

«УТВЕРЖДАЮ»

Заместитель министра внутренних дел
Республики Узбекистан


_____ З.К. Курбанов
«___» _____ 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
проекта:
СОЗДАНИЕ И ВНЕДРЕНИЕ
ИНФОРМАЦИОННОЙ СИСТЕМЫ «АНТИТЕРРОР»

на _____ листах
действует с «___» _____ 2026 г.

«ВНЕСЕНО»

Начальник Службы по борьбе с
терроризмом Оперативно-
розыскного Департамента МВД
Республики Узбекистан


_____ М.Ю. Миралимов
«___» _____ 20__ г.

«СОГЛАСОВАНО»

Начальник Управления
цифровой трансформации
Департамента ЦТиПС МВД
Республики Узбекистан


_____ У.А. Адизов
«___» _____ 20__ г.

Ташкент 2026 г.

1 . ОБЩИЕ СВЕДЕНИЯ.....	5
1.1 Полное наименование системы и ее условное обозначение.....	5
1.2 Наименование организаций заказчика и разработчика системы	5
1.3 Перечень документов, на основании которых создается ИС «Антитеррор».....	5
1.4 Плановые сроки начала и окончания работ	5
1.5 Порядок оформления и предъявления результатов работ	6
2 . НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ ИС «АНТИТЕРРОР»	6
2.1 Назначение ИС «Антитеррор».....	6
2.2 Цели создания ИС «Антитеррор».....	7
2.3 Ожидаемые результаты	8
3 . ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	9
3.1 Краткие сведения об объекте автоматизации.....	9
4 . ТРЕБОВАНИЯ К ИС «АНТИТЕРРОР».....	11
4.1 Требования к ИС «Антитеррор» в целом	11
4.1.1 Требования к структуре и функционированию ИС «Антитеррор».....	13
4.1.1.1 Перечень подсистем, их назначение и основные характеристики	14
4.1.1.2 Перечень сторонних систем, с которыми должно быть обеспечено взаимодействие	15
4.1.1.3 Требования к режимам функционирования ИС «Антитеррор».....	19
4.1.1.4 Перечень и описание сценариев использования ИС «Антитеррор».....	21
4.1.1.4.1 Общий бизнес-процесс взаимодействия пользователей с ИС «Антитеррор»	22
4.1.1.5 Требования по диагностированию ИС «Антитеррор».....	29
4.1.1.6 Перспективы развития и модернизации ИС «Антитеррор».....	30
4.1.2 Требования к взаимодействию со сторонними информационными системами.....	31
4.1.2.1 Требования к способам и средствам связи для информационного обмена между компонентами ИС «Антитеррор».....	34
4.1.3 Требования к численности и квалификации пользователей.....	35
4.1.3.1 Требования к правилам работы пользователей с различными ролями	35
4.1.3.2 Требования к квалификации пользователей, порядку их подготовки и контроля знаний и навыков	36
4.1.3.3 Требуемый режим работы пользователей информационной системы.....	37
4.1.4 Показатели назначения.....	38
4.1.5 Требования к надежности.....	39
4.1.6 Требования безопасности.....	40
4.1.6.1 Требования по разграничению доступа к различным частям ИС «Антитеррор»	43
4.1.7 Требования к эргономике и технической эстетике	45
4.1.8 Требования к патентной и лицензионной чистоте.....	46
4.1.9 Требования к транспортабельности	48
4.1.10 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов ИС «Антитеррор».....	48
4.1.11 Требования по стандартизации и унификации.....	49
4.1.12 Дополнительные требования	49
4.1.13 Требования к месту выполнения работ и оказания услуг	50
4.1.14 Дополнительные требования к Исполнителю	51
4.2 Требования к функциям, выполняемым ИС «Антитеррор».....	52
4.2.1 Требования к подсистеме ведения централизованной базы данных.....	52
4.2.1.1 Требования к модулю учета лиц	52

4.2.1.2 Требования к модулю учета интернет-ресурсов	53
4.2.1.3 Требования к модулю хранения материалов.....	53
4.2.2 Требования к подсистеме информационного обмена	53
4.2.2.1 Требования к модулю территориальной маршрутизации	53
4.2.2.2 Требования к модулю запросов	54
4.2.3 Требования к подсистеме интеграции	54
4.2.3.1 Требования к модулю внешних взаимодействий	54
4.2.4 Требования к подсистеме формирования отчетности	54
4.2.4.1 Требования к модулю отчетности.....	54
4.2.5 Требования к подсистеме информационной безопасности.....	55
4.2.5.1 Требования к модулю управления доступом.....	55
4.2.5.2 Требования к модулю аудита	55
4.2.6 Требования к подсистеме администрирования	55
4.2.6.1 Требования к модулю управления справочниками	55
4.2.6.2 Требования к модулю управления картографическими данными	55
4.2.6.3 Требования к модулю системного администрирования	56
4.3 Требования к видам обеспечения.....	56
4.3.1 Требования к математическому обеспечению	56
4.3.2 Требования к информационному обеспечению	56
4.3.3 Требования к лингвистическому обеспечению.....	57
4.3.4 Требования к программному обеспечению	57
4.3.5 Требования к техническому обеспечению	59
4.3.6 Требования к метрологическому обеспечению.....	62
4.3.7 Требования к организационному обеспечению	62
4.3.8 Требования к методическому обеспечению	62
5 . СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС «АНТИТЕРРОР».	64
6 . ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС «АНТИТЕРРОР»	65
7 . ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ИС «АНТИТЕРРОР» К ВВОДУ В ДЕЙСТВИЕ	66
8 . ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ	66

Определения, обозначения и сокращения

ГОСТ/ O‘zDSt		Государственный стандарт
БД	База данных	Совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ
ТЗ	Техническое задание	Документ, используемый заказчиком в качестве средства для описания и определения задач, выполняемых при реализации договора
ПО	Программное обеспечение	Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ
ИБ	Информационная безопасность	Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки
API	Application Programming Interface	Программный интерфейс приложения
МТО		Международные террористические организации
РЭО		Радикально экстремистская организация
МВД		Министерство внутренних дел
СГБ		Служба государственной безопасности
СБТ		Служба по борьбе с терроризмом
ГУБТ		Главного управления по борьбе с терроризмом и экстремизмом

1. ОБЩИЕ СВЕДЕНИЯ

Настоящее Техническое задание проекта «Создание и внедрение информационной системы «Антитеррор»» (ИС «Антитеррор») разработано в соответствии с государственным стандартом Республики Узбекистан O‘zDSt 1987:2018 «Информационная технология. Техническое задание на создание информационной системы».

1.1 Полное наименование системы и ее условное обозначение

Полное наименование информационной системы: ИС «Антитеррор».

Условное обозначение системы: «Антитеррор», система.

1.2 Наименование организаций заказчика и разработчика системы

Заказчик – Министерство Внутренних Дел Республики Узбекистан

Адрес: Республика Узбекистан, город Ташкент, улица Юнуса Раджаби, дом 1

Телефон: +998 (71) 231-50-10

E-mail: akt@iiv.uz

Исполнитель (разработчик) – Исполнитель выбирается на основании конкурсных и/или тендерных торгов, либо иным путем, согласно нормативно-правовым актам и другим нормативным документам.

Для выполнения отдельных работ Разработчик ИС «Антитеррор» может привлекать сторонние организации в качестве соисполнителей, при обязательном согласовании с Заказчиком.

1.3 Перечень документов, на основании которых создается ИС «Антитеррор»

Основанием для разработки данного проекта является Протокол совместного совещания СГБ/МВД РУЗ №12м/07 от 14 декабря 2024 года.

Настоящее техническое задание разработано также с учётом требований Закона Республики Узбекистан от 2 июля 2019 года № ЗРУ-547 «О персональных данных», поскольку в ИС «Антитеррор» предусмотрены централизованный сбор и обработка персональных данных граждан, в том числе особых категорий персональных данных — сведений о состоянии здоровья и анатомических данных, а также биометрических данных.

Требования к обработке персональных данных приведены в подразделе 4.1.6 настоящего технического задания.

1.4 Плановые сроки начала и окончания работ

Начало работ – дата заключения договора.

Срок выполнения работ (оказания услуг) – в течение 365 (триста шестьдесят пять) рабочих дней с даты заключения договора.

Окончание работ – 365-й рабочий день с даты заключения договора. Сроки отдельных этапов приведены в разделе 5 настоящего технического задания, исчисляются в рабочих днях и отсчитываются от даты заключения договора.

1.5 Порядок оформления и предъявления результатов работ

Работы по созданию и внедрению ИС «Антитеррор» сдаются Исполнителем поэтапно в соответствии с календарным планом проекта.

Приемка отдельных этапов работ должна производиться согласно этапам календарного плана работ, утвержденного комиссией Заказчика, согласованных и подписанных Заказчиком и Исполнителем документов (протоколов совместных заседаний, дополнений к данному документу и т.д.). Приемка отдельных этапов работ должна оформляться соответствующими двухсторонними техническими актами, содержащими краткое описание выполненных работ и их результатов.

Приёмка лицензионных прав (при необходимости) осуществляется актом приёма передачи соответствующих лицензий.

Приемка ИС «Антитеррор» должна осуществляться на основании подписанных Заказчиком и каждым Исполнителем финансовых, организационно-распорядительных, программных и эксплуатационных документов. Перечень предоставляемой Заказчику документации на ИС «Антитеррор» должен быть согласован между Заказчиком и Исполнителем на этапе подписания договора на проведение работ по созданию и внедрению ИС «Антитеррор».

ИС «Антитеррор» считается полностью принятой в промышленную эксплуатацию Заказчиком с момента подписания акта приема-передачи выполненных работ.

Представление результатов работы состоит из:

1. Исполнителем внедрена ИС «Антитеррор» на объекте автоматизации и полностью протестирована ответственными специалистами Заказчика.
2. Устранение недостатков, после полного тестирования ИС «Антитеррор» (при необходимости).
3. Проведение курсов обучения для ответственных специалистов Заказчика по использованию и администрированию составляющих подсистем и модулей ИС «Антитеррор».

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ ИС «АНТИТЕРРОР»

2.1 Назначение ИС «Антитеррор»

Информационная система «Антитеррор» предназначена для осуществления всестороннего централизованного учета, систематического мониторинга и комплексного анализа информации следующих категорий:

физических лиц, в том числе лидеров, эмиссаров, вербовщиков, активных участников и рядовых членов религиозно-экстремистских организаций и международных террористических объединений, которые осуществляют целенаправленную деятельность по распространению идей религиозного экстремизма и терроризма, а также занимаются активным рекрутированием новых последователей с использованием современных возможностей глобальной сети Интернет;

Данная информационная система предназначена для существенного повышения оперативности и эффективности деятельности

правоохранительных органов в сфере своевременного выявления, предупреждения и комплексного пресечения противоправной деятельности по распространению экстремистских и террористических идей в современном информационном пространстве, а также для обеспечения информационной поддержки принятия обоснованных решений в области противодействия информационным угрозам экстремистского и террористического характера.

документально подтвержденных фактов и обстоятельств привлечения вышеуказанных лиц к различным видам ответственности, включая случаи возбуждения уголовных дел, вынесения обвинительных приговоров, наложения административных взысканий, постановки на профилактический учет в правоохранительных органах, а также применения к ним иных мер правового воздействия и общественного контроля;

электронных информационных ресурсов различных типов и форматов, в том числе веб-сайтов, персональных профилей, тематических групп, информационных каналов, виртуальных сообществ в мобильных мессенджерах, социальных сетях и видеохостингах, которые систематически используются для распространения материалов экстремистского и террористического содержания.

2.2 Цели создания ИС «Антитеррор»

Целями создания ИС «Антитеррор» являются:

концентрация сведений в отношении ранее попадавших в поле зрения органов МВД и СГБ сторонников религиозно-экстремистских и террористических организаций, зарубежных клерикальных центров, радикально настроенных лиц. В том числе вносится информация относительно ранее привлеченных к уголовной либо административной ответственности, а также профилированных членов РЭО/МТО;

накопление информации в отношении попадающих в ходе организуемых оперативно-розыскных мероприятий в поле зрения заинтересованности МВД/СГБ лиц, занимающихся распространением идей религиозного экстремизма и терроризма, радикализма, призывов к исламизации, рекрутированием новых последователей посредством сети Интернет;

по вновь выявляемым лицам вносятся полные установочные данные путем интегрирования из базы ГЦП (через ввод ПНФЛ) - ФИО, дата и место рождения, место прописки (при необходимости – род деятельности, семейное положение, наличие детей, используемые телефонные номера), сведения о принятых в отношении них мерах (взятие в проверку, возбуждение уголовных и административных дел, привлечение к уголовной либо административной ответственности, применение мер профилактического характера, не подтверждение информации);

накопление материалов (литература, видео-, аудиофайлы и т.д.);

в отношении лидеров и активистов религиозно-экстремистских и террористических структур, проповеди которых активно используются вербовщиками РЭО/МТО;

накопление информации в отношении Интернет-ресурсов (веб-сайты, профили, группы, каналы, сообщества мобильных мессенджеров, социальных сетей, видеохостингов и т.д.) экстремистской и террористической направленности с обязательным указанием их уникальных идентификационных данных (ID, URL, привязка к номеру);

координация деятельности отделов по борьбе с терроризмом и экстремизмом территориальных подразделений МВД/СГБ по ведению оперативно-розыскного производства;

повышение эффективности работы по борьбе с терроризмом и экстремизмом путем предоставления актуальной информации, минимизации дублирования проводимых мероприятий.

2.3 Ожидаемые результаты

- Повышение эффективности выявления лиц, причастных к распространению экстремистской и террористической идеологии, за счет сокращения времени на поиск и анализ информации о них не менее чем на 80%;

- Обеспечение оперативного межведомственного информационного взаимодействия подразделений МВД и СГБ путем сокращения времени передачи информации между подразделениями с нескольких дней до 1 часа;

- Увеличение результативности мероприятий по противодействию распространению экстремистской и террористической идеологии в сети Интернет за счет повышения скорости реагирования на выявленные факты не менее чем на 60%;

- Сокращение трудозатрат сотрудников подразделений по борьбе с терроризмом на ведение учета и подготовку аналитических материалов не менее чем на 50% за счет автоматизации рутинных операций;

- Обеспечение достоверности и актуальности информации об лицах и интернет-ресурсах экстремистской и террористической направленности путем внедрения механизмов верификации и регулярного обновления данных;

- Создание единого информационного пространства для всех подразделений по борьбе с терроризмом с возможностью одновременной работы не менее 1000 пользователей;

- Повышение обоснованности принимаемых решений в сфере противодействия экстремизму и терроризму за счет предоставления полной и достоверной информации в режиме реального времени.

Целевые показатели результатов, их базовые (исходные) значения и порядок измерения:

– время поиска и анализа информации о лице, причастном к распространению экстремистской и террористической идеологии:

базовое значение – 8 часов;

целевое значение – сокращение не менее чем на 80 %;

- время передачи информации между подразделениями МВД и СГБ:
базовое значение – 1 суток;
целевое значение – не более 1 часа;
- время реагирования на выявленный факт распространения экстремистских и террористических материалов в сети Интернет:
базовое значение – 2 часов;
целевое значение — сокращение не менее чем на 60 %;
- трудозатраты на ведение учёта и подготовку аналитических материалов:
базовое значение: 4 часов;
целевое значение – сокращение не менее чем на 50 %;
- количество пользователей Системы:
не менее 1000 человек, в том числе одновременно работающих — не менее 1000.

Достижение целевых значений проверяется при приёмочных испытаниях и по результатам опытной эксплуатации – по журналам Системы и контрольным выборкам не менее 100 операций по каждому показателю.

