Программные модули должны иметь компоненты по методике испытаний и тестирования, позволяющие провести контроль возможности функционирования основных режимов работы модулей.

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

В рамках разработки Программы и методики испытаний должен быть сформирован контрольный пример, обеспечивающий проверку работоспособности узлов и подключения взаимодействующих информационных систем как при первоначальной установке и загрузке базы данных, так и в процессе повседневной работы.

4.1.5. ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ И КВАЛИФИКАЦИИ ПЕРСОНАЛА СИСТЕМЫ И РЕЖИМУ ЕГО РАБОТЫ

4.1.6. ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ ПЕРСОНАЛА (ПОЛЬЗОВАТЕЛЕЙ) ИС

Численность персонала пользователей внедряемых информационных систем определяется Исполнителем на этапе разработки Технического проекта и согласовывается протоколом с Заказчиком. Детальные требования к функциональным группам, составу, численности, квалификации персонала должны быть определены на этапе разработки Технического проекта в соответствии с организационной структурой, определенной на этапе обследования объекта автоматизации.

4.1.7. ТРЕБОВАНИЯ К КВАЛИФИКАЦИИ ПЕРСОНАЛА, ПОРЯДКУ ЕГО ПОДГОТОВКИ И КОНТРОЛЯ ЗНАНИЙ И НАВЫКОВ

Требования к порядку подготовки персонала Системы и контроля знаний и навыков:

- Исполнитель должен обеспечить обучение отдельно ключевых пользователей Системы;
- Для проведения контроля знаний и навыков по работе с Системы должны быть разработаны опросники и методика оценки полученных знаний.

4.1.8. ТРЕБУЕМЫЙ РЕЖИМ РАБОТЫ ПЕРСОНАЛА ИС

Штатное расписание Системы также определяется Исполнителем на этапе разработки Технического проекта и согласовывается протоколом с Заказчиком.

4.1.8.1. Требования к численности и квалификации персонала системы и режиму его работы

Персонал Системы можно разделить на две категории:

Основной персонал – пользователи, выполняющие эксплуатацию систему в своей деятельности.

Персонал технического обслуживания - администраторы и персонал технического обслуживания.

4.1.8.2. Требования к правилам работы пользователей с различными ролями

Поскольку Система предназначена для доступа ограниченного круга должностных лиц, в Системе должно быть предусмотрено разделение пользователей по типам. Должны быть представлены следующие типы пользователей: - незарегистрированные пользователи. Данная группа пользователей должна иметь доступ ко всем открытым информационным разделам Системы, предназначенным для публичного доступа. Не должно быть возможности для изменения содержимого Системы данной группой пользователей. - зарегистрированные пользователи. Данная группа пользователей должна иметь доступ ко всем открытым информационным разделам и сервисам Системы.

Также должна быть предоставлена возможность персональной настройки и модификации содержащихся в Системе данных в рамках, назначенных зарегистрированным пользователям прав доступа. - персонал Системы. Данная группа состоит из пользователей, которые ответственны за поддержание функционирования Системы, пополнение и обновление информации, обслуживание информационных сервисов и выполнение прочих операций, связанных с процессами информирования и обеспечения сервисами пользователей Системы.

Для выполнения своих функций персоналу присваиваются следующие роли:

специалист по информационному обслуживанию (оператор). Вносит изменения в закрепленные за ним информационные объекты через административный интерфейс.

специалист по техническому обслуживанию. Выполняет плановые и аварийные работы по поддержанию Системы в работоспособном состоянии. Перечень и плановые сроки проведения указанных работ должен быть оформлен в виде соответствующего регламента.

администратор. Назначает роли обслуживающему персоналу Системы и назначает права доступа зарегистрированным пользователям. Выполняет функции по контролю за функционированием Системы в целом.

В системе установлены следующие функциональные возможности для уполномоченных/зарегистрированных пользователей:

- Заполнение/ Редактирование/Правка данных;
- Поиск, фильтрация и выгрузка введенных данных;
- Поиск, фильтрация и выгрузка по всем отчетам;
- Администрирование.

4.1.9. ПОКАЗАТЕЛИ НАЗНАЧЕНИЯ

Степень приспособляемости системы к изменению процессов и методов управления:

- Меню программного комплекса должны быть сгруппированы в соответствии с тематикой информации, функциональными задачами и технологией работы с возможностью изменения состава;

- Администратор безопасности должен иметь возможность изменять права доступа пользователей к данным и меню при изменении организационной структуры, технологии работы или других факторов, влияющих на права доступа к информации;

- В целях реализации требований законодательства и нормативных актов в Системе должна быть обеспечена возможность изменения состава форматов данных, используемых при работе программного обеспечения. Вновь применяемые форматы данных должны быть описаны и утверждены Заказчиком;

- В случае изменений нормативно-правовой базы создаваемой системы, влекущих за собой изменения в структуре и составе баз данных, его функциональности, все доработки системы проводятся в рамках его модернизации по отдельным договорам.

Производительность системы:

- Система должна отвечать требованиям масштабируемости, то есть входящее в ее состав аппаратное обеспечение ПО должно обеспечивать одновременную работу необходимого числа пользователей путем наращивания вычислительных ресурсов;
- Недоступность какого-либо информационного ресурса системы не должна оказывать влияния на производительность системы в целом;
- Время обмена данными между информационными ресурсами центрального и регионального уровней системы определяется техническими возможностями аппаратного обеспечения, на которых размещены ресурсы, и пропускной способностью каналов сети передачи данных между ресурсом и потребителем информации.

Показатели назначения, характеризующие степень соответствия Системы предъявляемым к ней требованиям для организационно-экономических Систем информатизации, в которых управленческое решение и его реализация зависят от человека, трудно формализуются.

Поэтому для Системы степень соответствия назначению будет определяться выполнением требований настоящего технического задания, особенно, в части состава (и содержания) автоматизированных функций и задач, решаемых в подсистемах и отдельных модулях (например, в процентах от запланированных), точности и достоверности исходной и расчетной информации и получаемых решений, возможности их непосредственного использования (таблица 4.1.4.).

Таблица 4.1.4. Показатели степени соответствия Системы назначению

№	Наименование показателей назначения	Пояснение
	Показатели надежности	Характеризуют функциональное соответствие Системы заявленным целям и способность Системы выполнять заданные функции в различных условиях
1.1	Валидность	Система должна соответствовать заявленным целям и функциональным требованиям технического задания
1.2	Защищенность	Система должна иметь возможность предотвращать несанкционированный доступ к данным
1.3	Работоспособность	Система должна функционировать в заданных режимах при отсутствии дестабилизирующих воздействий
1.4	Согласованность	Система и документация должны иметь однозначные, непротиворечивые описания для одинаковых объектов, функций, терминов, определений и т.д.
1.5	Устойчивость	Система должна иметь способность, обеспечивающую продолжение работы Системы после возникновения отклонений,

		вызванных дестабилизирующими воздействиями
2	Показатели эффективности	Характеризуют степень удовлетворения потребности пользователя в получении информации с учетом экономических, временных и других ресурсов Системы
2.1	Быстродействие	Система должна быть способной выполнять действия в интервале времени, отвечающем заданным требованиям
2.2	Экономичность	Система должна иметь возможность работы на минимальных ресурсах Системы
3	Показатели технологичности	Характеризуют технологические аспекты, обеспечивающие простоту устранения ошибок в Системе
3.1	Модифицируемость	Система должна иметь возможность, обеспечивающую простоту внесения необходимых изменений и доработок в Систему в процессе эксплуатации
3.2	Повторяемость	В Системе должно быть использованы типовые проектные решения или компоненты
3.3	Структурность	Система должна состоять из комплексов, выполняющих взаимосвязанные функции

4.1.10. ТРЕБОВАНИЯ К НАДЕЖНОСТИ

Показатели надежности для системы должны определяться действующими требованиями по надежности автоматизированных информационных систем для органов власти и управления и могут быть уточнены в техническом проекте. Также в техническом проекте должны быть определены методы и средства выполнения работ в случае сбоев системы.