Количество одновременно работающих пользователей проверяется нагрузочным испытанием.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1 Краткие сведения об объекте автоматизации

Объектом информатизации является Служба борьбы с терроризмом МВД Республики Узбекистан – головное подразделение, осуществляющее контроль за корректной эксплуатацией информационной системы «Антитеррор».

При этом пользователями ИС «Антитеррор» будут являться специально назначенные сотрудники:

Службы по борьбе с терроризмом МВД (далее СБТ МВД) Республики Узбекистан;

Главного управления по борьбе с терроризмом и экстремизмом (далее ГУБТ СГБ);

Управлений по борьбе с терроризмом ГУВД/УВД;

Отделов по борьбе с терроризмом УСГБ, отделов (отделений, групп) БТ РУВД (РОВД, ГОВД) и районных отделов СГБ.

Ниже приведено описание предмета информатизации:

1. Процессы учета и регистрации:

- ведение учетных карточек на лиц, причастных к экстремистской и террористической деятельности
- регистрация фактов привлечения к ответственности
- учет интернет-ресурсов экстремистской направленности
- регистрация результатов проверочных мероприятий
- учет принятых мер воздействия

2. Процессы информационного обмена:

- передача информации между территориальными подразделениями

- оповещение о новых фактах и угрозах
- формирование и направление запросов
- получение ответов на запросы
- обмен оперативно значимой информацией

3. Процессы мониторинга:

- отслеживание активности лиц в сети Интернет
- мониторинг состояния выявленных интернет-ресурсов
- контроль исполнения поручений
- наблюдение за динамикой ситуации
- мониторинг результативности принимаемых мер

4. Аналитические процессы:

- анализ связей между лицами и организациями
- оценка эффективности проводимых мероприятий
- формирование статистических отчетов
- выявление новых угроз и тенденций
- прогнозирование развития ситуации

5. Процессы принятия решений:

- оценка достаточности информации
- определение необходимых мер реагирования
- выбор методов профилактического воздействия
- распределение задач между подразделениями
- контроль исполнения решений

6. Процессы информационной безопасности:

- управление доступом пользователей
- защита конфиденциальной информации
- резервное копирование данных
- аудит действий пользователей
- обеспечение целостности информации

В настоящее время деятельность подразделений МВД и СГБ по противодействию распространению экстремистской и террористической идеологии осуществляется с частичным использованием информационных технологий. Имеющаяся база данных позволяет осуществлять базовый поиск и извлечение информации, однако не обеспечивает полноценной автоматизации всех необходимых процессов.

Существующие недостатки текущей ситуации:

- отсутствие единой централизованной системы учета и мониторинга
- ограниченные возможности оперативного информационного обмена между подразделениями
- низкий уровень автоматизации аналитической работы
- отсутствие автоматизированных механизмов выявления связей между объектами учета
- недостаточная оперативность актуализации данных

- сложность формирования комплексных аналитических материалов

- высокие трудозатраты на поиск и обработку информации

Указанные недостатки обуславливают необходимость создания современной информационной системы, обеспечивающей комплексную автоматизацию всех ключевых процессов в сфере противодействия экстремизму и терроризму.

4. ТРЕБОВАНИЯ К ИС «АНТИТЕРРОР»

4.1 Требования к ИС «Антитеррор» в целом

Системная архитектура Системы должна соответствовать технологии микросервисной архитектуры построения информационных систем, иметь модульную структуру и обеспечивать выполнение следующих требований:

- обеспечение ведения единой, централизованной базы данных на уровне всех подсистем, исключение дублирования кодов, использование единого справочника ролей и полномочий пользователей;

- реализация единого средства обеспечения информационной безопасности Системы, многоуровневого администрирования с распределением полномочий между администраторами разных уровней по нисходящей «вертикали» и пользователями текущего уровня;

- обеспечение возможности взаимодействия с внешними участниками процессов по согласованному регламенту и структурным макетам обмениваемой информации;

- обеспечение возможности работы под управлением распространенных операционных систем (Linux, AIX, HP-UX, Solaris, Windows Server), базирования на стандартных интерфейсах и протоколах передачи данных;

- динамическое распределение нагрузок для сохранения работоспособности при критических нагрузках.

Система должна обеспечивать единый механизм аутентификации и авторизации пользователей.

Система должна иметь мультиязычный (узбекский (латиница), русский, каракалпакский языки) web-интерфейс взаимодействия пользователя с информационной системой с использованием веб-браузеров (Google Chrome, Opera, Internet Explorer, Mozilla Firefox, Safari и другие) не ниже версий, актуальных на начало 2024 года.

При проектировании архитектуры и программного обеспечения Системы необходимо руководствоваться следующими основными принципами, отвечающими требованиям к автоматизированным системам подобного класса:

- масштабируемость;
- информационная безопасность;
- гибкость;
- наблюдаемость;
- достоверность;
- стандартизация (унификация) и информационная совместимость.

Принцип масштабируемости

Архитектура Системы должна гарантировать сохранение работоспособности Системы при увеличении числа пользователей, возможности последующей адаптации к растущим нагрузкам и дополнительным функциям: расширяемость для обеспечения возможности подключения к вновь

появляющимся внешним системам, а также должна допускать не менее чем 3-кратное увеличение объема обрабатываемых данных при соответствующем наращивании вычислительной мощности технических средств, на которых будет функционировать Система.

Состав разрабатываемой Системы должен состоять из подсистем и модулей, обеспечивающих возможность развития Системы без изменения ранее созданных компонентов. Разработка должна обеспечивать возможность добавления новых функций без нарушения ее работоспособности. Система также должна поддерживать возможность увеличения числа пользователей.

Принцип информационной безопасности

В разрабатываемой Системе предполагается обработка, как общедоступной информации, так и конфиденциальной информации, такой как персональные данные граждан. При разработке должны быть учтены требования законодательства Республики Узбекистан, нормативно-правовые документы, регламентирующие обработку персональной информации и требования, предъявляемые к информационной безопасности государственных информационных ресурсов (систем).

Должен обеспечиваться надлежащий уровень целостности, исключительности, доступности и эффективности защиты данных от потерь, искажения, разрушения и несанкционированного использования. Безопасность системы предполагает устойчивость к атакам и защиту конфиденциальности, целостности, готовность к работе как системы, так и ее данных. Система должна использовать механизмы, обеспечивающие автоматизацию режима разграничения доступа в отношении отдельных модулей, функций и данных

Использование информации Системы требует обеспечения целостности и высокой достоверности формируемых данных. Для этого на всех этапах обработки и ввода информации необходимо использовать различные формы ее контроля, требования к которому формируются из состава решаемых задач и обрабатываемых данных. Система должна обеспечивать резервное копирование информации, и восстановление системы после сбойных или аварийных ситуаций без потери целостности данных.

Принцип гибкости

При разработке Системы должна предусматриваться возможность добавления новых компонентов без нарушения ее функционирования.

Принцип наблюдаемости

Система должна позволять отслеживать и логировать действия и обращения к данным пользователей Системы. Администраторы Системы, в соответствии с требованиями законодательства, должны иметь возможность просматривать все обращения пользователей Системы к имеющимся данным, а также полную информацию о любых действиях, совершаемых с этими данными, в рамках своих полномочий.

Принцип достоверности

Система должна гарантировать неизменность и достоверность данных, полученных от пользователей и поставщиков данных Системы, а также хранящихся в Системе, с момента поступления информации от отправителя и на протяжении всего нахождения данных в Системе, вплоть до конца срока архивного хранения.

Принцип стандартизации (унификации) и информационной совместимости

Одним из условий эффективного функционирования Системы должно быть использование стандартных комплексов технических и программных средств, унифицированных форм представления какой – либо информации, документов, использование единых государственных справочников и классификаторов.

На всех стадиях реализации проекта должна обеспечиваться унификация проектных решений, что должно обеспечиваться единообразным подходом к решению однотипных задач, унификацией технического, информационного, лингвистического, математического, информационного и организационного обеспечения.

Пользовательские интерфейсы Системы должны иметь единый стиль оформления экранных форм.

Для уменьшения количества ошибок при заполнении экранных форм, а также для облегчения процесса их заполнения, пользователю должны предлагаться возможные варианты заполнения полей формы, в том числе с использованием словарей, выпадающих списков, шаблонов данных, единой системы классификации и кодирования информации и т.д.

4.1.1 Требования к структуре и функционированию ИС «Антитеррор»

ИС «Антитеррор» представляет собой комплексное информационное решение, разрабатываемое для эффективного учета и мониторинга лиц, занимающихся распространением идей религиозного экстремизма и терроризма интернет – ресурсов и документально подтвержденных фактов, и обстоятельств привлечения вышеуказанных лиц к различным видам ответственности.

В этом разделе определены основные принципы организации работы Системы, включая ее структуру, функциональные возможности и принципы взаимодействия с пользователями и другими информационными системами (базами данных).

1. Архитектура Системы:

- Система должна быть построена на современной и гибкой архитектуре, обеспечивающей высокую производительность, масштабируемость и отказоустойчивость.

- Разделение на логические слои (представление, бизнес-логика, доступ к данным) для упрощения разработки, тестирования и поддержки.

2. Модульная структура:

- Система должна быть разделена на отдельные функциональные модули, каждый из которых отвечает за определенные этапы работы с лицами и ресурсами экстремистской направленности, а также фактами привлечения вышеуказанных лиц к различным видам ответственности (например, первичный учет и регистрация, мониторинг интернет-пространства, аналитическая обработка, межведомственное взаимодействие, формирование доказательной базы для правоохранительных органов).

- Каждый модуль должен быть независимым и гибким для обеспечения простоты разработки и поддержки.

3. Основные функциональные возможности:

Ведение централизованного учета лиц, причастных к распространению экстремистской и террористической идеологии, с отражением всей значимой информации (установочные данные, принадлежность к организациям, факты судимости, административные правонарушения, профилактический учет).

Мониторинг интернет-ресурсов экстремистской направленности с фиксацией связей между ресурсами и конкретными лицами, отслеживанием статуса ресурсов и историей принятых мер.

Автоматическое оповещение и маршрутизация информации между подразделениями с учетом территориальной принадлежности и зоны ответственности.

Формирование аналитической отчетности, выявление скрытых связей, построение прогнозных моделей развития ситуации.

Обеспечение защищенного межведомственного взаимодействия, включая формирование запросов и получение информации из внешних систем.

Накопление и систематизация материалов (документы, аудио, видео) с возможностью их категоризации и быстрого поиска.

Обеспечение информационной безопасности, включая разграничение доступа, протоколирование действий пользователей и защиту передаваемых данных.

4. Принципы взаимодействия с пользователями:

- Интуитивно понятный пользовательский интерфейс для облегчения работы с системой и минимизации времени обучения.

- Механизмы аутентификации и авторизации пользователей для обеспечения безопасности данных и контроля доступа к информации.

- Поддержка обратной связи и консультаций для пользователей, включая механизмы обращения в техническую поддержку и получения помощи.

4.1.1.1 Перечень подсистем, их назначение и основные характеристики

1. Подсистема ведения централизованной базы данных

- Модуль учета лиц;
- Модуль учета интернет-ресурсов;
- Модуль хранения материалов;

2. Подсистема информационного обмена

- Модуль территориальной маршрутизации;
- Модуль запросов;

3. Подсистема интеграции

- Модуль внешних взаимодействий;

4. Подсистема формирования отчетности

- Модуль отчетности;
- 5. Подсистема информационной безопасности**
 - Модуль управления доступом
 - Модуль аудита
- 6. Подсистема администрирования**
 - Модуль управления справочниками;
 - Модуль управления картографическими данными;
 - Модуль системного администрирования;

4.1.1.2 Перечень сторонних систем, с которыми должно быть обеспечено взаимодействие

ИС «Антитеррор» должна быть интегрирована со следующими сторонними информационными системами и базами данных через предоставляемые соответствующими разработчиками интерфейсы взаимодействия (API):

1. Системы МВД Республики Узбекистан
2. Системы Министерства юстиции Республики Узбекистан
3. Система Государственного налогового комитета Республики Узбекистан
4. Системы АО «Uzbekistan Airways»
5. Системы АО «Узбекистон темир йуллари»
6. Системы СГБ Республики Узбекистан
7. Системы Министерства здравоохранения Республики Узбекистан
8. Системы Агентства по кадастру при Министерстве экономики и финансов Республики Узбекистан
9. Системы Министерства занятости и сокращения бедности Республики Узбекистан
10. Системы Министерства высшего образования, науки и инноваций Республики Узбекистан

Список внешних интеграций

№	Тип данных	Поставщик данных
1.	Данные из системы atm.gov, информация о нотариальных действиях	Министерства юстиции Республики Узбекистан
2.	Информация о доходах и месте работы	Государственный налоговый комитет Республики Узбекистан
3.	Данные о билетах на авиатранспорт	АО «Uzbekistan Airways»
4.	Данные о билетах на железнодорожный транспорт	АО «Узбекистон темир йуллари»
5.	Пограничные данные	СГБ Республики Узбекистан
6.	Карточки здоровья и анатомические данные человека	Министерства здравоохранения Республики Узбекистан

7.	Информация о земельных участках и жилой недвижимости	Агентства по кадастру при Министерства экономики и финансов Республики Узбекистан
8.	Данные о месте работы человека	Министерства занятости и сокращения бедности Республики Узбекистан
9.	Информация об образовательных учреждениях (государственные и частные)	1. Министерства высшего образования, науки и инноваций Республики Узбекистан

Список внутренних интеграций

№	Тип данных	Поставщик данных
1.	Данные уголовно-правовой статистики, административный, розыск и т.д	Центр правовой статистики и оперативного учета информации МВД РУз
2.	«Паспор-виза» КААТ	Главное управление миграции и оформления гражданства МВД РУз
3.	База по учету лиц находящихся в пробации «Е-Пробация»	Департамент общественной безопасности МВД РУз
4.	Программное обеспечение «Папилон-Полифейс» система биометрической идентификации по лицам в реальном времени.	Главный экспертно-криминалистический центр МВД РУз

Список внешних интеграций

№	Поставщик данных	Интегрируемые данные	То что получить
1.	Министерство юстиции (atm.gov)	• сведения о нотариальных действиях; • оформленных доверенностях; • сделках купли-продажи; • наследственных делах.	• какие юридические действия совершал человек; • участвовал ли он в сделках; • есть ли подозрительные операции с имуществом
2.	Налоговый комитет	• официальные доходы; • место работы; • регистрацию ИП;	• проверить финансовое положение человека;

		• налоговую историю.	• увидеть несоответствие доходов и имущества; • подтвердить факт официальной занятости.
3.	Uzbekistan Airways	• данные о купленных авиабилетах; • маршруты перелётов; • даты вылета и прилёта	• отследить перемещения; • проверить, находился ли человек в стране или за границей; • подтвердить или опровергнуть определённые обстоятельства
4.	Узбекистон темир йуллари	• информацию о железнодорожных билетах; • маршруты поездок внутри страны.	Анализировать перемещения по регионам
5.	Пограничная служба (СГБ)	• факты пересечения границы; • даты въезда и выезда; • пункты пропуска.	• контроля миграции; • проверки выезда за границу; • установления факта нахождения в стране.
6.	Министерство здравоохранения	• медицинские карты; • сведения о состоянии здоровья; • анатомические и биометрические данные	• подтверждения личности; • судебно-медицинских проверок; • установления состояния здоровья
7.	Кадастровое агентство	• сведения о земельных участках; • данные о недвижимости;	• анализировать имущественное положение; • выявлять скрытые активы;

		• историю перехода прав собственности	• проверять законность сделок.
8.	Министерство занятости	• сведения о трудоустройстве; • статус безработного; • участие в программах занятости.	• Помогает понять социальный статус человека
9.	Министерство высшего образования	• данные об обучении; • сведения о вузах; • академический статус.	• Используется для подтверждения образования

Список внутренних интеграций

№	Поставщик данных	Интегрируемые данные	То что получить
1.	Правовая статистика МВД	• сведения о судимостях; • административные правонарушения; • данные розыска. •	• видеть криминальную историю; • формировать аналитические отчёты; • проверять статус лица. •
2.	Паспорт-виза (миграционная база)	• паспортные данные; • регистрацию; • гражданство; • миграционный статус. •	• основа идентификации личности.
3.	«Е-Пробация»	• данные о лицах на probation; • условия ограничений; • сроки контроля. •	• нужно для контроля исполнения наказаний

4.	«Папилон-Полифейс»	• биометрическую идентификацию по лицу; • сопоставление с базами розыска; • фотоархив. •	• возможность автоматического распознавания личности в реальном времени. •
----	--------------------	---	---

4.1.1.3 Требования к режимам функционирования ИС «Антитеррор»

ИС «Антитеррор» должна корректно функционировать в существующей инфраструктуре информационных технологий Заказчика в круглосуточном режиме 365 дней в году, за исключением периодов проведения плановых профилактических работ, а также устранения возникших аварийных ситуаций в корпоративной вычислительной сети, каналах связи, аппаратном, системном, программном обеспечении Заказчика.

ИС «Антитеррор» должна поддерживать следующие режимы функционирования:

штатный режим (основной режим функционирования, непрерывная круглосуточная работа);

режим регламентного обслуживания хранилища данных;

режим опытной эксплуатации;

сервисный режим;

аварийный режим.

В штатном режиме функционирования ИС «Антитеррор»:

обмен данными при взаимодействии со сторонними системами происходит по запланированному графику;

клиентская оболочка ИС «Антитеррор» и технические средства пользователей и администратора ИС «Антитеррор» обеспечивают возможность функционирования круглосуточно;

серверное программное обеспечение и технические средства обеспечивают возможность круглосуточного функционирования, с перерывами на обслуживание;

исправно работает оборудование, составляющее комплекс технических средств.

В штатном режиме ИС «Антитеррор» должна обеспечивать круглосуточное, длительно-непрерывное исправное функционирование программных и аппаратных средств при условии регулярного регламентного обслуживания и мониторинга параметров работы.

В режиме регламентного обслуживания хранилища данных ИС «Антитеррор» обеспечивается:

обновление данных (экспорт/импорт);

архивация данных (создание архивов);

создание резервной копии для обеспечения возможности восстановления ИС «Антитеррор» в аварийных ситуациях.

Режим регламентного обслуживания хранилища данных функционирует при штатном режиме. Режим применяется в строго определенное время по расписанию. Рекомендуются применять данный режим в часы минимальной нагрузки на ИС «Антитеррор» в вечернее или ночное время.

В режиме опытной эксплуатации ИС «Антитеррор»:

Режим опытной эксплуатации применяется при внедрении нового функционала модернизируемой ИС «Антитеррор» или ее подсистем (модулей).

В режиме опытной эксплуатации должны осуществляться следующие работы:

- пуск, остановка и перезапуск ИС «Антитеррор»;
- установка новых или доработанных модулей и компонентов ИС «Антитеррор»;
- модификация общесистемных ресурсов;
- выполнение регламентных операций по обслуживанию прикладной программной платформы (тестирование, резервное копирование ПО);
- настройка общих параметров прикладной программной платформы и сетевого окружения.

Работы по обновлению рекомендуется проводить в нерабочее время, когда количество пользователей ИС «Антитеррор» минимально.

В режиме опытной эксплуатации допускается останавливать работу ИС «Антитеррор» частично (подсистема или модуль) на срок не более 2 часов в рабочее время и 10 часов в нерабочее время. В рабочее время остановка работы ИС «Антитеррор» может производиться только для исправления критических ошибок, препятствующих её эксплуатации в штатном режиме.

В сервисном режиме функционирования ИС «Антитеррор»:

Сервисный режим предусматривает проведение плановых работ (техническое обслуживание, реконфигурация, обновление) на аппаратном, системном, программном обеспечении корпоративной вычислительной сети, каналов связи, серверного оборудования Заказчика.

Выполняемые работы, в общем случае, не должны приводить к остановке процесса функционирования всей ИС «Антитеррор» (или отдельных подсистем).

Регламентное обслуживание должно осуществляться обученным обслуживающим персоналом ИС «Антитеррор» в целях профилактики. Регламент обслуживания должен быть разработан на этапе технического проектирования.

По результатам работ диагностирования работоспособности ИС «Антитеррор» принимается решение о переводе ИС «Антитеррор» (или отдельных подсистем) в штатный или аварийный режим.

Работы в сервисном режиме рекомендуется проводить в нерабочее время, когда количество пользователей ИС «Антитеррор» минимально.

В аварийном режиме функционирования ИС «Антитеррор»:

Аварийный режим функционирования ИС «Антитеррор» характеризуется отказом одного или нескольких компонентов программного и (или) технического обеспечения ИС «Антитеррор», или недоступностью до устранения причин аварии и запуска ИС «Антитеррор» в штатном или сервисном режимах.

В случае перехода ИС «Антитеррор» в аварийный режим необходимо: завершить работу всех приложений, с сохранением данных; выполнить резервное копирование БД.

После этого необходимо выполнить комплекс мероприятий по устранению причины перехода ИС «Антитеррор» в аварийный режим.

Если причиной перехода в аварийный режим является устанавливаемое обновление, то должна быть запущена процедура отката к последней работоспособной версии ИС «Антитеррор».

4.1.1.4 Перечень и описание сценариев использования ИС «Антитеррор»

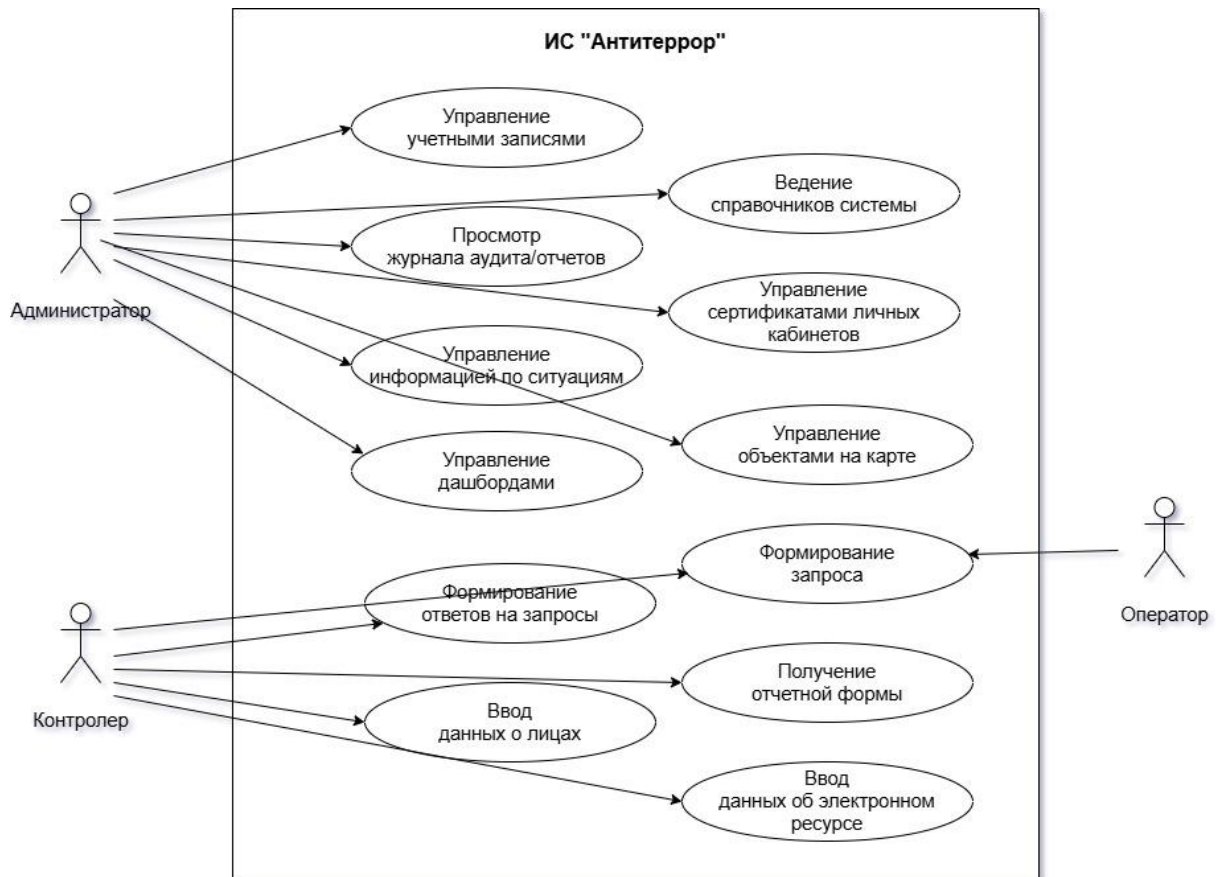


Рисунок 1. Общая UML-диаграмма сценариев использования ИС «Антитеррор»:

Список использования сценариев приведена в таблице:

ID	Наименование сценария использования	Действующие лица	Тип сценария
UC01	Управление учетными записями	Администратор	Основной
UC02	Ведение справочников системы	Администратор	Основной
UC03	Просмотр журнала аудита/отчетов	Администратор	Основной

ID	Наименование сценария использования	Действующие лица	Тип сценария
UC04	Управление сертификатами личных кабинетов	Администратор	Основной
UC05	Управление информацией по ситуациям	Администратор	Основной
UC06	Управление объектами на карте	Администратор	Основной
UC07	Управление дашбордами	Администратор	Основной
UC08	Формирование запроса	Оператор, Контролер	Основной
UC09	Формирование ответов на запросы	Контролер	Основной
UC10	Получение отчетной формы	Контролер	Вспомогательный
UC11	Ввод данных о лицах	Контролер	Основной
UC12	Ввод данных об электронном ресурсе	Контролер	Основной

4.1.1.4.1 Общий бизнес-процесс взаимодействия пользователей с ИС «Антитеррор»

«UC01» Сценарий использования: Управление учетными записями

Условия запуска: возникает необходимость создания новой учетной записи пользователя, изменения прав существующего пользователя или блокировки/удаления учетной записи.

Основное действующее лицо: Администратор

Предусловия:

Администратор авторизован в системе и обладает правами управления пользователями.

Порядок выполнения сценария:

1. Администратор переходит в раздел «Пользователи».
2. Система отображает список зарегистрированных пользователей с возможностью поиска и фильтрации.
3. Администратор выбирает одно из действий:
 - создать нового пользователя;
 - отредактировать существующего;
 - заблокировать или удалить учетную запись.
4. При создании нового пользователя администратор заполняет обязательные поля (ФИО, логин, роль, подразделение и т.д.).
5. Назначаются роли и права доступа.
6. Администратор подтверждает сохранение.
7. Система проверяет корректность введенных данных и сохраняет изменения в базе данных.
8. Система выводит уведомление об успешном выполнении операции.

Альтернативные потоки:

- Если логин уже существует — система выводит сообщение об ошибке.
- Если не заполнены обязательные поля — система не позволяет сохранить запись.

Регламент времени выполнения: Сохранение изменений — не более 5 секунд.

Выходные данные: Созданная, обновленная или заблокированная учетная запись.

Возможные расширения: Поддержка двухфакторной аутентификации, интеграция с SSO.

«UC02» Сценарий использования: Ведение справочников системы

Условия запуска: возникает необходимость добавления, изменения или удаления данных в системных справочниках.

Основное действующее лицо: Администратор

Предусловия: Администратор авторизован в системе и имеет права на редактирование справочников.

Порядок выполнения сценария:

1. Администратор переходит в раздел «Справочники».
2. Система отображает перечень доступных справочников (категории, типы объектов, статусы и т.д.).
3. Администратор выбирает нужный справочник.
4. Выполняет одно из действий:
 - добавление новой записи;
 - редактирование существующей;
 - деактивация/удаление записи.
5. Вводит или изменяет данные.
6. Нажимает «Сохранить».
7. Система проверяет корректность данных и сохраняет изменения.

Альтернативные потоки:

- При попытке удаления используемой записи система выводит предупреждение.
- При дублировании значения система блокирует сохранение.

Регламент времени выполнения: Сохранение изменений — не более 5 секунд.

Выходные данные: Обновленный справочник.

Возможные расширения: Импорт данных из Excel.

«UC03» Сценарий использования: Просмотр журнала аудита и отчетов

Условия запуска: необходимо проверить действия пользователей или сформировать отчет за определенный период.

Основное действующее лицо: Администратор

Предусловия: В системе ведется журнал аудита.

Порядок выполнения сценария:

1. Администратор открывает раздел «Журнал аудита».
2. Система отображает список событий (вход в систему, изменения данных, удаление записей и др.).
3. Администратор задает параметры фильтрации:
 - период времени;
 - конкретного пользователя;
 - тип действия.
4. Нажимает кнопку «Сформировать отчет».
5. Система обрабатывает запрос и выводит отфильтрованные данные.
6. При необходимости администратор выгружает отчет в файл (PDF/Excel).

Альтернативные потоки:

- Если за выбранный период нет данных — система выводит уведомление «Данные отсутствуют».
- При большом объеме данных формирование может происходить с индикатором загрузки.

Регламент времени выполнения: Формирование отчета — не более 6 секунд.

Выходные данные: Отчет с перечнем действий пользователей.

Возможные расширения: Автоматическая отправка отчетов на электронную почту по расписанию.

«UC04» Сценарий использования: Управление сертификатами личных кабинетов

Условия запуска:
Требуется выпуск, продление, блокировка или отзыв сертификата пользователя.

Основное действующее лицо: Администратор

Предусловия: Пользователь зарегистрирован в системе.

Порядок выполнения:

1. Администратор открывает раздел «Сертификаты».
2. Выбирает конкретного пользователя.
3. Просматривает текущий статус сертификата.
4. Выполняет одно из действий:
 - выпуск нового сертификата;
 - продление срока действия;
 - отзыв или блокировка.
5. Подтверждает действие.
6. Система обновляет статус сертификата.

Альтернативные потоки:

- Если сертификат уже активен — система предупреждает.
- При технической ошибке операция отменяется.

Регламент времени выполнения: Обновление статуса — не более 5 секунд.

Выходные данные: Актуальный статус сертификата.

Возможные расширения: Автоматическое уведомление о завершении срока действия.

«UC05» Сценарий использования: Управление информацией по ситуациям

Условия запуска: необходимо внести новую информацию о ситуации или скорректировать существующую.

Основное действующее лицо: Администратор

Предусловия: Система функционирует корректно.

Порядок выполнения:

1. Переход в раздел «Ситуации».
2. Выбор действия: создать, изменить или закрыть ситуацию.
3. Заполнение или корректировка данных:
 - описание ситуации;
 - статус;
 - дата и время;
 - ответственные лица.

4. Сохранение изменений.

5. Система фиксирует обновления.

Альтернативные потоки:

- При отсутствии обязательных данных сохранение невозможно.
- При изменении статуса система фиксирует изменение в журнале аудита.

Регламент времени выполнения: Сохранение — не более 5 секунд.

Выходные данные: Актуальная информация по ситуации.

Возможные расширения: Прикрепление документов и фото.

«UC06» Сценарий использования: Управление объектами на карте

Условия запуска: требуется добавить новый объект на карту или изменить данные существующего.

Основное действующее лицо: Администратор

Предусловия: Картографический модуль подключен и функционирует корректно.