Показатели надежности Системы:

- коэффициент готовности 0,9999;
- время восстановления всей системы 4 часа;
- время восстановления отдельных подсистем не более 2 часов.

Коэффициент готовности определяется отношением времени, проведенном системой в работоспособном состоянии, к общему времени работы.

Время восстановления включает время на выявление аварии (сбоя) и устранение его последствий. В том числе (при необходимости) - восстановление баз данных из архивных копий.

Надежность *создаваемой системы* обеспечивается:

- высокой технологичностью разрабатываемых программных средств и организационного обеспечения, позволяющего сохранять циркулирующую в системе информацию при сбоях и других ситуациях, нарушающих или разрушающих устойчивость функционирования системы;

- выбором отказоустойчивого оборудования и его структурным резервированием;
- горячим резервированием наиболее важных узлов Системы, к которым относятся серверы базы данных, серверы приложений, компоненты сети хранения данных, оборудование,

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

С целью предотвращения несанкционированного доступа к информационным ресурсам системы должно быть обеспечено выполнение следующих функций:

- Защита информации от атак извне;
- Защита информации от несанкционированного доступа пользователей;
- Обеспечение целостности информации (при хранении, передаче, и обработке данных);

Все системы в части безопасности должны разрабатываться с учетом требований действующих стандартов и нормативных документов Республики Узбекистан.

Информационная безопасность в системе должна достигаться за счет комплексного использования:

- средств защиты информации от несанкционированного доступа для рабочих станций, серверов и сетевого телекоммуникационного оборудования;
- межсетевых экранов (Firewall);
- средств анализа защищенности, обнаружения и предотвращения вторжений;
- средств антивирусной защиты информации;
- средств аутентификации и управления доступом, а также протоколирования действий пользователей.

Система защиты информации системы в части защиты локальных вычислительных сетей и автоматизированных рабочих мест должна соответствовать требованиям национальных стандартов:

- O'zDSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения»;
- O'zDSt ISO/IEC 27001:2016 Информационные технологии. Методы обеспечения безопасности системы управления информационной безопасностью. Требования;
- O'zDSt ISO/IEC 27002:2016 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.

4.1.13. ТРЕБОВАНИЯ К РАЗГРАНИЧЕНИЮ ПРАВ ДОСТУПА

Требования не предоставляются

4.1.14. ТРЕБОВАНИЯ ПО СОХРАННОСТИ ИНФОРМАЦИИ ПРИ АВАРИЯХ

Сохранность информации Системы должна обеспечиваться при следующих аварийных ситуациях:

- нарушения электропитания;
- полный или частичный отказ технических средств системы, включая сбои и отказы накопителей на жестких магнитных дисках;
- сбой общего или специального программного обеспечения системы;
- ошибки в работе персонала;
- выход из строя:
 - комплекса технических средств из-за аварий техногенного характера – повреждение внешних каналов связи, нарушение системы электропитания зданий и т.д.;
 - элемента сетевой инфраструктуры системы;
 - одиночного сервера;
 - одиночного дискового массива сервера;
 - диска сервера;

обеспечивающее связь подсистем, а также связь пользователей каждой подсистемы с серверами БД;

- использованием источников бесперебойного питания;
- выбором топологии телекоммуникационной и локальных вычислительных сетей, обеспечивающих вариантность маршрутизации потоков информации;
- дублированием носителей информации;
- высоким уровнем квалификации и организации работы обслуживающего персонала;
- организацией технического обслуживания, использованием современных методов и средств диагностики;
- использованием только лицензионных программных продуктов;
- отладкой и тестированием модулей всех подсистем;
- наличием исчерпывающих комплектов технической документации, обеспечивающих надежную эксплуатацию всех модулей подсистем;
- работой модулей подсистем, которые не должны вызывать разрушение, искажение и/или утрату сведений, хранящихся в прикладных автоматизированных информационных системах субъектов взаимодействия Системы.

Все действия пользователей должны записываться в соответствующих журналах. Доступ к журналам действий пользователей должен иметь только администратор(ы). Никто (даже администратор) не должен иметь права на изменение/удаление записей журналов.

При вводе данных в поля должен осуществляться контроль входной информации по типу данных и диапазону допустимых значений. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

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

4.1.11. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ

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

4.1.12. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

При разработке Системы должны быть учтены требования политики информационной безопасности действующие в объекте информатизации, чтобы избежать возникновения конфликтных ситуаций при проведении мероприятий по обеспечению информационной безопасности. Количество неудачных попыток входа в Системы должно быть ограничено и при его превышении ИС должна блокироваться на определенный промежуток времени. Доступ и взаимодействие с Системы должен осуществляться по защищенным каналам связи. Доступ пользователей к системе должен осуществляться в соответствии с их ролями. Обеспечение аутентификации пользователей системы привести минимальные требования к паролям пользователей которым они должны отвечать: - содержать как строчные, так и прописные символы (например, a-Z, A-Z) - кроме букв содержать цифры и символы пунктуации (например, 0-9, !@#\$%Л&*); - содержать не менее восьми буквенно-цифровых символов. Вводимые при входе данные не должны отображаться явно на экране и должны храниться в зашифрованном виде.

С целью защиты информации и программных средств от несанкционированного доступа и действия вредоносных программ (компьютерных вирусов и вредоносных скриптов) при модернизации существующего комплекса Заказчика и эксплуатации системы будут предприняты организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

- процессора сервера;
- сетевого адаптера сервера;
- внутреннего источника питания сервера;
- нарушение логической целостности информации, хранящейся на диске сервера.

В целях сохранности информации при авариях и сбоях средствами операционной системы и СУБД обеспечивается:

- возможность полного или частичного восстановления программ в результате сбойных ситуаций;
- наличие системы дублирования информации на резервные устройства хранения с последующим восстановлением.
- В случаях отказа технических средств из-за потери электропитания в целях сохранности информации и обеспечения бесперебойного функционирования системы должны быть предусмотрены:
 - кратковременная (до 20-30 минут) поддержка электроснабжения путем автоматического включения устройств бесперебойного питания;
 - обеспечение постоянного электроснабжения путем включения дизель-генераторных систем.

4.1.15. ТРЕБОВАНИЯ ЗАЩИТЕ ОТ ВЛИЯНИЯ ВНЕШНЕГО ВОЗДЕЙСТВИЯ

Все компоненты Системы должны быть размещены в специальных помещениях, оборудованных и защищенных в соответствии с требованиями стандарта Республики Узбекистан O‘zDSt 2875:2014 «Информационная технология. Требования к дата центрам. Инфраструктура и обеспечение информационной безопасности», нормативно-технической документации (Руководящий документ RH 45-201:2011 Технические требования к зданиям и сооружениям для установки средств вычислительной техники») и документации производителей оборудования.

Непроизводственный характер Система определяет ограниченность возможных внешних воздействий – агрессивные газы и пары, запыленность, радиационное излучение, мощные электромагнитные, электрические и тепловые поля, вибрация и прочее.

Защита системы от воздействий внешних электрических и магнитных полей, а также помех по цепям питания должна быть достаточной для эффективного выполнения техническими средствами своего назначения при функционировании Системы.