Порядок выполнения сценария:

1. Администратор открывает модуль карты.
2. Система отображает интерактивную карту с уже нанесенными объектами.
3. Администратор выбирает действие:
 - добавить новый объект;
 - изменить существующий;
 - удалить объект.
4. При добавлении нового объекта:
 - указывается местоположение (клик по карте или ввод координат);
 - заполняются атрибуты объекта (название, тип, описание и др.).

5. Администратор сохраняет изменения.
6. Система записывает данные в базу и отображает объект на карте.

Альтернативные потоки:

- Если координаты указаны некорректно — система выводит сообщение об ошибке.
- При отсутствии соединения с сервером — отображается уведомление о невозможности сохранения.

Регламент времени выполнения: Отображение нового объекта — не более 6 секунд.

Выходные данные: Объект отображается на карте и доступен для дальнейшей работы.

Возможные расширения: Импорт объектов из внешних файлов (GeoJSON, Excel).

«UC07» Сценарий использования: Управление дашбордами

Условия запуска: требуется создать новый дашборд или изменить существующий.

Основное действующее лицо: Администратор

Предусловия:

Данные для аналитики доступны в системе.

Порядок выполнения:

1. Администратор открывает раздел «Дашборды».
2. Выбирает создание нового или редактирование существующего дашборда.
3. Добавляет виджеты (графики, таблицы, индикаторы).
4. Настраивает источники данных и параметры отображения.
5. Сохраняет конфигурацию.
6. Система формирует и отображает обновленный дашборд.

Альтернативные потоки:

- При отсутствии данных виджет отображается пустым.
- При ошибке конфигурации система уведомляет пользователя.

Регламент времени выполнения: Отображение обновленного дашборда — не более 5 секунд.

Выходные данные: Настроенная аналитическая панель.

Возможные расширения: Персонализация дашбордов для разных ролей.

«UC08» Сценарий использования: Формирование запроса

Условия запуска: Оператор или Контролер инициирует новый служебный запрос.

Основное действующее лицо: Оператор, Контролер

Предусловия: Пользователь авторизован в системе.

Порядок выполнения сценария:

1. Пользователь открывает раздел «Запросы».
2. Нажимает кнопку «Создать запрос».
3. Система открывает форму ввода данных.

4. Пользователь заполняет обязательные поля:

- тема запроса;
- описание;
- приоритет;
- прикрепленные файлы (при необходимости).

5. Нажимает «Отправить».

6. Система регистрирует запрос, присваивает уникальный номер и сохраняет в базе данных.

7. Пользователь получает уведомление о регистрации.

Альтернативные потоки:

- Если обязательные поля не заполнены — система подсвечивает ошибки.
- При техническом сбое запрос не регистрируется и выводится сообщение.

Регламент времени выполнения: Регистрация запроса — не более 5 секунд.

Выходные данные: Зарегистрированный запрос с уникальным номером.

Возможные расширения: Автоматическое назначение исполнителя по категории.

«UC09» Сценарий использования: Формирование ответов на запросы

Условия запуска: Зарегистрирован запрос, требующий рассмотрения.

Основное действующее лицо: Контролер

Предусловия: Запрос находится в статусе «В работе».

Порядок выполнения:

1. Контролер открывает список входящих запросов.
2. Выбирает конкретный запрос.
3. Анализирует содержание и приложенные материалы.
4. Формирует текст ответа.
5. При необходимости прикрепляет файл.
6. Нажимает «Отправить».
7. Система меняет статус запроса на «Исполнен» или «Ответ направлен».

Альтернативные потоки:

- При отсутствии ответа система не позволяет изменить статус.
- Возможность возврата запроса на доработку.

Регламент времени выполнения: Отправка ответа — не более 6 секунд.

Выходные данные: Отправленный ответ и измененный статус запроса.

Возможные расширения: Согласование ответа с руководителем.

«UC10» Сценарий использования: Получение отчетной формы

Условия запуска: необходимо сформировать отчет по заданным параметрам.

Основное действующее лицо: Контролер

Предусловия: В системе имеются данные за выбранный период.

Порядок выполнения:

1. Контролер переходит в раздел «Отчеты».
2. Выбирает тип отчета.
3. Указывает параметры (период, регион, категория).
4. Нажимает «Сформировать».
5. Система обрабатывает данные и формирует отчет.
6. Пользователь просматривает отчет или скачивает файл.

Альтернативные потоки:

- При отсутствии данных выводится уведомление.
- При большом объеме данных отображается индикатор загрузки.

Регламент времени выполнения: Формирование отчета — не более 6 секунд.

Выходные данные: Сформированный отчет (PDF, Excel).

Возможные расширения: Автоматическая отправка отчета по расписанию.

«UC11» Сценарий использования: Ввод данных о лицах

Условия запуска: Контролеру необходимо внести сведения о новом лице в систему.

Основное действующее лицо: Контролер

Предусловия: Контролер имеет права на добавление данных.

Порядок выполнения сценария:

1. Контролер открывает раздел «Лица».
2. Нажимает «Добавить запись».
3. Система отображает форму ввода данных.
4. Контролер заполняет:
 - ФИО;
 - дату рождения;
 - идентификационные данные;
 - контактную информацию.
5. Нажимает «Сохранить».
6. Система выполняет проверку корректности введенных данных.
7. При успешной проверке информация сохраняется в базе данных.
8. Отображается уведомление об успешном сохранении.

Альтернативные потоки:

- Если лицо уже существует в базе — система предупреждает о возможном дублировании.
- При некорректных данных сохранение невозможно.

Регламент времени выполнения: Сохранение записи — не более 4 секунд.

Выходные данные: Новая запись о лице в базе данных.

Возможные расширения: Автоматическая проверка данных через внешние государственные реестры.

Примечание: Заказчик по требованию Исполнителя должен предоставить разъяснения по каждому этапу процесса, а также предоставить схематичное описание процесса.

«UC12» Сценарий использования: Ввод данных об электронном ресурсе

Условия запуска: необходимо зарегистрировать новый электронный ресурс.

Основное действующее лицо: Контролер

Предусловия: Контролер имеет соответствующие права доступа.

Порядок выполнения:

1. Контролер открывает раздел «Электронные ресурсы».
2. Нажимает «Добавить ресурс».
3. Заполняет форму:
 - наименование ресурса;
 - URL;
 - описание;
 - категорию.
4. Сохраняет запись.
5. Система проверяет корректность формата URL.
6. Данные сохраняются в базе.

Альтернативные потоки:

- При некорректном формате URL система выдает ошибку.
- При дублировании ресурса выводится предупреждение.

Регламент времени выполнения: Сохранение данных — не более 4 секунд.

Выходные данные: Зарегистрированный электронный ресурс.

Возможные расширения: Автоматическая проверка доступности ресурса

4.1.1.5 Требования по диагностированию ИС «Антитеррор»

Каждый компонент ИС «Антитеррор» должен предоставлять инструменты диагностирования основных процессов, и мониторинг их выполнения. Компоненты должны предоставлять удобный интерфейс для возможности просмотра диагностических событий, мониторинга процессов функционирования.

Диагностирование прикладных программных средств должно предусматривать проверку работоспособности компонентов ИС «Антитеррор». При возникновении аварийных ситуаций, либо ошибок в программном обеспечении, диагностические инструменты должны позволять сохранять полный набор информации, необходимой для идентификации проблемы.

Для обеспечения высокой надежности функционирования компонентов ИС «Антитеррор» должно обеспечиваться выполнение требований по диагностированию ее состояния.

В процессе эксплуатации компонентов ИС «Антитеррор», тестирование и диагностика программно-технических комплексов должны

осуществляться системными администраторами в автоматическом режиме при их запуске.

Для всех технических компонентов силами Заказчика необходимо обеспечить регулярный и постоянный контроль состояния и техническое обслуживание. В целях оперативного информирования администраторов ИС «Антитеррор» о возникновении нештатных ситуаций, кроме экранных информационных сообщений, в компонентах ИС «Антитеррор» должны быть разработаны и внедрены механизмы оповещения посредством электронной почты и/или смс-оповещение.

4.1.1.6 Перспективы развития и модернизации ИС «Антитеррор»

При разработке компонентов ИС «Антитеррор» должны быть предусмотрены возможности их последующей модернизации и развития в ходе появления новых задач, изменений в регулирующих нормативных документах и т.д. при минимальных временных и финансовых затратах по следующим направлениям:

Масштабируемость и производительность

Система должна быть спроектирована с учетом потенциального роста объемов данных и количества пользователей. Для этого необходимо предусмотреть возможности для горизонтального и вертикального масштабирования.

Перспективы:

- Горизонтальное масштабирование: Внедрение дополнительных серверов и ресурсов для распределения нагрузки.
- Вертикальное масштабирование: Увеличение мощности существующих серверов (увеличение оперативной памяти, процессорных мощностей и емкости хранилищ).
- Оптимизация производительности: Регулярное проведение анализа производительности и оптимизация запросов к базе данных.

Интеграция с новыми источниками данных

Система должна поддерживать возможность интеграции с новыми внешними информационными системами для расширения функциональности и улучшения качества данных.

Перспективы:

- Добавление новых источников данных: Интеграция с дополнительными информационными системами государственных органов (базы данных миграционной службы, пограничного контроля, таможни) и операторов связи для расширения возможностей мониторинга и анализа деятельности лиц, причастных к распространению экстремистской идеологии, а также для повышения эффективности выявления и пресечения деятельности экстремистских организаций в информационном пространстве.
- Улучшение существующих интеграций: Оптимизация и автоматизация процессов интеграции с существующими источниками данных.

Расширение функциональности Системы

Система должна поддерживать возможность добавления новых функциональных модулей и сервисов в соответствии с меняющимися потребностями пользователей.

Перспективы:

- Разработка новых модулей: Внедрение новых функциональных модулей, таких как модули прогнозирования и аналитики, на основе машинного обучения и искусственного интеллекта.

- Расширение аналитических возможностей: Улучшение возможностей для анализа данных, создание новых отчетов и дашбордов.

Обновление и модернизация технических средств

Регулярное обновление аппаратного обеспечения и инфраструктуры для обеспечения безопасности и надежности Системы.

Перспективы:

- Модернизация серверного оборудования: Обновление серверов и систем хранения данных для повышения их производительности и надежности.

- Внедрение новых технологий: Использование современных технологий для улучшения отказоустойчивости и масштабируемости Системы.

Улучшение безопасности и защиты данных

Система должна обеспечивать высокие стандарты безопасности и защиты данных, чтобы соответствовать требованиям законодательства и ожиданиям пользователей.

Перспективы:

- Внедрение новых методов защиты: Использование современных методов шифрования и многофакторной аутентификации.

- Обновление политики безопасности: Регулярный пересмотр и обновление политик безопасности в соответствии с новыми угрозами и уязвимостями.

Функциональные изменения, расширения ИС «Антитеррор» могут быть осуществлены Разработчиком в рамках отдельных договоров на функциональное расширение или в рамках технического сопровождения по согласованию с Заказчиком.

4.1.2 Требования к взаимодействию со сторонними информационными системами

При обеспечении совместимости системы с другими информационными системами и базами данных, должны соблюдаться требования государственного стандарта О‘zDSt 2590:2012 «Информационная технология. Требования к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы», в том числе в части:

- применения единых форматов и структур передаваемых данных, обеспечивающих информационную совместимость взаимодействующих систем;

- регламентации порядка информационного обмена двусторонними соглашениями (регламентами) между Заказчиком и владельцем каждой интегрируемой системы, определяющими состав, объём, периодичность и условия передачи данных;

- применения единых государственных классификаторов и справочников при передаче данных;

- обеспечения юридической значимости передаваемых данных средствами электронной цифровой подписи в соответствии с O'z DSt 1092:2009;

- протоколирования всех операций информационного обмена с фиксацией состава переданных данных, инициатора операции, даты и времени.

Взаимодействие с системами «Электронного правительства» должно обеспечиваться на следующих условиях:

- получение сведений из центральных баз данных системы «Электронное правительство» осуществляется через межведомственную интеграционную платформу по запросу в отношении конкретного объекта учёта и в объёме, необходимом для выполнения функций Системы; полное копирование (репликация) центральных баз данных в Систему не допускается;

- условия хранения, использования и уничтожения полученных из центральных баз данных сведений определяются соглашением между Заказчиком и владельцем соответствующей центральной базы данных;

- каждое обращение к центральным базам данных фиксируется в журнале аудита Системы с указанием пользователя, основания запроса, состава полученных данных, даты и времени;

- при недоступности интегрируемой системы Система должна сохранять работоспособность в части собственных функций, информировать пользователя о недоступности источника и обеспечивать повторное выполнение запроса после восстановления связи.

Для обеспечения эффективной интеграции ИС «Антитеррор» с внешними системами необходимо предусмотреть ряд требований, которые обеспечат надежность, безопасность и согласованность данных. Ниже описаны ключевые требования к взаимодействию со сторонними информационными системами:

Поддержка стандартных протоколов обмена данными

Система должна поддерживать стандартные протоколы обмена данными для обеспечения совместимости с различными внешними системами.

Требования:

- REST API: Система должна предоставлять и поддерживать RESTful API для взаимодействия с внешними системами. API должен быть хорошо документирован и поддерживать методы HTTP (GET, POST, PUT, DELETE).

- Все REST интерфейсы должны сопровождаться спецификацией OpenAPI 3.0, размещённой в репозитории документации и доступной по

URL <https://api.example.gov/docs>. OpenAPI должен содержать модели запросов/ответов, описания ошибок и примеры payload. Изменения в спецификации публикуются в репозитории с отметкой версии;

- Операции создания (POST) должны поддерживать заголовок Idempotency-Key. При повторном получении запроса с тем же ключом система должна возвращать одно и то же итоговое состояние и тот же response-id;

- SOAP: Система должна поддерживать протокол SOAP для взаимодействия с системами, использующими этот протокол.

- JSON и XML: Система должна поддерживать обмен данными в форматах JSON и XML для обеспечения гибкости и совместимости с различными системами.

Безопасность взаимодействия

Для обеспечения безопасности передачи данных между Системой и внешними системами и базами данных необходимо использовать современные методы защиты данных.

Требования:

- SSL/TLS: Все взаимодействия с внешними системами должны быть защищены с использованием протоколов SSL/TLS для шифрования данных при передаче.

- OAuth 2.0: для аутентификации и авторизации при доступе к API системы должен использоваться протокол OAuth 2.0. Это обеспечит безопасный доступ к данным и предотвратит несанкционированный доступ.

- IP-белые списки: Взаимодействие с внешними системами должно быть ограничено до доверенных IP-адресов, указанных в белом списке.

Надежность и отказоустойчивость

Система должна обеспечивать надежное и бесперебойное взаимодействие с внешними системами, минимизируя риски потери данных и сбоев.

Требования:

- Очереди сообщений: для обеспечения надежного обмена данными и обработки данных в асинхронном режиме должны использоваться очереди сообщений, такие как Apache Kafka или RabbitMQ.

- Механизмы повторной отправки: В случае неудачной попытки передачи данных должны быть предусмотрены механизмы повторной отправки данных, чтобы гарантировать доставку информации.

- Мониторинг и логирование: Все взаимодействия с внешними системами должны быть тщательно логированы и мониторингованы для своевременного выявления и устранения проблем.

Совместимость и интеграция

Система должна быть совместима с различными внешними информационными системами и обеспечивать возможность интеграции с ними.

Требования:

- Гибкость интеграции: Система должна поддерживать интеграцию с различными типами внешних систем (базы данных, веб-сервисы, файловые системы и т.д.).

- Конфигурация и настройка: Взаимодействие с внешними системами должно быть легко настраиваемым и конфигурируемым через административный интерфейс.

- Тестирование интеграции: перед запуском Системы необходимо провести тестирование всех интеграций с внешними системами и базами данных для обеспечения их корректной работы.

Управление версиями API

Для обеспечения совместимости и возможности модернизации системы необходимо предусмотреть управление версиями API.

Требования:

- Версионирование API: API Системы должно поддерживать управление версиями, чтобы изменения в API не нарушали работу существующих интеграций.

- Документация: Должна быть доступна подробная документация по каждой версии API, включая примеры использования и описание методов.

Типы обмена данными:

Поддерживается комбинированный подход, включающий Межведомственную сеть передачи данных (МСПД) электронного правительства для автоматизированного взаимодействия в реальном времени, а также файловый обмен для передачи больших объемов данных или работы с системами, не поддерживающими онлайн-интеграцию.

Режимы обмена информацией:

Реализуется гибридный подход, предусматривающий односторонний (получение или отправка данных) и двусторонний обмен информацией между внешними системами в зависимости от их функциональных возможностей и потребностей интеграции.

Техническая реализация:

Разработчик обязан создать технологическую инструкцию (ТИ) и прикладной программный интерфейс (API), обеспечивающие безопасный, стабильный и удобный для использования обмен данными между Системой и внешними источниками.

4.1.2.1 Требования к способам и средствам связи для информационного обмена между компонентами ИС «Антитеррор»

Информационный обмен в ИС «Антитеррор» должен обеспечиваться с помощью современных протоколов и форматов передачи данных. Для организации информационного обмена должны использоваться только документированные программные интерфейсы. Не допускается прямой вызов функций и данных одного программного модуля из другого, минуя документированный интерфейс или протокол обмена.

Форматы данных должны быть разработаны на этапах проектирования компонентов ИС «Антитеррор» и отражены в документе «Техно-рабочий проект».

Информационный обмен между компонентами ИС «Антитеррор» должен включать в себя сетевой режим передачи информации, предполагающий использование локальной сети, в которой данные передаются по протоколам SOAP/HTTP.

Для доступа к основным компонентам ИС «Антитеррор» из сети Интернет они должны быть помещены в демилитаризованную зону (DMZ) и отделены от других компонентов локальной сети межсетевым экраном.

Связь всех компонентов ИС «Антитеррор» должна осуществляться по выделенным (арендованным) каналам связи, ЛВС и по каналам сети Интернет с образованием VPN и обеспечением требуемых режимов безопасности.

4.1.3 Требования к численности и квалификации пользователей

Общее количество пользователей информационной системы составляет не менее 1000 человек. Система должна обеспечивать одновременную работу не менее 1000 пользователей.

Указанное значение является единым для настоящего технического задания и соответствует показателю, приведённому в подразделе 2.3.

4.1.3.1 Требования к правилам работы пользователей с различными ролями

Пользователи информационной системы распределяются по следующим ролям в разрезе региона:

1. Администратор
2. Оператор
3. Контролёр

Наименования ролей пользователей соответствуют перечню действующих лиц сценариев использования, приведённому в подразделе 4.1.1.4, и требованиям к модулю управления доступом (подраздел 4.2.5.1). Роли назначаются в разрезе региона и подразделения МВД/СГБ Республики Узбекистан.

Для каждой из указанных ролей в ИС «Антитеррор» предусмотрены следующие права и не только:

В задачи администратора входит установка и поддержание работоспособности программного обеспечения и компьютерной техники информационной системы, создание учётных записей пользователей, заполнение справочников, создание и восстановление резервных копий, просмотр журнала аудита, управление сертификатами личных кабинетов верифицированных пользователей и др.

В задачи оператора входит ввод, изменение, формирование запросов на проверку по базе данных информационной системы.

В задачи контролёра помимо функций оператора входит также формирование ответов на запросы на проверку по базе данных информационной системы, а также получение отчетной формы, имеющейся в базе данных.

4.1.3.2 Требования к квалификации пользователей, порядку их подготовки и контроля знаний и навыков

Требования к квалификации пользователей, порядку их подготовки и контроля знаний и навыков:

1. Общие требования ко всем категориям пользователей:

- Наличие базовых навыков работы с персональным компьютером
- Знание правил информационной безопасности при работе с конфиденциальной информацией
- Понимание нормативно-правовой базы в сфере противодействия терроризму и экстремизму
- Знание внутренних регламентов и инструкций по работе с системой

2. Требования к администраторам системы:

- Высшее техническое образование в сфере информационных технологий
- Опыт администрирования информационных систем не менее 2 лет
- Знание принципов построения защищенных информационных систем
- Навыки работы с системами управления базами данных
- Понимание принципов информационной безопасности

3. Требования к контролерам:

- Высшее образование
- Опыт работы в профильных подразделениях не менее 3 лет
- Знание методик анализа и обработки оперативной информации
- Навыки работы с аналитическими инструментами

4. Требования к операторам:

- Среднее специальное или высшее образование
- Базовые навыки работы с информационными системами
- Знание предметной области в рамках своих должностных обязанностей

5. Порядок подготовки:

- Первичное обучение при внедрении Системы:
 - Теоретическая подготовка (4 часа)
 - Практические занятия (8 часов)
 - Тестирование полученных знаний
- Периодическое повышение квалификации:
 - Ежегодные курсы обновления знаний (4 часа)
 - Практические занятия при внедрении новых функций

6. Контроль знаний и навыков:

- Входной контроль перед допуском к работе:
 - Тестирование знаний регламентов работы
 - Проверка практических навыков
 - Собеседование по вопросам информационной безопасности
- Периодический контроль:

- Ежегодная проверка знаний
- Внеплановые проверки при инцидентах безопасности
- Аттестация при изменении роли пользователя

7. Методическое обеспечение:

- Предоставление пользователям:
 - Руководств пользователя по работе с Системой
 - Регламентов и инструкций
 - Учебных материалов
 - Интерактивных обучающих курсов

8. Требования к сопровождению:

- Техническая поддержка пользователей
- Консультирование по вопросам работы с системой
- Оперативное решение возникающих проблем

4.1.3.3 Требуемый режим работы пользователей информационной системы

1. Режим работы пользователей в центральных аппаратах (СБТ МВД и ГУБТ СГБ):

- Администраторы системы:
 - Круглосуточный режим работы (24/7)
 - Организация дежурных смен
 - Постоянный мониторинг работоспособности системы
- Контролеры:
 - Рабочие дни: понедельник - пятница
 - Время работы: 09:00 - 18:00
 - Экстренный доступ в нерабочее время при чрезвычайных ситуациях

- Пользователи:
 - Рабочие дни: понедельник - пятница
 - Время работы: 09:00 - 18:00
 - Доступ в нерабочее время по согласованию с руководством

2. Режим работы пользователей в территориальных подразделениях (ГУВД/УВД, УСГБ, РУВД/РОВД/ГОВД):

- Контролеры:
 - Рабочие дни: понедельник - пятница
 - Время работы: 09:00 - 18:00
 - Оперативный доступ при необходимости
- Пользователи:
 - Рабочие дни: понедельник - пятница
 - Время работы: 09:00 - 18:00
 - Доступ в выходные дни для дежурных смен

3. Особые условия:

- Обеспечение доступа к Системе в случае чрезвычайных ситуаций вне зависимости от времени суток

- Возможность удаленного доступа для определенных категорий пользователей при соблюдении требований информационной безопасности
- Поддержка одновременной работы всех авторизованных пользователей Системы
- Возможность временного ограничения доступа пользователей при проведении регламентных работ

4. Технические требования для обеспечения режима работы:

- Обеспечение бесперебойной работы серверного оборудования в режиме 24/7
- Проведение регламентных работ по обслуживанию Системы в нерабочее время
- Резервирование каналов связи для обеспечения постоянного доступа
- Наличие резервных источников питания для критически важных компонентов Системы

4.1.4 Показатели назначения

ИС «Антитеррор» должна предусматривать возможность масштабирования по производительности и объему обрабатываемой информации без модификации ее программного обеспечения путем модернизации используемого комплекса технических средств. Возможности масштабирования должны обеспечиваться средствами используемого базового программного обеспечения.

Целевое назначение ИС «Антитеррор» должно сохраняться на протяжении всего срока эксплуатации. Срок эксплуатации определяется сроком устойчивой работы программно-аппаратных средств, своевременным проведением работ по обновлению программного обеспечения и наращиванию вычислительных мощностей по сопровождению программного обеспечения, его развитию и модернизации. При условии постоянного выполнения этих работ целевое назначение ИС «Антитеррор» должно сохраняться неограниченно долго.

При разработке компонентов ИС «Антитеррор» необходимо учитывать возможные изменения и развитие законодательства и обеспечить устойчивость ИС «Антитеррор» по отношению к таким изменениям. Необходимо предусмотреть возможность обеспечения настройки отдельных параметров ИС «Антитеррор» без перепрограммирования. Адаптация ИС «Антитеррор» должна осуществляться путем проведения параметрической настройки соответствующей функциональности компонентов ИС «Антитеррор».

Процесс настройки и адаптации должен проводиться экспертами в предметной области и программистами.

ИС «Антитеррор» должна быть реализована, как «открытая», и допускать наращивание функциональных возможностей при изменении состава и содержания технологических процедур предметной области.

ИС «Антитеррор» должна обеспечивать независимость от изменений в организационной структуре ведомств, при сохранении состава и содержания выполняемых функций.

ИС «Антитеррор» должна сохранять работоспособность при увеличении количества пользователей в пределах, поддерживаемых аппаратно–программной средой серверов и рабочих станций.

ИС «Антитеррор» должна быть спроектирована с учетом обеспечения:

- работоспособности ИС «Антитеррор» независимо от совершенствования, модернизации и наращивания информационной системы;
- возможности интеграции со сторонними информационными системами и программными продуктами;
- возможности встраивания и взаимодействия с любыми другими системами.

ИС «Антитеррор» не должна зависеть от изменения:

- ёмкости базы данных для хранения учетных сведений при расширении количества пользователей системы, а также количества их реквизитов;
- ёмкости базы данных гарантированной доставки при увеличении потока сообщений и сопутствующей информации;
- количества одновременно работающих пользователей;
- количества обрабатываемой информации.

Аппаратные и программные средства ИС «Антитеррор» должны обеспечивать возможность ее модернизации:

- при превышении ранее установленных пределов на изменяемые параметры объекта автоматизации;
- при изменении состава требований к выполняемым функциям и видам обеспечения.

Модернизация и развитие ИС «Антитеррор» должны осуществляться с учетом факторов, обеспечивающих их экономическую обоснованность, установленные сроки окупаемости и периодов морального старения.

Модернизация и развитие ИС «Антитеррор» должны проводиться экспертами в предметных областях.

Вероятностно-временные характеристики, при которых сохраняется целевое назначение ИС «Антитеррор»:

Минимальный срок эксплуатации ИС «Антитеррор»:

- ИС «Антитеррор» в целом - не менее 10 лет;
- отдельных функциональных компонентов - не менее 5 лет;
- базы данных централизованного хранилища – не менее 10 лет.

4.1.5 Требования к надежности

Для обеспечения высокой надежности ИС «Антитеррор» необходимо установить и поддерживать строгие требования к надежности как технических средств, так и программного обеспечения. Эти требования

включают в себя аспекты доступности, отказоустойчивости, безопасности и производительности ИС «Антитеррор».

ИС «Антитеррор» должна функционировать круглосуточно, в штатном режиме, кроме времени проведения работ по резервному копированию данных, восстановлению данных, смене версий программного обеспечения, других профилактических работ по техническому обслуживанию, требующих остановку технических средств в части, касающейся одного или нескольких компонентов ИС «Антитеррор».

Организационные меры по обеспечению надежности должны быть направлены на минимизацию количества пользователей для доступа к ИС «Антитеррор», а также персонала службы технической поддержки при эксплуатации и проведении работ по обслуживанию комплекса технических средств ИС «Антитеррор», минимизацию времени ремонта или замены вышедших из строя компонентов за счет:

- квалификации пользователей ИС «Антитеррор»;
- квалификации обслуживающего технического персонала;
- регламентации и нормативного обеспечения выполнения работ персонала (пользователей);
- регламентации проведения работ и процедур по обслуживанию и восстановлению компонентов ИС «Антитеррор»;
- своевременного оповещения пользователей о случаях нештатной работы компонентов ИС «Антитеррор»;
- своевременной диагностики неисправностей;
- наличия договоров на сервисное обслуживание и поддержку компонентов комплекса технических и программных средств.

Дополнительные требования к составу и количественным значениям показателей надежности, перечню аварийных ситуаций, по которым должны быть регламентированы требования к надежности, и значения соответствующих показателей, надежности технических средств и программного обеспечения, методам оценки и контроля показателей надежности на разных стадиях создания компонентов ИС «Антитеррор» будут определены на этапе реализации настоящего проекта.

4.1.6 Требования безопасности

Все технические решения, использованные в настоящем проекте, должны соответствовать общим требованиям безопасности программно – аппаратных комплексов, включая требования по монтажу, наладке, эксплуатации, обслуживанию и ремонту технических средств ИС «Антитеррор» (защита от воздействий электрического тока, электромагнитных полей, афотических шумов и т. п.), по допустимым уровням освещенности, вибрационных и шумовых нагрузок и т.д. Внедрение ИС «Антитеррор» не должно нарушать политику информационной безопасности Заказчика.

Функционирование ИС «Антитеррор» не должно наносить вреда здоровью персонала и окружающей среде. Эксплуатация компонентов ИС «Антитеррор» должна соответствовать действующим нормам и правилам

техники безопасности, пожарной безопасности и взрывобезопасности, а также охраны окружающей среды.

Эксплуатация компонентов ИС «Антитеррор» персоналом должна вестись с соблюдением общих правил техники безопасности при работе с электронно-вычислительной техникой.

Все внешние элементы технических средств, находящиеся под напряжением, должны обеспечивать защиту эксплуатируемого персонала от поражения электрическим током и иметь защиту от случайного прикосновения. Технические средства должны иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81 «Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление». Подключение электропитания к оборудованию должно выполняться в соответствии с «Правилами устройства электроустановок».

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

Дополнительные требования к безопасности при монтаже, наладке, эксплуатации, обслуживании технических средств ИС «Антитеррор» определяются в документации на соответствующее оборудование.

Безопасность также определяется наличием средств защиты от несанкционированного доступа к базам данных компонентов ИС «Антитеррор» путем поддержки многоступенчатой парольной защиты и распределения уровней доступа за счет использования стандартных средств операционных систем и внутренних средств контроля доступа, обеспечивающих высокую степень конфиденциальности.

Все действия пользователей, предусмотренные функционалом Платформы, результат этих действий, точная дата и время должны записываться в журналы действий (log-файлы) с обязательным указанием пользователя, выполнившего операцию. Никто не должен иметь права на изменение/удаление записей журналов.

Также, Система и ее сетевая инфраструктуры должны быть спроектированы с учетом указанных требований в действующих законодательствах и следующих нормативных документах:

- О‘z DSt 1092:2009 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
- О‘z DSt 1105:2009 «Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных»;
- О‘z DSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;
- О‘z DSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации»;

- О‘з DSt 2816:2014 «Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недеklarированных возможностей»;
- О‘з DSt 2817:2014 «Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации».

ИС «Антитеррор» относится к системам обработки информации ограниченного пользования.

Система является многопользовательской, пользователи имеют различные права доступа к информации, а обрабатываемая информация имеет различные уровни конфиденциальности.