Средства защиты информации Системы от внешних воздействий должны обеспечивать:

- стабильность электропитания технических средств в соответствии с требованиями, определяемыми техническими условиями эксплуатации;
- исключение влияния сильных электрических и магнитных полей;
- уровень вибрации в пределах установленных норм;
- пожарную безопасность;
- требуемые микроклиматические условия в помещениях.

4.1.16. ТРЕБОВАНИЯ К ЭРГОНОМИКЕ И ТЕХНИЧЕСКОЙ ЭСТЕТИКЕ

Обслуживающий персонал системы при работе с системой не должен испытывать неудобств, связанных с неправильной организацией рабочего места или взаимодействия человека с элементами системы.

Смонтированные элементы системы не должны портить внешний вид помещений, где они будут установлены.

Оборудование рабочих мест административного персонала подсистемы должно обеспечивать в штатном режиме непрерывный работы (без необходимости покидания рабочего места для осуществления производственных операций) цикл работы в соответствии с эксплуатационной и технологической документацией.

Эргономические решения должны быть едиными для всех компонентов Системы.

В системе должны быть предусмотрены необходимые виды интерфейсов для всех категорий административного персонала. Интерфейсы могут реализовываться в виде веб приложений, графических оболочек или командной строки.

Пользовательский интерфейс Системы должен отвечать следующим требованиям:

1. Дизайн экранных форм должен быть стандартным и подвергаться изменению только в случае невозможности решить задачу стандартной формой;
2. Система должна быть удобна и понятна;
3. Эргономические решения должны быть едиными для всех компонентов и модулей Системы;
4. Пользователь должен иметь возможность доступа к контекстно-зависимой справке по стандартному компоненту Системы и руководству пользователя;
5. Интерфейс пользователей должен способствовать уменьшению вероятности совершения случайных ошибочных действий;
6. Интерфейс должен быть оптимизирован для выполнения типовых и часто используемых прикладных операций.

Объем и представление информации, предоставляемые пользователю клиентскими интерфейсами Системы должны соответствовать возможностям человека по восприятию и переработке информации.

При ошибках в действиях пользователя должно выдаваться сообщение, содержащее информацию о причине возникновения ошибки.

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав Системы должно осуществляться посредством визуального графического интерфейса.

Интерфейс Системы не должен быть перегружен графическими элементами. Навигационные элементы должны быть выполнены в удобной для пользователя форме.

Ввод-вывод данных Системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов.

Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Экранные формы Системы должны проектироваться с учетом требований унификации:

- все экранные формы должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
- для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций, а также последовательности действий пользователя при их выполнении, должны быть унифицированы;

внешнее поведение сходных элементов интерфейса должны реализовываться одинаково для однотипных элементов.

4.1.17. ТРЕБОВАНИЯ К ТРАНСПОРТАБЕЛЬНОСТИ

Требования к транспортабельности для подвижных ПО не предъявляются, поскольку ИС устанавливается стационарно и один раз и в последующем перемещение ИС с аппаратными средствами не предусмотрено

4.1.18. ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ, ТЕХНИЧЕСКОМУ ОБСЛУЖИВАНИЮ, РЕМОНТУ И ХРАНЕНИЮ КОМПОНЕНТОВ СИСТЕМЫ

Система должна быть рассчитана на эксплуатацию в составе Системы Заказчика. Техническая и физическая защита аппаратных компонентов системы, носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, текущее обслуживание реализуется техническими и организационными средствами, предусмотренными в ИТ инфраструктуре Заказчика.

Должна быть обеспечена возможность функционирования Системы в круглосуточном режиме.

Инсталляционные комплекты Системы должны храниться у администраторов систем в помещениях с ограниченным контролируемым доступом.

Для хранения и восстановления данных в системе должны использоваться средства СУБД или внутренние программные инструменты Системы. Реализация этих требований должна быть обеспечена соответствующими организационными мерами – регламентным обслуживанием системы.

Требования к эксплуатации и регламент обслуживания технических средств (оборудования) системы определяются соответствующими эксплуатационными документами и инструкциями от производителя соответствующего оборудования.

Требования к эксплуатации и регламент обслуживания, необходимого для функционирования Системы, системно-программного обеспечения (операционная система, база данных и т.д.) определяются соответствующими эксплуатационными документами и инструкциями от производителя программного обеспечения.

Требования к допустимым площадям для размещения обслуживающего персонала Системы определяются в соответствии с требованиями норм охраны труда и техники безопасности, установленными в Республике Узбекистан.

Требования к размещению технических средств, параметрам сетей энергоснабжения и условиям эксплуатации разрабатываются на основе соответствующих технических условий, предъявляемых к разрабатываемым средствам аппаратного обеспечения.

4.1.19. ТРЕБОВАНИЯ К ПАТЕНТНОЙ И ЛИЦЕНЗИОННОЙ ЧИСТОТЕ

Реализация Системы должна отвечать требованиям патентной чистоты согласно действующему законодательству и регламентирующих распорядительных документов.

4.1.20. ТРЕБОВАНИЯ ПО СТАНДАРТИЗАЦИИ И УНИФИКАЦИИ

При разработке Системы необходимо соблюдать принцип унификации используемых средств.

Данные, загружаемые, вводимые и обрабатываемые в Систему, должны отвечать основным принципам единообразия, непротиворечивости, однократности ввода, полноты и достоверности информации.

Система должна соответствовать следующим показателям, устанавливающим требуемую степень использования стандартных, унифицированных методов реализации функций (задач), поставляемых программных средств:

- Поддержка форматов электронных документов для распространения данных, CSV, DOC, EXL, PDF;

- Поддержка автоматического преобразования форматов данных в формат HTML, для обеспечения просмотра информации без установки специальных программных средств;

- Возможность функционирования на различных аппаратных платформах.

Используемое решение должно обеспечивать функционирование задач, операций и интерфейсов в следующих операционных системах: Windows, MAC-OS.

Разрабатываемая документация должна быть представлена в строгом соответствии с нормативными документами, утвержденными у Заказчика или по согласованию сторон по стандартам, принятым в компании – вендоре производителя Системы.

4.2. ТРЕБОВАНИЯ К ФУНКЦИЯМ (ЗАДАЧАМ), ВЫПОЛНЯЕМЫМ ИНФОРМАЦИОННОЙ СИСТЕМОЙ

4.2.1. ПЕРЕЧЕНЬ ФУНКЦИЙ, ЗАДАЧ, ВЫПОЛНЯЕМЫХ ПОДСИСТЕМАМИ

ТРЕБОВАНИЯ К ПОДСИСТЕМЕ «ХАВФСИЗ ЙУЛЬ»

Мобильное приложение должно предоставлять возможность пользователю мобильного приложения (далее-Пользователь) осуществлять отправку сообщений, содержащих материалы фотосъемки, и свидетельствующих о наличии события административного правонарушения в области дорожного движения и (или) благоустройства территории в части парковки и хранения транспортных средств (далее – сообщения/уведомления/материалы).

Использование мобильного приложения должно регулироваться действующими нормативными правовыми актами Республики Узбекистан.

Мобильное приложение – должно быть реализовано с поддержкой современных мобильных платформ (iOS и Android версии не ниже 14 и 11 соответственно).

Приложение должно быть доступно для установки и скачивания через соответствующие сервисы в сети Интернет и с веб-сайта Заказчика.

Приложение должно использовать внутренние коммутационные средства связи для соединения с сервером приложений.

В непосредственные задачи приложения входит:

1. Соединение с сервером приложений;
2. Доступ к фронтальной камере смартфона или планшетного компьютера, при её наличии;
3. Запись данных с камеры устройства;
4. Получение координат устройства в момент записи данных (фото или видео), с встроенного модуля GPS устройства; 5.