Требования по защите информации от несанкционированного доступа, соответствующие присвоенному классу защищённости, должны быть реализованы в полном объёме. Применяемые средства защиты информации должны соответствовать требованиям О‘з DSt 2815:2014 (межсетевые экраны), О‘з DSt 2816:2014 (контроль отсутствия недеklarированных возможностей) и О‘з DSt 2817:2014 (средства вычислительной техники).

Требования к защите информации от несанкционированного доступа

Защита информации должна включать в себя комплекс организационных мер и программно-аппаратных методов и средств защиты информации, обеспечивающих предотвращение утечки информации и несанкционированного доступа к информационным ресурсам.

Классификация межсетевых экранов (МСЭ, файрволов, брандмауэров) по уровню защищенности от несанкционированного доступа к информации должна устанавливаться в соответствие с требованиями действующих стандартов О‘з DSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации».

Дополнительные требования по разграничению доступа к различным компонентам ИС «Антитеррор», к защите информации от несанкционированного доступа, порядку использованию средств криптографической защиты информации, по сохранности информации при авариях, к защите от влияния внешнего воздействия, защите данных от сбоев общего и специального программного обеспечения будут определены на этапе реализации настоящего проекта.

Требования к обработке персональных данных

В ИС «Антитеррор» предусмотрены централизованный сбор и обработка персональных данных граждан, в том числе особых категорий персональных данных: сведений о состоянии здоровья и анатомических данных (взаимодействие с системами Министерства здравоохранения

Республики Узбекистан) и биометрических данных (взаимодействие с программным обеспечением биометрической идентификации).

Обработка персональных данных в Системе должна осуществляться в соответствии с Законом Республики Узбекистан от 2 июля 2019 года № ЗРУ-547 «О персональных данных», в том числе с соблюдением следующих требований:

- обработка персональных данных осуществляется исключительно в объёме и в целях, предусмотренных задачами Системы; сбор избыточных персональных данных не допускается;

- хранение и обработка персональных данных граждан Республики Узбекистан осуществляются на технических средствах, физически размещённых на территории Республики Узбекистан;

- доступ к персональным данным предоставляется по принципу минимально необходимых полномочий и разграничивается по ролям в соответствии с подразделом 4.1.3.1;

- каждое обращение к персональным данным фиксируется в журнале аудита с указанием пользователя, основания обращения, состава полученных данных, даты и времени; записи журнала изменению и удалению не подлежат;

- особые категории персональных данных (сведения о состоянии здоровья, анатомические и биометрические данные) должны обрабатываться с применением криптографической защиты при хранении и передаче в соответствии с O‘z DSt 1105:2009;

- передача персональных данных третьим лицам, в том числе Исполнителю, за пределы установленного Заказчиком порядка не допускается;

- сроки хранения персональных данных, порядок их обезличивания и уничтожения по достижении целей обработки определяются регламентом, разрабатываемым Заказчиком на этапе ввода Системы в действие;

- Исполнитель при выполнении работ на данных Заказчика обязан соблюдать требования Закона Республики Узбекистан № ЗРУ-547 «О персональных данных» и обеспечивать конфиденциальность персональных данных, доступ к которым он получает.

4.1.6.1 Требования по разграничению доступа к различным частям ИС «Антитеррор»

Для обеспечения безопасности и контроля доступа к различным частям ИС «Антитеррор» реализуется многоуровневая система аутентификации и авторизации пользователей.

1. Идентификация и аутентификация пользователей:

- **IP-адрес пользователя:** для повышения уровня безопасности доступ к ИС «Антитеррор» предоставляется только с авторизованных физических устройств, зарегистрированных по их IP-адресам.
- **Логин и пароль:** каждому пользователю ИС «Антитеррор» предоставляется уникальная учетная запись (логин),

защищенная паролем, соответствующим требованиям к сложности (например, длина пароля не менее 8 символов, использование букв разных регистров, цифр и специальных символов).

2. Разграничение доступа по ролям:

Доступ к различным частям ИС «Антитеррор» ограничивается на основе роли пользователя:

Администратор:

Администратор имеет полный доступ к функционалу Системы, включая:

- Управление учетными записями пользователей: создание, редактирование, блокировка и удаление аккаунтов.
- Доступ к справочникам для их наполнения и обновления.
- Просмотр и анализ журнала аудита, а также отчетов для мониторинга действий пользователей и общей работоспособности Системы.
- Управление сертификатами личных кабинетов верифицированных пользователей: их выдача, обновление или отзыв.
- Управление информацией о правонарушениях и ситуациях, включая данные из уголовного и административного кодексов.
- Управление объектами: добавление, изменение или удаление объектов, включая инфраструктурные и стратегические.
- Управление дашбордами: настройка виджетов, данных и отображения аналитической информации.

Оператор

Оператор имеет доступ к функционалу, связанному с обработкой данных и отправкой запросов:

- Доступ к интерфейсу формирования запросов: ввод данных, редактирование существующих записей и создание новых запросов для проверки информации в базе данных.
- Доступ к интерфейсу отправки запросов на проверку, включая выбор параметров и фильтров для анализа.

Контролер

Контролер обладает доступом к функциям контроля и отчетности:

- Формирование запросов для уточнения или проверки данных в системе.
- Создание ответов на запросы других пользователей (например, операторов) после анализа данных.
- Доступ к отчетным формам, их скачиванию и просмотру.
- Возможность ввода данных о физических лицах, участвующих в ситуациях, и об электронных ресурсах (например, веб-сайтах или документах).

3. Механизмы ограничения доступа:

- Доступ к отдельным модулям или функциям Системы предоставляется только в рамках роли пользователя.

- Попытки несанкционированного доступа фиксируются в журнале безопасности с указанием IP-адреса, учетной записи пользователя и времени попытки.
- Для подключения к Системе из внешних сетей используются защищенные каналы связи (VPN или шифрованные соединения).

4. Дополнительные меры безопасности:

- Регулярная смена паролей, предусмотренная политикой безопасности.
- Отключение учетных записей при многократных неудачных попытках входа.
- Проведение периодических проверок на актуальность данных, зарегистрированных IP-адресов и электронных подписей.

Данные меры направлены на обеспечение конфиденциальности, целостности и доступности информации в рамках информационной системы.

4.1.7 Требования к эргономике и технической эстетике

Принципы построения ИС «Антитеррор» должны учитывать уровень относительно низкой подготовленности конечных пользователей. Компоненты ИС «Антитеррор» должны быть простыми для освоения и исключать неопределенность при выборе решений. Для просмотра и обработки информации должен быть разработан соответствующий пользовательский интерфейс, который позволит организовать доступ пользователя в соответствующий компонент ИС «Антитеррор» с любого компьютера, имеющего доступ к нему. Для доступа к компоненту ИС «Антитеррор» через веб-расширение необходимо наличие на рабочей станции установленного интернет-браузера.

Пользовательский интерфейс по вводу/редактированию, отображению и обработке данных должен быть простой и интуитивно понятный для пользователя. Интерфейс пользователя должен включать меню сообщений для пользователя, и встроенную контекстно-зависимую помощь на узбекском (кириллица, латиница), русском языках, предоставляя пользователю возможность выбирать установку языка по умолчанию.

Компоненты ИС «Антитеррор» должны обеспечивать удобный и однозначный интерфейс для работы со всем предоставляемым функционалом. Дизайнерские решения должны использовать достижения современной эргономики и дизайна и наиболее эффективно создавать положительную эмоциональную реакцию у пользователей.

Дополнительные требования к эргономике и технической эстетике компонентов ИС «Антитеррор» будут определены на этапе реализации настоящего проекта.

4.1.8 Требования к патентной и лицензионной чистоте

Система должна отвечать требованиям по патентной чистоте, согласно действующему законодательству Республики Узбекистан. Реализация технических, программных, организационных и иных решений, предусмотренных разработкой Системы, не должна приводить к нарушению авторских и смежных прав третьих лиц.

Патентная чистота ИС «Антитеррор» и ее компонентов должна быть обеспечена в отношении патентов, действующих на территории Республики Узбекистан.

Реализация технических, программных, организационных и иных решений, предусмотренных проектом на разработку и внедрение компонентов ИС «Антитеррор», не должны приводить к нарушению авторских и смежных прав третьих лиц.

При использовании в ИС «Антитеррор» программных комплексов или компонентов, разработанных третьими лицами, условия, на которых передается право на использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию ИС «Антитеррор» по его прямому назначению.

Исключительное право владения на ИС «Антитеррор» принадлежит Заказчику – МВД Республики Узбекистан.

Условия передачи исключительных прав

Состав передаваемых объектов. Исполнитель передаёт Заказчику исключительные права на результаты интеллектуальной деятельности, созданные в рамках договора:

прикладное программное обеспечение Системы (исходные коды, объектные и исполняемые модули, сценарии сборки и развёртывания), структуру и схему базы данных, проектную, рабочую и эксплуатационную документацию, макеты и графические материалы пользовательского интерфейса, программы и методики испытаний, а также иные результаты работ, предусмотренные разделом 8 настоящего технического задания.

Объём передаваемых прав. Исключительные права передаются Заказчику в полном объёме, без ограничения по территории и сроку действия, включая право использования, воспроизведения, распространения, модификации и доработки, в том числе силами третьих лиц, тиражирования на неограниченное число рабочих мест и передачи в эксплуатацию подведомственным подразделениям Заказчика.

Момент перехода прав. Исключительные права на результаты работ по каждому этапу переходят к Заказчику с даты подписания акта приёма-передачи выполненных работ по соответствующему этапу. Исключительные права на Систему в целом переходят к Заказчику с даты подписания акта сдачи-приёмки Системы в промышленную эксплуатацию.

Порядок оформления передачи. Передача исключительных прав оформляется актом приёма-передачи исключительных прав, подписываемым одновременно с актом сдачи-приёмки Системы в промышленную эксплуатацию. К акту прилагаются перечень передаваемых

объектов и машинный носитель, содержащий исходные коды, схему базы данных, сценарии сборки и развёртывания и комплект документации. Вознаграждение за передачу исключительных прав включено в цену договора и отдельно не выплачивается.

Ограничение. Условия настоящего блока не распространяются на коммерческое (проприетарное) программное обеспечение третьих лиц, применённое в составе Системы. В отношении такого программного обеспечения Заказчику передаются права использования (лицензии) на условиях, установленных настоящим подразделом.

Гарантии Исполнителя. Исполнитель гарантирует, что передаваемые объекты созданы им самостоятельно либо права на них приобретены в объёме, достаточном для передачи Заказчику, не обременены правами третьих лиц и не нарушают исключительных прав иных лиц. При предъявлении к Заказчику претензий третьих лиц, связанных с нарушением их исключительных прав, Исполнитель урегулирует такие претензии самостоятельно и за свой счёт.

Правила и ограничения использования коммерческого программного обеспечения

В соответствии с пунктом 6.5.3.4 О‘з DSt 1987:2018 при использовании в составе ИС «Антитеррор» коммерческого (проприетарного) программного обеспечения устанавливаются следующие правила и ограничения:

- коммерческое программное обеспечение применяется только при отсутствии функционально эквивалентного свободного программного обеспечения с открытым исходным кодом, обеспечивающего выполнение требований настоящего технического задания;

- состав коммерческого программного обеспечения подлежит согласованию с Заказчиком на этапе технического проектирования; Исполнитель представляет реестр такого программного обеспечения с указанием наименования, версии, назначения, типа и количества лицензий, срока их действия, порядка взимания платы, а также условий и стоимости послегарантийной технической поддержки;

- лицензии на коммерческое программное обеспечение должны быть бессрочными (постоянными), неисключительными, оформленными на имя Заказчика, без ограничений по числу пользователей, количеству вычислительных ядер и объёму обрабатываемых данных;

- стоимость лицензий на коммерческое программное обеспечение, входящее в состав поставляемого Исполнителем прикладного решения, включается в цену договора, передача лицензий Заказчику оформляется актом приёма-передачи.

- Общесистемное и серверное (платформенное) программное обеспечение приобретается Заказчиком в соответствии с подразделом 4.3.5;

- не допускается применение программного обеспечения, требующего для работы обязательного подключения к внешним серверам за пределами контура Заказчика, передачи телеметрии, эксплуатационных или

обрабатываемых данных третьим лицам либо периодической онлайн-активации;

- не допускается применение программного обеспечения, лицензионные условия которого препятствуют использованию Системы по прямому назначению, её модернизации, масштабированию или передаче в эксплуатацию иным подразделениям Заказчика;

- коммерческое программное обеспечение не должно создавать функциональной или технологической зависимости Системы от одного поставщика: форматы хранения и обмена данными должны быть открытыми и документированными, обеспечивая возможность замены компонента на функционально эквивалентный без переработки прикладного программного обеспечения Системы;

- в случае прекращения производителем поддержки применённого коммерческого программного обеспечения в течение гарантийного срока Исполнитель обеспечивает его замену на функционально эквивалентное без дополнительных затрат для Заказчика;

- исходные коды прикладного программного обеспечения, разработанного Исполнителем в рамках настоящего проекта, передаются Заказчику в полном объёме и к коммерческому программному обеспечению не относятся.

4.1.9 Требования к транспортабельности

Требования к транспортабельности не предъявляются.

4.1.10 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов ИС «Антитеррор»

Техническое обслуживание и сопровождение компонентов ИС «Антитеррор» возлагается на персонал соответствующего подразделения Заказчика. Персонал должен иметь навыки тестирования компонентов ИС «Антитеррор» с использованием специализированного прикладного программного обеспечения, предназначенного для диагностики простейших неисправностей. Перечень простейших неисправностей, способы их устранения, простейшие операции по обслуживанию технических средств должны быть указаны в эксплуатационной документации на компоненты ИС «Антитеррор».

Режим эксплуатации и обслуживания компонентов ИС «Антитеррор» определяется режимом работы объектов автоматизации. Техническая и физическая защита компонентов ИС «Антитеррор», носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, текущее обслуживание реализуется техническими и организационными средствами, предусмотренными в ИТ инфраструктуре Заказчика.

При вводе ИС «Антитеррор» в опытную эксплуатацию должен быть разработан план выполнения диагностики, резервного копирования программного обеспечения и обрабатываемой информации. Во время промышленной эксплуатации ИС «Антитеррор», персонал, ответственный

за эксплуатацию ИС «Антитеррор», должен придерживаться разработанного плана.

Порядок регламентного обслуживания ИС «Антитеррор», его компонентов и отдельных технических средств должен определяться в эксплуатационной документации.

4.1.11 Требования по стандартизации и унификации

Применяемые при внедрении ИС «Антитеррор» технические (форматы данных, протоколы передачи и т.п.) и организационные (регламенты, требования, инструкции и т.п.) решения должны быть специфицированы и доступны для использования. Применение не специфицированных или недоступных решений не допускается.

Унификация информационной базы (нормативно-справочной информации, входных и выходных документов, описаний информационных объектов и правил задания и представления реквизитов описания этих объектов) должна обеспечивать целостность и однозначной взаимосвязи данных в базе данных ИС «Антитеррор».

При разработке компонентов ИС «Антитеррор» и моделировании процессов должна применяться унифицированная методология, а также должна максимально использоваться заложенная в поставляемом прикладном программном обеспечении функциональность.

Прикладное программное обеспечение ИС «Антитеррор» должно быть построено с использованием стандартных и унифицированных методов разработки информационных систем.

В составе ИС «Антитеррор» должны применяться типовые (унифицированные) классификаторы и справочники, действие которых на территории Республики Узбекистан определено соответствующими нормативными актами и стандартами. В компонентах ИС «Антитеррор» должна быть предусмотрена возможность наращивания классификаторов и справочников, как в отношении количества элементов, так и в части развития их структуры (развитие иерархических структур, создание дополнительных группировок и т.д.).