Передача данных на сервер приложений; Логика работы приложения состоит из нескольких шагов:

Все действия приложения должны проводиться только аутентифицированными пользователями. Для доступа к приложению пользователь должен быть зарегистрирован в Системе, и иметь роль пользователя «Участник групп». Для доступа к приложению используется уникальная комбинация Логин\Пароль предоставляемая пользователю. В случае если пароль пользователя сброшен администратором ИС или установлен на пароль по умолчанию, пользователь приложения должен изменить свой пароль после прохождения аутентификации.

В приложении должны быть заблокированы возможности автоматического соединения или сохранения пользовательского логина и пароля. Уникальная комбинация Логин\Пароль не должны храниться на устройстве.

В случае бездействия пользователя длительный промежуток времени (30 минут), приложение должно отключить пользователя от сервера приложений, но сохранить за ним собранные полевые данные (фото, видео, координаты, дата, описание). С момента аутентификации пользователя, приложение должно проверить доступность встроенных устройств, камеры и GPS модуля.

Определение местоположения устройства должно проводиться всё время в течение работы пользователя с приложением. Координаты устройства должны отображаться в цифровом

формате в интерфейсе приложения.

После прохождения аутентификации пользователя в приложении, пользователь, в случае если он является участником более чем одной группы, должен выбрать, в какую из групп относить данные собранные с места события. В случае если группа у пользователя только одна, пользователь автоматически перемещается в раздел этой группы. После выбора группы, пользователь должен увидеть последние данные зафиксированные другими сотрудниками группы, с возможностью их загрузки. Данная функция реализуется для исключения дубликатов данных или повторной отправки одинакового набора информации.

После прохождения аутентификации и выбора группы, пользователь может приступить к загрузке данных. Приложение должно предоставлять пользователю возможность собирать с места события следующие данные:

- Видео материалы – возможность записи видео с фронтальной камеры или загрузка данных с файловой системы устройства;

Фото и видео материалы должны сопровождаться координатными данными с места съёмки, если таковые имеются или иметь возможность ручного указания координат места съёмки в координатной системе WGS 84. Каждый файл фото или видео может сопровождаться текстовым комментарием пользователя приложения. Дата фото или видео материала, загружаемого в данные группы, устанавливается автоматически на текущую дату, полученную с сервера приложений. В приложении, так же должна быть реализована функция отправки документов и текстовых данных распространённого формата (.doc, .docx, .xls, .xlsx, .txt, .rtf, .pdf), файлы документов так же должны сопровождаться комментариями пользователя приложения.

Выход из приложения и прерывание его работы, может быть инициализировано как закрытием приложения через головное меню устройства, так и выбором действия «Выход» в приложении. При выходе из приложения, аутентификация пользователя приложения должна обнулиться. Если работа приложения прервана окончательно, пользовательские данные фото, видео съёмки или документов, должны быть доступны для повторного отправления. Если данные были переданы на сервер, хранение их на устройстве не рекомендовано.

Начиная использовать мобильное приложение/его отдельные функции, либо пройдя процедуру регистрации, Пользователь считается принявшим Условия в полном объеме, без всяких оговорок и исключений. В случае несогласия Пользователя с какими либо из положений Условий, Пользователь не в праве использовать мобильное приложение. В случае если оператором были внесены какие-либо изменения в Условия, с которыми Пользователь не согласен, он обязан прекратить использование мобильного приложения.

Регистрация Пользователя. Учетная запись Пользователя

Для того чтобы воспользоваться мобильным приложением, Пользователю должен пройти процедуру регистрации, в результате которой для Пользователя будет создана уникальная учетная запись.

Для регистрации Пользователь должен обязуется предоставить достоверную и полную информацию о себе по вопросам, предлагаемым в форме регистрации, и поддерживать эту информацию в актуальном состоянии.

Если Пользователь предоставляет неверную информацию или у оператора будет основания полагать, что предоставленная Пользователем информация неполна или недостоверна, оператор будет иметь право по своему усмотрению заблокировать либо удалить

учетную запись Пользователя и отказать Пользователю в использовании мобильного приложения.

Обработка персональных данных Пользователей при использовании мобильного приложения должен производиться в соответствии с требованиями Закона Республики Узбекистан «О персональных данных»

UA-1. Вход пользователя в приложение

1. Пользователь запускает мобильное приложение.
2. Показать экран загрузки (S1).
3. Предложить пользователю выбрать язык интерфейса приложения. Показать экран выбора языка (S2):
 - a. Узбекский язык (кириллица);
 - b. Узбекский язык (латиница);
 - c. Русский язык.
4. Пользователь выбирает язык (нажимает на выбранный язык).
5. При первом входе пользователя показать экран ввода логина и пароля (S3).
6. Пользователь вводит логин и пароль и нажимает на кнопку «Авторизация»:
 - a. Отрицательный ввод: При неправильном вводе логина и пароля показать сообщение «Логин и пароль введены неверно»;
 - b. Пользователь нажимает на кнопку ОК и заново вводит корректный логин и пароль.
7. Показать экран установления секретного ключа (S4).
8. Ввод секретного ключа.
9. Повторный ввод секретного ключа и нажатие кнопки «Сохранить»:
 - a. Положительный ввод: Секретный код успешно установлен;
 - b. Отрицательный ввод: Длина секретного кода должна быть 4-х значной. Пользователь нажимает ОК и заново вводит секретный ключ;
 - c. Отрицательный ввод: Вывод сообщение «Секретный код не совпал» Пользователь нажимает ОК и заново вводит секретный ключ.
- 9.1 При повторных входах показать экран ввода секретного ключа (S4-1):
 - a. Отрицательный ввод: При неправильном вводе секретного ключа дать сигнал пользователю.
10. Показать главный экран (S5).
11. Конец сценария.

UA-2. Выбор Блока «Настройки».

1. Пользователь выбирает блок «Настройки» на Главном экране (S5).
2. Показать экран настроек (S11).
3. Конец сценария.

UA-2.1 Выбор раздела «Обновить приложение».

1. Пользователь нажимает на раздел «Обновить приложение»:
 - a. Показать диалоговое окно с сообщением «Приложение обновляется»:

- i. После завершения обновления, показать сообщение «Обновление завершено»;
 - ii. Пользователь нажимает на кнопку ОК;
 - iii. Возврат на экран настроек(S11).
 - b. Показать диалоговое окно с сообщением «У вас последняя версия приложения»:
 - i. Пользователь нажимает на кнопку ОК;
 - ii. Возврат на экран настроек(S11).
- 2. Конец сценария.

UA-2.2 Выбор раздела «Настройка безопасности».

1. Выполняется действие шага 6 сценария действий UA-1.
2. Конец сценария.

UA-2.3 Выбор раздела «Офлайн режим».

1. Пользователь нажимает на раздел «Офлайн режим».
2. Показать Экран синхронизации (S11-1).
3. Пользователь нажимает на кнопку «Загрузить» в части «Фото» Экрана синхронизации (S11-1).
 - a. Показать процент загрузки данных на карте;
 - b. При повторном нажатии на кнопку «Загрузить», отобразить сообщение «Вы уже отправляли заявку на получение данных».
4. Пользователь нажимает на кнопку «Загрузить» Экрана синхронизации (S11-1).
 - a. Показать процент загрузки данных на карте;
 - b. При повторном нажатии на кнопку «Загрузить», отобразить сообщение «Вы уже отправляли заявку на получение данных».
5. Конец сценария.

UA-2.4 Выбор раздела «Модули».

3. Пользователь нажимает на раздел «Модули»
 - c. Показать диалоговое окно с сообщением «Модули обновлены»
 - i. Пользователь нажимает на кнопку ОК
 - ii. Возврат на экран настроек(S11)
 - d. Показать диалоговое окно с сообщением «Нет новых модулей»
 - i. Пользователь нажимает на кнопку ОК
 - ii. Возврат на экран настроек(S11)
4. Конец сценария

UA-2.3 Выбор раздела «Изменить пароль».

1. Пользователь нажимает на раздел «Изменить пароль» (S11-2)
2. Ввод нового пароля
3. Повторный ввод нового пароля
4. Пользователь нажимает на кнопку «Сохранить»
 - e. Положительный ввод: Вывод сообщения «Пароль изменен успешно»
 - f. Отрицательный ввод: Вывод сообщения «Длина пароля должно быть не менее 3-х символов»

- g. Отрицательный ввод: Вывод сообщения «Пароли не совпали»
- 5. Возврат на экран настроек(S11)
- 6. Конец сценария

UA-2.4 Выбор раздела «ПИН-код».

- 1. Пользователь нажимает на раздел «ПИН-код»
- 2. Показать экран установления секретного ключа (S4)
- 3. Выполняются действия шага 8 и 9 сценария действий UA-1.
- 4. Возврат на экран настроек(S11)
- 5. Конец сценария

UA-2.5 Выбор раздела «Язык приложения».

- 1. Пользователь нажимает на раздел «Язык приложения» (отобразить текущий язык приложения)
- 2. Показать экран выбора языка (S2)
- 3. Выполняются действие шага 4 сценария действий UA-1.
- 4. Возврат на экран настроек(S11)
- 5. Конец сценария

UA-2.6 Выбор раздела «Изменить дистанцию»

- 1. Пользователь нажимает на раздел «Изменить дистанцию»
- 2. Показать диалоговое окно «Введите дистанцию»
- 3. Ввод дистанции и нажатие на кнопку ОК
 - h. Отрицательный ввод: Вывод сообщение «Дистанция должна быть на расстоянии от 50 до 200 метров.
- 4. Возврат на экран настроек(S11)
- 5. Конец сценария

UA-2.7 Выбор раздела «Повторная авторизация»

- 1. Пользователь нажимает на раздел «Повторная авторизация»
- 2. Вывод сообщения «Данное действие удалит установленный пин-код. Вы уверены, что хотите продолжить?»
- 3. Нажатие на кнопку ОК
- 4. Переход на экран экран загрузки (S1)
- 5. Выполняются с 3 по 9 шаги сценария действий UA-1
- 6. Показать главный экран (S5)
- 7. Конец сценария.

UA-3. Выбор Блока «Назорат».

- 1. Пользователь выбирает блок «Назорат» на Главном экране (S5).
- 2. Показать экран списка фотографии (S6).
- 3. Пользователь выбирает фото из списка нажимает на неё.
- 4. Пользователь нажимает на кнопку «Отправить»:
 - a. Показать диалоговое окно для ввода сообщений.
 - b. Ввод сообщений.
 - c. Положительный ввод: Вывод сообщения «Фото отправлены».
 - d. Нажать ОК

- e. Возврат на экран (S6-1)
- f. Возврат на экран (S6-1)
- 5. Показать главный экран (S5)
- 6. Конец сценария

UA-6. Выбор Блока «Отчеты».

1. Выбор блока «Отчеты»
2. Показать экран Отчеты (S9)
3. Нажатие на кнопку «Возврат назад»
4. Показать экран Отчеты (S9)
5. Конец сценария

UA-7. Выбор Блока «Сообщения».

1. Выбор блока «Сообщения»
2. Показать экран Сообщения (S10)
3. Нажать на кнопку Подробно
4. Показать Экран с полным текстом сообщения (S10-1)
5. Нажатие на кнопку «Возврат назад»
6. Показать экран Отчеты (S10)
7. Конец сценария

UA-8. Выход пользователя из приложения

1. Нажать на меню Навигации
2. Показать экран меню навигации (S12)
3. Нажать на кнопку Выход
4. Показать сообщение «Данное действие удалит установленный пин-код. Вы уверены, что хотите продолжить?»
5. Нажать на кнопку ОК
6. Выход из приложения
7. Конец сценария

ТРЕБОВАНИЯ К ЭКРАНЫМ ФОРМАМ ПРИЛОЖЕНИЯ

Экран S1. Splash screen

Структура экрана

Рис.1. Экран загрузки

S1. Splash screen

Элемент	Текст	Формат	Значение по умолчанию	Функциональные требования
Логотип	Хавфсиз йул	Картинка	-	Обозначение системы
Текст	Загружается...	Статистический текст	-	Информирование пользователя о загрузке приложения

Переход на экран S1. Splash screen

Переход на экран осуществляется при выполнении следующих сценариев:

- UA-2.7 Выбор раздела «Повторная авторизация»: шаг 5
- UA-8. Выход пользователя из приложения: шаг 6

Действия на экране S1. Splash screen

Выполнение каких-либо действий на экране не предусмотрено.

Ошибки на экране S1. Splash screen

Появление каких-либо ошибок на экране не предусмотрено.

Экран S2. Выбор языка

Структура экрана S2. Выбор языка

Элемент	Текст	Формат	Значение по умолчанию	Функциональные требования
Логотип	Хавфсиз йул	Картинка	-	Обозначение системы
Кнопка с надписью	Русский	Кнопка	-	Перевод языка системы на русский
Кнопка с надписью	Ўзбекча	Кнопка	-	Перевод языка системы на узбекский (кириллица)
Кнопка с надписью	O`zbekcha	Кнопка	-	Перевод языка системы на узбекский (латиница)
Текст		Статистический текст	-	Обозначение разработчика системы

Переход на экран S2. Экран выбора языка

Переход на экран осуществляется при выполнении следующих сценариев:

- UA-2.5 Выбор раздела «Язык приложения»: шаг 2
- UA-2.7 Выбор раздела «Повторная авторизация»: шаг 5

Действия на экране S2. Экран выбора языка

Действия	Реакция системы
Нажать на кнопку Русский	Переход на экран ввода логина и пароля S3 (русский язык)
Нажать на кнопку Ўзбекча	Переход на экран ввода логина и пароля S3 (узбекский -кириллица)

Нажать на кнопку O`zbekcha	Переход на экран ввода логина и пароля S3 (узбекский -латиница)
----------------------------	---

Ошибки на экране S2. Экран выбора языка

Появление каких-либо ошибок на экране не предусмотрено.

Экран S3. Ввод логина и пароля

Структура экрана S3. Ввод логина и пароля

Элемент	Текст	Формат	Значение по умолчанию	Функциональные требования
Логотип		Картинка	-	Обозначение системы
Поле ввода Логина	Логин	Латинские буквы, цифры, любой регистр, специальные	Незаполненно	При вводе логина плейсхолдер стирается
Поле ввода Пароля	Пароль	Латинские буквы, цифры, любой регистр, специальные	Незаполненно	При вводе пароля плейсхолдер стирается
Кнопка отображения пароля	-	Кнопка	Скрытые символы	При нажатии на кнопку «глаз» скрытые символы пароля отображаются (символ слеш). При повторном нажатии символы скрываются
Кнопка входа	Авторизация	Кнопка	Кликабельная	Если логин и пароль введены верно осуществляется вход в систему. Если логин и/или пароль не введены вызывается сообщение. Если логин и/или пароль введен неверно вызывается сообщение.