4.1.12 Дополнительные требования

Должны быть предусмотрены возможности модернизации компонентов ИС «Антитеррор», с целью улучшения функционала, исходя из новых функциональных модулей и сервисов в соответствии с меняющимися потребностями пользователей, увеличения объема хранимых данных, добавления новых участников бизнес-процессов и т.д.

Миграция данных из существующей системы:

1. Анализ данных существующей системы (базы данных):

- Провести аудит и анализ структуры, объема и качества данных, хранящихся в существующей системе.
- Определить данные, которые подлежат миграции, с учетом их актуальности, полноты и соответствия требованиям новой системы.

2. Подготовка данных к миграции:

- Разработать процедуры для очистки, преобразования и нормализации данных для соответствия требованиям новой системы.
- Обеспечить возможность сохранения связей между данными и их атрибутами.

3. Инструменты и технологии миграции:

- Предусмотреть разработку или использование готовых инструментов для автоматизированной миграции данных.
- Обеспечить совместимость форматов данных старой и новой системы.

4. Проверка и тестирование миграции:

- Реализовать этапы тестовой миграции данных для выявления ошибок и проверки корректности переноса.
- Организовать контрольные точки для валидации данных на каждом этапе миграции.

5. Обеспечение непрерывности работы:

- Предусмотреть поэтапную миграцию данных или миграцию в нерабочее время для минимизации влияния на текущие процессы.
- Обеспечить резервное копирование данных старой системы перед началом миграции.

6. Документирование процесса миграции:

- Разработать план миграции, включающий описание всех этапов, используемых инструментов и ожидаемых результатов.
- Обеспечить ведение отчета о выполнении миграции данных с фиксацией выявленных ошибок и способов их устранения.

Дополнительные требования по функциональным возможностям, архитектуре базы данных, дизайну и прочим вопросам не описанных в настоящем Техническом задании, могут быть реализованы в соответствующих ЧТЗ на создание и внедрение каждого компонента ИС «Антитеррор».

4.1.13 Требования к месту выполнения работ и оказания услуг

Место выполнения работ и оказания услуг: Республика Узбекистан, город Ташкент, улица Юнуса Раджаби, дом 1 – здание Министерства внутренних дел Республики Узбекистан (Служба по борьбе с терроризмом Оперативно-розыскного департамента МВД Республики Узбекистан).

Место размещения программных компонентов Системы и её баз данных: центр обработки данных Заказчика.

Размещение компонентов Системы и хранение обрабатываемых данных за пределами территории Республики Узбекистан не допускается.

По указанным адресам выполняются: обследование объекта автоматизации, установка и настройка программного обеспечения, интеграция со сторонними информационными системами, предварительные испытания, тестовая и опытная эксплуатация, обучение персонала Заказчика, сдача-приёмка Системы, а также работы по гарантийному сопровождению, требующие непосредственного доступа к инфраструктуре Заказчика.

Работы, не требующие непосредственного доступа к инфраструктуре и данным Заказчика (проектирование, разработка программного обеспечения, подготовка документации), могут выполняться по месту нахождения Исполнителя на территории Республики Узбекистан.

Доступ персонала Исполнителя на объекты Заказчика организуется Заказчиком по представленным Исполнителем спискам в соответствии с установленным пропускным режимом. Вынос носителей информации, содержащих данные Заказчика, и технической документации за пределы объектов Заказчика не допускается.

Изменение места выполнения работ допускается только по письменному согласованию с Заказчиком.

4.1.14 Дополнительные требования к Исполнителю

Помимо требований, установленных иными подразделами настоящего технического задания, Исполнитель:

- представляет перечень осуществляемых работ (оказываемых услуг) с конкретизацией их объёма и привлекаемых специалистов — состав проектной команды, квалификация каждого специалиста и трудоёмкость по этапам работ — в качестве обоснования формирования стоимости работ (услуг);

- представляет информацию об условиях лицензирования предлагаемого программного обеспечения (объём предоставления, порядок взимания платы, срок действия лицензий), а также о сервисах и подписках, включая условия и стоимость послегарантийной технической поддержки;

- обеспечивает сохранность конфиденциальной информации, к которой получает доступ при разработке, внедрении и сопровождении Системы, включая соблюдение требований к допуску своего персонала к сведениям ограниченного пользования, а также соблюдение техники безопасности своим персоналом при выполнении работ на технических ресурсах Заказчика;

- в рамках выделенного бюджета представляет полностью укомплектованное и работоспособное решение, необходимое для обеспечения полноты выполнения требований настоящего технического задания;

- в рамках выделенного бюджета вправе предложить своё аналогичное решение (в том числе с превосходящими характеристиками), которое выполняет все цели и задачи, поставленные настоящим техническим заданием, с учётом целевого назначения и установленных показателей.

Замена специалистов, заявленных в составе проектной команды, допускается только по письменному согласованию с Заказчиком при условии, что квалификация нового специалиста не ниже квалификации заменяемого.

4.2 Требования к функциям, выполняемым ИС «Антитеррор»

4.2.1 Требования к подсистеме ведения централизованной базы данных

Данная подсистема предназначена для ввода, хранения и обновления основных данных Системы.

Подсистема состоит из нижеследующих модулей:

Модуль учета лиц;

Модуль учета интернет-ресурсов;

Модуль хранения материалов.

4.2.1.1 Требования к модулю учета лиц

Модуль учета лиц должен обеспечивать:

- Ввод и редактирование обязательных установочных данных:
 - фамилия, имя, отчество;
 - дата рождения (день, месяц, год);
 - место рождения;
 - место жительства;
 - при необходимости - род деятельности, семейное положение, наличие детей;
 - используемые телефонные номера.
- Указание относимости к организации/течению:
 - «Исламское государство»;
 - «Исламское государство вelayaтa хорасан»;
 - «Катибатуль тавхид ва джихад»;
 - «Союз исламского джихада»;
 - «Джихадизм»;
 - «Салафизм»;
 - «Хизб ут-Тахрир»;
 - зарубежные клерикальные центры;
 - радикал;
 - сторонник неисламских течений.
- Учет принятых мер:
 - организация проверки;
 - заведение ОРД;
 - осуществление привода в ОВД;
 - проведение опросной беседы;
 - осмотр мобильного телефона;
 - задержание;
 - привлечение к административной ответственности;
 - возбуждение уголовного дела;
 - осуждение;
 - применение мер профилактики;
 - информация не подтвердилась.
- Фиксацию служебной информации:
 - наименование подразделения, вводящего информацию;
 - дата ввода информации;

- ФИО инициатора информации;
- телефонный номер инициатора.

4.2.1.2 Требования к модулю учета интернет-ресурсов

Модуль учета интернет-ресурсов должен обеспечивать:

- Ввод обязательных сведений:
 - название ресурса;
 - название социальной сети/мобильного мессенджера;
 - ID ресурса;
 - характер информации и относимость ресурса (аналогично списку организаций);
 - наименование подразделения, внесшего ресурс;
 - дата ввода информации;
 - ФИО инициатора ввода;
 - телефонный номер инициатора.
- При наличии сведений:
 - ФИО владельца ресурса/примерные установочные данные;
 - кличка;
 - дата рождения;
 - место рождения;
 - место жительства/примерное местонахождение;
 - известные средства связи;
 - сведения о блокировке/удалении ресурса.

4.2.1.3 Требования к модулю хранения материалов

Модуль хранения материалов должен обеспечивать:

- Загрузку и хранение:
 - литературы;
 - видео-файлов;
 - аудио-файлов;
 - материалов в отношении лидеров и активистов РЭО/МТО.
- Классификацию материалов по типам;
- Привязку материалов к конкретным лицам/ресурсам;
- Поиск по сохраненным материалам.

4.2.2 Требования к подсистеме информационного обмена

Данная подсистема предназначена для обеспечения взаимодействия между подразделениями.

Подсистема состоит из нижеследующих модулей:

Модуль территориальной маршрутизации;

Модуль запросов.

4.2.2.1 Требования к модулю территориальной маршрутизации

Модуль территориальной маршрутизации должен обеспечивать:

- Определение территориальной принадлежности по месту жительства лица;

- Автоматическое оповещение соответствующего подразделения МВД/СГБ:
 - новых внесенных лицах;
 - новых выявленных фактах;
 - необходимости проведения мероприятий.
- Контроль получения информации подразделениями.

4.2.2.2 Требования к модулю запросов

Модуль запросов должен обеспечивать:

- Формирование запроса с указанием:
 - адресата (ИС «Антитеррор»);
 - установочных данных/данных ресурса;
 - требуемой информации;
 - данных подразделения-инициатора;
 - должности и ФИО лица, санкционирующего запрос;
 - даты запроса;
 - ФИО и телефона инициатора.
- Обработку запроса в срок не более 10 дней;
- Формирование ответа:
 - при отсутствии данных - отметка «данные отсутствуют»;
 - при наличии - предоставление всей имеющейся информации;
- Контроль сроков исполнения запросов.

4.2.3 Требования к подсистеме интеграции

Данная подсистема предназначена для обеспечения взаимодействия с внешними системами и состоит из модуля внешних взаимодействий.

4.2.3.1 Требования к модулю внешних взаимодействий

Модуль внешних взаимодействий должен обеспечивать:

- Взаимодействие с информационными системами и базами данных государственных органов и организаций;
- Получение и обработку данных из внешних систем;
- Контроль достоверности получаемой информации.

4.2.4 Требования к подсистеме формирования отчетности

Данная подсистема предназначена для подготовки статистических и аналитических материалов и состоит из модуля отчетности.

4.2.4.1 Требования к модулю отчетности

Модуль отчетности должен обеспечивать:

- Формирование статистических отчетов по:
 - количеству учтенных лиц;
 - выявленным интернет-ресурсам;
 - принятым мерам;
 - результатам проверок;
- Выборку данных по различным критериям;
- Подготовку обобщенных сведений с санкции руководства.

4.2.5 Требования к подсистеме информационной безопасности

Данная подсистема предназначена для обеспечения защиты информации и управления доступом.

Подсистема состоит из нижеследующих модулей:

Модуль управления доступом;

Модуль аудита.

4.2.5.1 Требования к модулю управления доступом

Модуль управления доступом должен обеспечивать:

- Аутентификацию пользователей по логину и паролю;
- Разграничение прав доступа по ролям:
 - администратор;
 - контролер;
 - оператор.
- Контроль доступа к системе только с зарегистрированных ЭВМ.

4.2.5.2 Требования к модулю аудита

Модуль аудита должен обеспечивать:

- Протоколирование действий пользователей;
- Регистрацию событий безопасности;
- Контроль попыток несанкционированного доступа.

4.2.6 Требования к подсистеме администрирования

Данная подсистема предназначена для обеспечения управления системой.

Подсистема состоит из нижеследующих модулей:

Модуль управления справочниками;

Модуль управления картографическими данными;

Модуль системного администрирования.

4.2.6.1 Требования к модулю управления справочниками

Модуль управления справочниками должен обеспечивать:

- Ведение и актуализацию справочников:
 - организаций/течений;
 - подразделений;
 - типов мер воздействия;
 - видов ресурсов.
- Управление нормативно-справочной информацией.

4.2.6.2 Требования к модулю управления картографическими данными

Модуль управления картографическими данными должен обеспечивать:

- Управление объектами на интерактивной карте РУз:
 - добавление новых объектов (мечети, церкви, медресе);
 - ввод информации об объектах:
 - географические координаты;

- фотографии объекта;
- данные о работниках;
- вместимость;
- история постройки;
- регистрация случаев терактов:
 - координаты места происшествия;
 - описание события;
 - историческая справка;
- Редактирование и актуализацию данных об объектах;
- Управление отображением объектов на карте;

4.2.6.3 Требования к модулю системного администрирования

Модуль системного администрирования должен обеспечивать:

- Управление учетными записями пользователей;
- Мониторинг работоспособности системы;
- Создание и восстановление резервных копий;
- Настройку системных параметров.

4.3 Требования к видам обеспечения

4.3.1 Требования к математическому обеспечению

Математическое обеспечение ИС «Антитеррор» должно обеспечивать возможность использования средств шифрования, сертифицированных на соответствие действующим в Республике Узбекистан общим техническим требованиям к средствам криптографической защиты информации.

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.

Для математического обеспечения реализуемого проекта Заказчик должен предоставить соответствующую техническую и нормативную документацию (различные положения, инструкции, методики и т.д.) для решения поставленных перед соответствующим Исполнителем работ задач в части касающейся автоматизации процессов выполнения различных расчетов, анализа данных, сбора данных, шифрования данных и т.д.

4.3.2 Требования к информационному обеспечению

Состав, структура и способы организации данных в ИС «Антитеррор» должны быть определены на этапе технического проектирования соответствующего компонента ИС «Антитеррор».

Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД.

Средства СУБД, а также средства используемых операционных систем, должны обеспечивать документирование и протоколирование обрабатываемой в ИС «Антитеррор» информации.

Структура базы данных должна быть организована рациональным способом, исключающим единовременную полную выгрузку информации, содержащейся в распределенных базах данных ИС «Антитеррор».

Технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования.

В состав компонентов ИС «Антитеррор» должны входить специализированные подсистемы резервного копирования и восстановления данных.

При проектировании и развертывании компонентов ИС «Антитеррор» необходимо рассмотреть возможность использования накопленной информации из уже функционирующих информационных систем Заказчика.

Основные справочники и классификаторы в ИС «Антитеррор» должны быть едиными.

4.3.3 Требования к лингвистическому обеспечению

Используемые при разработке языки высокого уровня должны обеспечивать решение всех задач по реализации функций компонентов ИС «Антитеррор».

Все прикладное программное обеспечение компонентов ИС «Антитеррор» для организации взаимодействия с пользователем должно использовать русский, узбекский (латиница и кириллица) языки.

4.3.4 Требования к программному обеспечению

Для функционирования компонентов ИС «Антитеррор» в состав должны входить системное, прикладное и специальное программное обеспечение.

Системное ПО должно обеспечивать функционирование серверов баз данных, серверов приложений и рабочих станций пользователей, а также возможность подключения дополнительных средств защиты информации от несанкционированного доступа.

Прикладное ПО должно обеспечивать реализацию функциональных задач и возможность функционировать в среде операционной системы, дополненной средствами защиты информации от несанкционированного доступа.

Специальное ПО, состав которого определяется в процессе технического проектирования каждого компонента ИС «Антитеррор», используется в организации технической и криптографической защиты информации.

1. Общесистемное программное обеспечение

– серверная операционная система: 64-разрядная, многозадачная, с поддержкой производителем или сообществом разработчиков не менее 5 лет с даты заключения договора, со штатными средствами разграничения доступа и аудита, с поддержкой средств контейнеризации;

– клиентские рабочие места: работа с Системой осуществляется через веб-браузер без установки специализированного клиентского программного обеспечения; поддерживаются не менее трёх наиболее распространённых браузеров в версиях, выпущенных не ранее чем за 24 месяца до даты приёма;

– средства контейнеризации и оркестрации: соответствие открытой спецификации формата образов и среды выполнения контейнеров; автоматическое восстановление отказавших экземпляров и горизонтальное масштабирование без остановки Системы.