Переход на экран S3. Экран ввода логина и пароля

Переход на экран осуществляется при выполнении следующих сценариев:

- UA-2.7 Выбор раздела «Повторная авторизация»: шаг 5
- UA-8. Выход пользователя из приложения: шаг 6

Действия на экране S3. Экран ввода логина и пароля

Действия	Реакция системы
Ввести верный логин и пароль	Переход на экран установления пин-кода S4
Ввести только логин	Строка ввода логина подсвечивается красным цветом

Ввести только пароль	Строка ввода пароля подсвечивается красным цветом
Ввести неверный логин и верный пароль	Отобразить сообщение
Ввести верный логин и неверный пароль	Отобразить сообщение
Ввести неверный логин и пароль	Отобразить сообщение

Ошибки на экране S3. Экран ввода логина и пароля

Действия сценария UA-1. Вход пользователя в приложение: шаг 6

Экран S4. Установление секретного ключа

Структура экрана S4. Установление секретного ключа

Элемент	Текст	Формат	Значение по умолчанию	Функциональные требования
Логотип		Картинка	-	Обозначение системы
Поле ввода секретного ключа	Секретный код	Цифры	Незаполненно	При вводе кода плейшолдер стирается. При вводе букв и символов в поле ничего не вводится
Поле повторного ввода секретного ключа	Повторите секретный код	Цифры	Незаполненно	При вводе повторного кода плейшолдер стирается. При вводе букв и символов в поле ничего не вводится
Кнопка отображения секретного кода	-	Кнопка	Скрытые символы	При нажатии на кнопку «глаз» скрытые символы пароля отображаются (символ слеш). При повторном нажатии символы скрываются
Кнопка Сохранения	Сохранить	Кнопка Кликабельная	Кликабельная	Если секретный код введен в правильном формате выдать сообщение об успешном установлении кода. Если длина секретного кода введена меньше требуемого выдать сообщение. Если секретный код и повторно набранный секретный код не совпали, выдать сообщение

Переход на экран S4. Экран установления секретного ключа

Переход на экран осуществляется при выполнении следующих сценариев:

UA-2.4 Выбор раздела «ПИН-код»: шаг 2

Действия на экране S4. Экран установления секретного ключа

Действия	Реакция системы
Ввести верный формат кода и нажать сохранить	Переход на экран Главный экран S5
Ввести буквы или цифры	Поле неактивное (нет реакции)

Ввести длину секретного ключа меньше требуемого	Выдать сообщение
Ввести повторно секретный ключ различный от первого введенного	Выдать сообщение

Экран S4-1. Ввод секретного ключа

Отображается при повторных (последующих) входах пользователя.

Структура экрана S4-1. Ввод секретного ключа

Элемент	Текст	Формат	Значение по умолчанию	Функциональные требования
Логотип		Картинка	-	Обозначение системы
Заголовок	Введите пин-код	Текст	Незаполненно	При вводе кода заполняется поле
Поле ввода секретного кода	-	Цифры	Незаполненно	После корректного ввода секретного кода переходит на главный экран (S5). При некорректном вводе система выдает сообщение пользователю

Переход на экран S4. Экран ввода секретного ключа

Переход на экран осуществляется при выполнении следующих сценариев:

- UA-1. Вход пользователя в приложение: шаг 9.1

Действия на экране S4. Экран ввода секретного ключа

Действия	Реакция системы
Ввести верный код	Переход на экран Главный экран S5
Ввести неверный код	Выдать сообщение

Ошибки на экране S4. Ввод секретного ключа

Экран S5. Главный экран

Структура экрана S5. Главный экран

Элемент	Текст	Формат	Значение по умолчанию	Функциональные требования
Кнопка навигации	-	Список	-	При нажатии на кнопку отобразить список быстрого доступа
Логотип		Рисунок	-	Отображение названия приложения
ФИО	Пример текста: <i>Иванов Иван Иванович</i>	Текст	-	Показать ФИО
Кнопка	Отправить фото	Кнопка	-	Переход на экран Список фотографии (S6)
Кнопка	Отправить видео	Кнопка	-	Переход на экран Список видеофайлов (S7)
Кнопка	Отчеты	Кнопка	-	После клика переход на экран отчетов (S9)
Кнопка	Сообщения	Кнопка	-	После клика переход на экран список сообщений (S10)
Кнопка	Настройки	Кнопка	-	После клика переход на экран настройки (S11)

4.3. ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

4.3.1. ТРЕБОВАНИЯ К МАТЕМАТИЧЕСКОМУ ОБЕСПЕЧЕНИЮ

Математическое обеспечение Системы должно обеспечивать возможность эффективной разработки программных решений конкретных задач.

Математическое обеспечение Системы должно включать:

- типовые и разработанные методики и алгоритмы сбора и обработки информации (в том числе ввода данных в ПК, контроля достоверности данных и т.п.);
- алгоритмы поиска и сортировки данных.
- Общие требования к математическому обеспечению:
- использование стандартной библиотеки классов;
- максимальное использование типовых методов и алгоритмов;
- используемые математические методы должны учитывать технические возможности технических и программных средств, иметь минимальные значения времени решения и занимаемой оперативной памяти;
- документация на математическое обеспечение (постановка задач и алгоритмы решения) должна обеспечивать однозначное толкование и возможность программирования без дополнительных разъяснений;
- допускается любая форма описания задач – формульная, табличная, блок- схема, UML диаграмма, словесное описание и др.

Алгоритмы математического обеспечения должны отвечать следующим требованиям:

- допускать декомпозицию на относительно простые блоки;
- максимально использовать возможности языков программирования в своем описании;
- обеспечивать функциональную взаимосвязь задач.

Алгоритмы поиска и сортировки данных, используемые при решении практически всех функциональных задач Системы, должны базироваться на процедурах в системном математическом обеспечении и используемых в Системе. Эти алгоритмы должны обеспечивать поиск информации по заданным значениям признаков, формирования заданных структур информации и выполнение над ними необходимых операций.

Алгоритмы формирования выходных документов должны быть максимально унифицированы, позволять при необходимости быстро изменять формы документов и использовать стандартные процедуры и программные средства.

Алгоритмы решения задач, при необходимости, могут включать методы оптимизации и эвристические процедуры для конкретных задач.

4.3.2. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОМУ ОБЕСПЕЧЕНИЮ

- Должна быть обеспечена совместимость с информационным обеспечением Систем, взаимодействующих с разрабатываемой Системой;
- Формы документов должны отвечать требованиям корпоративных стандартов Заказчика (или унифицированной системы документации);
- Структура документов и экранных форм должна соответствовать характеристикам терминалов на рабочих местах конечных пользователей;
- Графики формирования и содержание информационных сообщений, а также используемые аббревиатуры должны быть общеприняты в этой предметной области и согласованы с Заказчиком;
- В Системе должны быть предусмотрены средства контроля входной и результатной информации, обновления данных в информационных массивах, контроля

целостности информационной базы, защиты от несанкционированного доступа;

- Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации;

- Необходимо предусмотреть возможность экстренного отключения доступа к Системе в случаях внештатных ситуаций.

4.3.3. ТРЕБОВАНИЯ К ЛИНГВИСТИЧЕСКОМУ ОБЕСПЕЧЕНИЮ

Необходимо, чтобы Система обеспечивала эффективную возможность ввода информации и работу интернационального офиса с помощью инструментов мультиязычности, которые должны обеспечить возможность использовать несколько языков в одном интерфейсе. При этом название полей в экранных формах должно быть на русском и узбекском языке.

4.3.4. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

ПО Системы должно обладать следующими характеристиками:

- выполнять весь перечень алгоритмов математического обеспечения;
- обеспечивать устойчивость к ошибочным ситуациям, в том числе при неверных и противоречивых данных; сбои в работе программ, отказы части вычислительных средств, ошибки персонала должны диагностироваться, сопровождаться сообщениями, и не должны вызывать нарушений в работе системы;
- обеспечивать перезапуск при восстановлении электрического питания после его отключения без выдачи ложных сигналов и управляющих воздействий;
- давать правильные результаты при всех комбинациях исходных данных, допустимых в рамках постановки задачи;
- иметь возможность оперативного конфигурирования в процессе функционирования Системы.

В случае отсутствия у производителя ПО технической документации на государственном (узбекском) языке, перевод технической документации на государственный язык осуществляется силами Исполнителя.

4.3.5. ТРЕБОВАНИЯ К СУБД

Требования к СУБД представлены в основном ТЗ Системы «E Jarima»

4.3.6. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ

Техническое обеспечение системы должно максимально и наиболее эффективным образом использовать существующие технические средства.

В состав комплекса должны быть следующие технические средства:

- Мобильные телефоны для пользователей системы;

Мобильные телефоны для пользователей системы: Android 4.4 и выше, а также iOS 15. Мобильные приложения для Android и iOS должно реализовываться нативными средствами, либо на основе платформы, обеспечивающей компиляцию в нативные приложения для обеспечения максимальной производительности.

4.3.7. ТРЕБОВАНИЯ К МЕТРОЛОГИЧЕСКОМУ ОБЕСПЕЧЕНИЮ

Дополнительных требований к метрологическому обеспечению не предъявляется.

4.3.8. ТРЕБОВАНИЯ К ОРГАНИЗАЦИОННОМУ ОБЕСПЕЧЕНИЮ

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

Заказчиком должны быть определены должностные лица, ответственные за:

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

К работе с системой должны допускаться сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации и прошедшие обучение работе с системой.

В процессе внедрения Системы подрядные организации по согласованию с заказчиком должны разработать инструкции пользователей всех её программно-технических комплексов (ПТК).

Решения по организационному обеспечению должны отражать порядок и регламент взаимодействия персонала, эксплуатирующего Системы, ИТ-администраторов подразделений.

Инструкции должны содержать четкие указания по действиям эксплуатационного персонала, ИТ-администраторов подразделений при различных ситуациях.

Структура и функции подразделений, участвующих в обеспечении функционирования Системы, организация функционирования Системы, порядок взаимодействия персонала, эксплуатирующего Системы, ИТ-администраторов подразделений должны быть определены на этапе проектирования и ввода Системы в действие.

4.3.9. ТРЕБОВАНИЯ К ГАРАНТИЙНОМУ ОБЕСПЕЧЕНИЮ

Исполнитель должен предоставить полный комплект документации, к каждой единице поставляемой Продукции должен быть приложен полный комплект-оригинал технической документации.

Гарантийное обслуживание на поставляемое оборудование должно быть не менее 3 лет, с даты принятия на эксплуатацию.

Помимо гарантийной поддержки оборудования, Исполнитель в течение действия гарантийных обязательств должен обеспечить необходимую информационно-консультационную помощь специалистам Заказчика.

Вместе с оборудованием, Исполнителем должна быть представлена эксплуатационная документация и руководства пользователя в бумажном и электронном виде.

Гарантийное сервисное обслуживание всего оборудования должно осуществляться по месту эксплуатации, специалистами авторизованного производителем сервис-центра или сервисного партнера в Республике Узбекистан.

Производитель оборудования, предложенный исполнителем, должен иметь в Республике Узбекистан признанный сервисный центр или сервисного партнера для обеспечения гарантийного ремонта поставляемого оборудования.

Сервисный центр или сервисный партнер должен иметь сертификаты авторизации от производителей поставляемого Исполнителем оборудования.

Гарантийное сервисное обслуживание всего представленного оборудования должно производиться в следующем порядке:

Уполномоченный представитель Исполнителя или сервис центра/сервисного-партнера после вызова уполномоченного представителя Заказчика выполняет следующие процедуры:

- Оформление акта о наличии дефекта оборудования;
- Замену (при наличии) или ремонт неисправного оборудования;
- Оформление акта выполненных работ (после выполнения работ). При этом срок реакции на заявку о техническом обслуживании оборудования не должен превышать 8 часов.

В случае отсутствия в наличии запасных частей у уполномоченного представителя Исполнителя или сервис центра, неисправное оборудование или его неисправная часть, после оформления акта о наличии дефекта оборудования, может быть отправлена для ремонта или замены в сервис центр, указанный Исполнителем в контракте.

Срок ремонта оборудования указывается в двухстороннем контракте и не должен превышать 30 рабочих дней с момента оформления акта о наличии дефекта оборудования.

Организация работ по созданию Системы должна осуществляться с использованием современных методов и инструментов проектного управления.

Должно быть обеспечено решение вопросов управления проектом по временным и стоимостным параметрам, управления качеством, персоналом проекта, коммуникациями, рисками.

4.3.10. ОБУЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ

Исполнитель проводит обучение Системы для пользователей в объеме не более 20 человек. Обучение проводится в г. Ташкент на материально технической базе Заказчика.

Заказчик обеспечивает обучающихся:

- Помещением удовлетворяющем требованиям для обучения соответствующего количества слушателей;
- Наличие компьютерного оборудования в помещении для обучения в нужном количестве и соответствующего требованиям работы в Системе;
- Презентационное оборудование.

4.3.11. ТРЕБОВАНИЯ К МЕТОДИЧЕСКОМУ ОБЕСПЕЧЕНИЮ

Методики расчётов, используемых при решении задач Системы, а также, при необходимости, иные специфические требования к реализации задач, детализируются на стадии разработки Технического проекта.

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

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

В состав методического обеспечения входит:

- нормативные правовые документы;
- должностные инструкции персонала, выполняющего работы с использованием Системы.

Состав методического обеспечения может уточняться в процессе техно-рабочего проектирования и согласовывается с заказчиком.

Нормативно-техническая документация должна соответствовать требованиям нормативных правовых актов и разрабатываться согласно следующих стандартов:

- O‘zDSt 1986:2018 Государственный стандарт Узбекистана Информационная технология. Информационные системы. Стадии создания
 - O‘zDSt 1987:2018 Государственный стандарт Узбекистана «Информационная технология. Техническое задание на создание информационной системы».
 - O‘zDSt 1985:2018 Виды, комплектность и обозначение документов при создании информационной системы (ИС),
 - RH 45-170:2004. Руководящий документ. Основные технические требования по созданию локальных и корпоративных ведомственных компьютерных сетей;
- T 45-194:2007 Рекомендации по применению программно-аппаратных средств, обеспечивающих предотвращение актов незаконного проникновения в информационные системы.

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО ВВОДУ СИСТЕМЫ

Реализация требований настоящего ТЗ должна проводиться в несколько этапов. Состав и содержание работ по этапам приведено в таблице ниже. Перечень стадий и этапов выполненных работ по внедрению автоматизированной системы указан в соответствии с O'zDSt 1986:2018 Информационная технология. Информационные системы. Стадии создания. Работы спроектированы с учетом того, что конечная Система должны быть сдана Заказчику Исполнителем «под ключ».

Номер этапа	Наименование работ и их содержание	Сроки выполнения		Исполнитель	Чем заканчивается этап	Доля выполнения от общего объема работ, %
		начало	конец			
Первый этап	Формирование требований к мобильному приложению, Разработка сценария действий пользователя приложения, Разработка прототипов приложения	01.06.2022	10.09.2022	Академия Генеральной прокуратуры	Техническое задание	30%
Второй этап	Создание дизайна мобильного приложения	05.10.2022	10.12.2022	Академия Генеральной прокуратуры		
Третий этап	Разработка мобильного приложения	11.10.2022	31.12.2022	Академия Генеральной прокуратуры	Технический проект	55%
Четвертый этап	Тестирование и доработка	02.01.2023	05.01.2023	Академия Генеральной прокуратуры	Отчет о тестировании приложения	10%
					Отчет о проведении обучения	
Пятый этап	Обучение пользователей, Разработка пользовательской документации, ввод в эксплуатацию	06.01.2023	10.01.2023	Академия Генеральной прокуратуры	Инструкция пользователя Акт ввода в эксплуатацию	5%
					Акты, рапорты о проведенных работах по тех. сопровождению	-
Шестой этап	Техническое сопровождение	10.01.2023	10.01.2024	Академия Генеральной прокуратуры		

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Контроль и приемка Системы должны проводиться в соответствии с требованиями O'zDSt 1986:2018 Информационная технология. Информационные системы. Стадии создания.

Контролю, испытаниям и приемке могут подвергаться как Система в целом, так и ее отдельные очереди (пусковые комплексы), подсистемы и отдельные задачи.

Для Системы устанавливаются следующие основные виды испытаний:

- предварительные испытания;
- опытно-промышленная эксплуатация;
- промышленная эксплуатация

Для планирования проведения всех видов испытаний разрабатываются документы «Программа и методика испытаний» соответствующих видов испытаний, которые должны устанавливать необходимый и достаточный объем и сроки испытаний, обеспечивающие заданную достоверность получаемых результатов. Программа и методика испытаний может разрабатываться на Систему в целом и (или) ее части. В качестве приложения могут включаться тесты (контрольные примеры).

При проведении испытаний Системы должно быть проверено и установлено соответствие Техническому заданию (ТЗ) на создание Системы следующего:

- качество выполнения комплексом программных и технических средств автоматизированных функций во всех режимах функционирования Системы;
- знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования Системы;
- полнота содержащихся в эксплуатационной документации указаний персоналу по выполнению им функций во всех режимах функционирования Системы;
- количественные и (или) качественные характеристики выполнения автоматических и автоматизированных функций Системы;
- другие свойства Системы, которым она должна соответствовать согласно требованиям Технического задания.

Испытания Системы проводятся на объекте Заказчика. По согласованию между Заказчиком и Поставщиком предварительные испытания и приемку программных средств Системы допускается проводить на технических средствах Поставщика при создании условий получения достоверных результатов испытаний.

Статус и состав приемочной комиссии определяется Заказчиком.

По результатам испытаний составляются протоколы проведения с перечнем замечаний и акты завершения испытаний, на основании которых принимается решение о возможности (или невозможности) перехода к следующему виду испытания или приемки Системы в постоянную эксплуатацию. Виды испытаний могут повторяться до устранения всех замечаний к Системе и соответствующей корректировки эксплуатационной документации.

Испытания Системы выполняются после проведения отладки и тестирования, поставляемых программных и технических средств Системы и представления Исполнителем соответствующих документов об их готовности к испытаниям, а также после ознакомления технических специалистов Заказчика с эксплуатационной документацией Системы.

В процессе эксплуатации и испытаний проводится проверка готовности отдельных частей, комплексов и задач Системы, а также предъявленной документации к функционированию в реальных условиях. Эксплуатация Системы и ее частей начинается с момента утверждения акта приемки в эксплуатацию.

Возникшие в процессе предварительных испытаний и эксплуатации дополнительные требования Заказчика, не предусмотренные в техническом задании, не являются основанием для

отрицательной оценки результатов эксплуатации и испытаний. Они могут быть удовлетворены по дополнительному соглашению в согласованные сроки.

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

К моменту окончания периода опытной эксплуатации обслуживающий персонал системы должен полностью овладеть практическими навыками работы с программно-техническим комплексом.

Для подготовки объекта к вводу Системы Заказчику необходимо выполнить следующие работы:

- разработать и реализовать, совместно с организацией - исполнителем, план мероприятий по подготовке объекта модернизации к внедрению Системы (подсистем);
- разработать, совместно с организацией-разработчиком, и утвердить дополнения и изменения в должностных инструкциях, определяющих работу персонала в условиях функционирования Системы;
- при необходимости внести изменения в организационную структуру предприятия с целью обеспечения необходимого количества сотрудников и технического персонала, обеспечивающего эксплуатацию Системы в соответствии с требованиями к персоналу, изложенными в разделе 4 настоящего документа;
- утвердить нормативные документы, в рамках проекта по внедрению Системы;
- приобрести, установить и протестировать технические средства, обеспечивающие функционирование Системы (подсистем), с проведением соответствующих мероприятий по защите технических средств от внешних воздействий и несанкционированного доступа;
- подготовить и оформить необходимую организационно-распорядительную документацию;
- обеспечить решение организационных вопросов по консультации и повышению квалификации сотрудников, которые будут работать с Системой;
- организовать изучение пользовательской документации Системы всеми отделами и подразделениями уполномоченного органа;
- обеспечить изучение пользователями эксплуатационной документации;
- подготовить нормативно-справочную и иную информацию и занести ее в соответствующие базы данных;
- провести контрольные испытания Системы (подсистем) совместно с исполнителем на рабочем месте администратора и пользователя Системы.
- Для подготовки объекта к вводу Системы организация-исполнитель обязана:
- разработать и реализовать совместно с организацией-заказчиком, план мероприятий по подготовке объекта к внедрению Системы (подсистем);
- разработать и обеспечить пользователей необходимой эксплуатационной документацией для работы с прикладным программным обеспечением Системы;
- провести контрольные испытания Системы (подсистем, задач) совместно с Заказчиком на рабочем месте администратора и пользователя Системы;
- обучить работе Системой ключевых пользователей;
- провести консультацию ключевых пользователей Системы.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

8.1. ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Перечень подлежащих разработке комплектов и видов документов, соответствующих требованиям O'zDSt 1985:2018, Исполнитель согласовывает с Заказчиком на основании протоколов.

Документация по СЗИ должна соответствовать РН 34-381-1022:2009. «Положение. Общие требования по организации комплексной защиты и обеспечению информационной безопасности».

Передаваемая Заказчику документация должна быть выполнена в бумажном и электронном виде на носителе.

Поставка Системы должна сопровождаться представлением комплекта документации следующего состава на русском языке:

- Руководства пользователя (в т.ч. должны быть описаны операции загрузки и ручного ввода данных, работа с отчетными формами, другими средствами отображения данных и др.);
- Руководство администратора (в т.ч. должны быть описаны порядок установки и настройки Системы - клиентской части и СУБД, порядок разграничения прав доступа и управления учетными записями пользователей, восстановления работоспособности ПО в случае сбоев, аудит и др.);
- Поставщик должен обеспечить поддержку и ведение документации в актуальном состоянии на весь срок действия договора.
- Техническое описание настроенных интеграций.

9 ИСТОЧНИКИ РАЗРАБОТКИ

Источниками разработки настоящего технического задания являются государственные отраслевые стандарты РУз, руководящие документы и методические материалы:

- О‘zDSt 1986:2018 «Информационная технология. Информационные системы. Стадии создания»;
- О‘zDSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы»;
- О‘zDSt ISO/IEC 2392-8:2015 «Информационные технологии. Информационная безопасность. Термины и определения»;
- О‘zDSt ISO/IEC 27001:2016 «Информационные технологии. Методы обеспечения безопасности системы управления информационной безопасностью. Требования»;
- О‘zDSt ISO/IEC 27002:2016 «Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью»;
- РН 45-170:2004. Руководящий документ. «Основные технические требования по созданию локальных и корпоративных ведомственных компьютерных сетей»;
- Т 45-194:2007 «Рекомендации по применению программно-аппаратных средств, обеспечивающих предотвращение актов незаконного проникновения в информационные системы».