2. Серверное программное обеспечение

– веб-сервер (обратный прокси-сервер, балансировщик нагрузки): поддержка HTTP/1.1 и HTTP/2, протокола TLS версии не ниже 1.2, обслуживание не менее 1000 одновременных пользовательских сессий, распределение нагрузки не менее чем между двумя экземплярами прикладного сервера;

– система управления базами данных: реляционная, с поддержкой транзакций (свойства ACID), уровня изоляции не ниже READ COMMITTED, языка SQL по ISO/IEC 9075, потоковой репликации на резервный узел, восстановления на произвольный момент времени, секционирования таблиц, полнотекстового поиска и геопространственных типов данных; отсутствие архитектурных ограничений, препятствующих трёхкратному росту объёма обрабатываемых данных; поддержка пула соединений, обеспечивающего одновременную работу не менее 1000 пользователей;

– средство асинхронного обмена сообщениями (брокер сообщений): гарантия доставки не ниже «не менее одного раза», сохранение порядка сообщений в пределах логического раздела, хранение сообщения до подтверждения его обработки получателем, горизонтальное масштабирование;

– средства извлечения, преобразования и загрузки данных: выполнение регламентных заданий по расписанию и по событию, обработка форматов JSON и XML, ведение журнала выполнения, повторный запуск задания без потери и дублирования данных;

– средства аналитики и визуализации данных: построение отчётов и информационных панелей средствами веб-интерфейса без программирования, выгрузка результатов в форматы PDF, XLSX и CSV, разграничение доступа к отчётам по ролям, работа с базой данных Системы без создания отдельного хранилища вне контура Заказчика.

3. Прикладное программное обеспечение

– язык программирования и программный каркас серверной и клиентской частей выбираются Исполнителем при условии наличия

открытой опубликованной спецификации и поддержки не менее 5 лет с даты заключения договора;

- прикладное программное обеспечение должно иметь модульную структуру, соответствующую составу подсистем и модулей по подразделу 4.1.1.1;

- взаимодействие компонентов Системы и внешних систем обеспечивается по документированным программным интерфейсам в соответствии с подразделом 4.1.2.

4. Средства обеспечения информационной безопасности

- защита передаваемых данных: протокол TLS версии не ниже 1.2 с использованием алгоритма шифрования не ниже AES-256, механизма согласования ключей ECDHE и хеш-функции не ниже SHA-256;

- криптографическая защита информации и электронная цифровая подпись — в соответствии с O‘z DSt 1105:2009 и O‘z DSt 1092:2009;

- аутентификация и авторизация — с использованием открытых протоколов делегирования доступа (OAuth 2.0 / OpenID Connect) и с учётом требований подраздела 4.1.2 в части единой системы идентификации;

- хранение паролей — исключительно в виде необратимых хеш-значений с использованием алгоритма, устойчивого к подбору;

- глубина хранения журналов событий безопасности — не менее 12 месяцев.

5. Средства резервного копирования и восстановления

- допустимая точка восстановления (RPO) — не более 15 минут; допустимое время восстановления (RTO) — не более 2 часов;

- полное резервное копирование — не реже одного раза в неделю, инкрементальное — не реже одного раза в сутки;

- срок хранения резервных копий — не менее 12 месяцев; резервные копии хранятся на территории Республики Узбекистан отдельно от основной площадки;

- проверка восстановления из резервной копии проводится не реже одного раза в квартал с оформлением протокола;

- средства резервного копирования должны обеспечивать восстановление как базы данных целиком, так и отдельных объектов на заданный момент времени.

4.3.5 Требования к техническому обеспечению

Комплекс технических средств ИС «Антитеррор» должен быть достаточным для выполнения всех предусмотренных в нем автоматизированных функций.

В комплексе технических средств должны в основном использоваться технические средства серийного производства. При необходимости допускается применение технических средств единичного производства.

Технические средства должны быть размещены с соблюдением требований, содержащихся в технической, в том числе эксплуатационной, документации на них, и так, чтобы было удобно использовать их при

функционировании компонентов ИС «Антитеррор» и выполнять техническое обслуживание.

Размещение технических средств должно соответствовать требованиям эргономики, определенным в соответствующих стандартах.

Любое из технических средств ИС «Антитеррор» должно допускать замену его средством аналогичного функционального назначения без каких-либо конструктивных изменений или регулировки в остальных технических средствах ИС «Антитеррор» (кроме случаев, специально оговоренных в технической документации).

Предметом настоящего технического задания является создание и внедрение информационной системы. Закупка аппаратного обеспечения в объём настоящего проекта не входит.

Требования к вычислительным ресурсам (Ресурсы), необходимым для функционирования Системы, формируются Исполнителем на основании требований настоящего технического задания и представляются Заказчику в составе технического проекта не позднее 30 рабочих дней с даты заключения договора.

Закупка и поставка аппаратно-программного обеспечения, включая общесистемное и серверное (платформенное) программное обеспечение, осуществляются Заказчиком отдельно, после определения Исполнителя и получения от него согласованных требований к вычислительным ресурсам.

Зона ответственности Заказчика в части технического обеспечения

- предоставление вычислительных ресурсов (серверных мощностей, систем хранения данных, ресурсов виртуализации) в объёме, соответствующем согласованному ресурсу, в сроки, обеспечивающие выполнение календарного плана работ по разделу 5;

- предоставление инженерной инфраструктуры центра обработки данных: гарантированного электропитания и систем бесперебойного питания, климатического обеспечения, структурированной кабельной системы, систем пожарной безопасности и физической охраны;

- предоставление локальной вычислительной сети, каналов связи и сетевой связности с интегрируемыми информационными системами, а также организация сетевого доступа персонала Исполнителя к выделенным ресурсам;

- предоставление рабочих станций пользователей и периферийного оборудования;

- приобретение общесистемного и серверного (платформенного) программного обеспечения и соответствующих лицензий: операционных систем серверов, средств виртуализации, системы управления базами данных, веб-сервера, брокера сообщений, средств интеграции и формирования отчётности;

- организация пропускного режима и допуска персонала Исполнителя на объекты;

- эксплуатация, техническое обслуживание и ремонт технических средств в течение всего срока эксплуатации Системы;

- выполнение резервного копирования на предоставленных технических средствах по регламенту, разработанному Исполнителем.

Зона ответственности Исполнителя в части технического обеспечения

- разработка, обоснование и согласование с Заказчиком требований к вычислительным ресурсам, в том числе для основной и резервной площадок;
- установка, настройка и оптимизация общесистемного и прикладного программного обеспечения на предоставленных Заказчиком вычислительных ресурсах;
- обеспечение работоспособности Системы и достижения установленных показателей в пределах согласованных и фактически предоставленных вычислительных ресурсов;
- разработка программы и методики испытаний и подтверждение установленных показателей на предоставленных ресурсах;
- разработка регламентов резервного копирования, восстановления и мониторинга Системы;
- обучение персонала Заказчика администрированию Системы;
- гарантийное сопровождение Системы в части программного обеспечения.

Факт предоставления Заказчиком вычислительных ресурсов фиксируется двусторонним актом. Исполнитель не несёт ответственности за недостижение установленных показателей в случае предоставления вычислительных ресурсов в объёме меньшем, чем согласованный.

При недостаточности предоставленных ресурсов Исполнитель обязан письменно уведомить Заказчика с приложением расчёта требуемого объёма ресурсов.

Разграничение ответственности за приобретение программного обеспечения

- Исполнитель разрабатывает и внедряет прикладное программное обеспечение Системы. В цену договора включается стоимость лицензий только на коммерческое программное обеспечение, входящее в состав поставляемого Исполнителем прикладного решения;
- общесистемное и серверное (платформенное) программное обеспечение – операционные системы серверов, средства виртуализации, система управления базами данных, веб-сервер, брокер сообщений, средства интеграции и формирования отчётности приобретается Заказчиком вне рамок настоящего технического задания, одновременно с закупкой аппаратного обеспечения;
- состав и количество лицензий такого программного обеспечения определяются Заказчиком на основании требований к вычислительным ресурсам, представляемых Исполнителем на этапе технического проектирования.

4.3.6 Требования к метрологическому обеспечению

Метрологическое обеспечение ИС «Антитеррор» должно включать в себя совокупность организационных мероприятий, технических средств, требований, положений, правил, норм и методик, необходимых для обеспечения единства измерений и требуемой точности измерений и вычислений.

Состав информационных, управляющих функций ИС «Антитеррор», измеряемых параметров объектов управления, их точные характеристики, метрологические характеристики должны быть определены и согласованы Заказчиком совместно с Исполнителями работ.

Метрологическая совместимость технических средств компонентов ИС «Антитеррор» обеспечивается за счет выбора Исполнителями работ совместимых программных и технических средств разработки каждого компонента ИС «Антитеррор».

4.3.7 Требования к организационному обеспечению

Организационное обеспечение ИС «Антитеррор» должно быть достаточным для эффективного выполнения персоналом возложенных на него обязанностей при осуществлении автоматизированных и связанных с ними неавтоматизированных функций ИС «Антитеррор». Заказчиком должны быть определены должностные лица, ответственные за:

- обработку информации в ИС «Антитеррор»;
- администрирование ИС «Антитеррор»;
- обеспечение безопасности информации в ИС «Антитеррор»;
- управление работой персонала по обслуживанию ИС «Антитеррор».

4.3.8 Требования к методическому обеспечению

Компоненты ИС «Антитеррор» должны разрабатываться на основании действующих нормативных правовых актов и организационно-распорядительных документов Заказчика.

Разработка нормативно-технической документации и компонентов ИС «Антитеррор» должна вестись с учетом следующих нормативных и нормативно-правовых документов, таких как:

- О‘zDSt 1987:2018 Информационные технологии. Техническое задание на создание информационной системы.
- О‘zDSt 1986:2018 Информационные технологии. Информационные системы. Стадии создания.
- О‘zDSt 1985:2018 Информационные технологии. Виды, комплектность и обозначение документов при создании информационных систем.
- О‘zDSt 1047:2018 Информационные технологии. Термины и определения.
- О‘zDSt 2814:2014 Информационная технология, Автоматизированные системы, Классификация по уровню защищенности от несанкционированного доступа к информации.

Исполнители работ должны обеспечить обучение персонала Заказчика, включая внутренних пользователей и администраторов каждого компонента ИС «Антитеррор».

Обучение специалистов Заказчика должно проводиться по следующим направлениям:

- специалистов по сопровождению компонентов ИС «Антитеррор»;
- сотрудников, использующих компоненты ИС «Антитеррор» в своей повседневной деятельности.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС «АНТИТЕРРОР»

Реализация требований настоящего ТЗ должна проводиться в несколько этапов. Состав и содержание работ по этапам, а также сроки начала и окончания работ по созданию ИС «Антитеррор» включают работы, приведенные в таблице ниже.

Содержание работ отдельных этапов, а также сроки начала и окончания работ могут быть дополнительно уточнены между Заказчиком и Исполнителями работ в процессе технического проектирования.

Сроки этапов указаны в рабочих днях, отсчитываемых от даты заключения договора.

Общий срок выполнения работ – 365 (триста шестьдесят пять) рабочих дней с даты заключения договора.

Состав работ по реализации Проекта

№	Наименование и их содержание	Сроки выполнения		Исполнитель (организация)	Чем заканчивается этап
		начало	окончание		
1	Разработка, экспертиза и утверждение технического задания	до заключения договора		СБТ МВД РУ УЦТ МВД РУ	Утвержденное ТЗ
2	Определение Исполнителя (разработчика)	до заключения договора		ДФиМТО МВД РУ СБТ МВД РУ	Заключение соответствующего договора на разработку
3	Обследование объекта автоматизации, техническое проектирование, представление Исполнителем требований к вычислительным ресурсам	1-й день	30-й день	Исполнитель согласно контракту	Технический проект; согласованные требования к вычислительным ресурсам
4	Предоставление Заказчиком вычислительных ресурсов в соответствии с согласованными	31-й день	90-й день	СБТ МВД РУ УЦТ МВД РУ	Двусторонний акт предоставления вычислительных ресурсов

	требованиями (подраздел 4.3.5)				
5	Разработка Системы	31-й день	210-й день	Исполнитель согласно контракту	Система
6	Установка, настройка, интеграция со сторонними информационными системами, предварительные испытания и тестовая эксплуатация, доработка технических решений	211-й день	285-й день	Исполнитель согласно контракту	Тестирование Платформы в рабочих условиях Заказчика. Доработанное программное обеспечение с учетом представленных предложений и замечаний
7	Обучение ответственного персонала Заказчика	256-й день	285-й день	Исполнитель согласно контракту	Обученные специалисты Заказчика по управлению Системой
8	Опытная эксплуатация	286-й день	340-й день	Заказчик	Самостоятельное управление Системой
9	Сопровождение Системы	согласно договору	согласно договору	Исполнитель согласно контракту	Оказание технической поддержки
10	Сдача-приёмка Системы в промышленную эксплуатацию	341-й день	365-й день	СБТ МВД РУ Исполнитель согласно контракту	АКТ

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС «АНТИТЕРРОР»

Компоненты ИС «Антитеррор» должны быть подвергнуты предварительным испытаниям в соответствии с разработанными на этапах проектирования методиками испытаний. По положительным результатам предварительных испытаний компоненты ИС «Антитеррор» должны быть введена в опытную эксплуатацию.

Опытная эксплуатация компонентов ИС «Антитеррор» должна осуществляться персоналом Заказчика из числа лиц, прошедших обучение. Оценка результатов опытной эксплуатации должна быть отражена в протоколе по результатам опытной эксплуатации.

Прием проводимых работ будет осуществляться комиссией Заказчика с обязательным участием Исполнителей работ по созданию каждого компонента ИС «Антитеррор». Приемочная комиссия по приемке компонентов ИС «Антитеррор» создается Заказчиком. Руководителем приемочной комиссии назначается представитель Заказчика.

В приемочную комиссию в обязательном порядке включается представитель Исполнителя и Заказчика. Если Исполнителем в процессе создания каждого компонента ИС «Антитеррор» были привлечены любые сторонние силы на основании условий субподряда, в обязанности Исполнителя входит обеспечение присутствия представителей субподрядчиков в составе приемочной комиссии.

По результатам своей работы приемочная комиссия оформляет акт приемки работ, который подписывается всеми членами приемочной комиссии и представляется на утверждение Заказчику.

7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ИС «АНТИТЕРРОР» К ВВОДУ В ДЕЙСТВИЕ

В ходе реализации настоящего проекта на разработку и внедрение ИС «Антитеррор» на объекте автоматизации Заказчика требуется выполнить работы по подготовке к вводу каждого компонента ИС «Антитеррор» в промышленную эксплуатацию. При подготовке к вводу в промышленную эксплуатацию, Заказчик должен обеспечить выполнение следующих работ:

- определить подразделение и ответственных должностных лиц, ответственных за внедрение и проведение опытной эксплуатации;
- обеспечить присутствие пользователей для обучения работе с ИС «Антитеррор», проводимым Разработчиком;
- обеспечить соответствие помещений и рабочих мест пользователей ИС «Антитеррор» в соответствии с требованиями настоящего ТЗ на создание и внедрение ИС «Антитеррор»;
- обеспечить выполнение требований, предъявляемых к программно-техническим средствам, на которых должны быть развернуты компоненты ИС «Антитеррор»;
- совместно с Разработчиком подготовить план развертывания ИС «Антитеррор» на технических средствах Заказчика;
- провести опытную эксплуатацию.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Проектная документация должна соответствовать требованиям государственных стандартов, норм и действующего законодательства Республики Узбекистан. При разработке проектной, рабочей и эксплуатационной документации Разработчик ИС «Антитеррор» должен руководствоваться следующим государственным стандартом:

О‘zDSt 1985:2018 Информационные технологии. Виды, комплектность и обозначение документов при создании информационных систем.

Разработчик по результатам выполненных работ должен предоставить полный комплект документов, необходимых для эксплуатации соответствующего компонента ИС «Антитеррор».

Комплектность, построение и оформление технической документации на каждый компонент ИС «Антитеррор» должны быть достаточным для понимания принципов их работы, а также для администрирования и обслуживания.

В соответствии с О‘zDSt 1985:2018 в состав технической и эксплуатационной документации должны быть включены:

- 1) Руководство пользователя.
- 2) Руководство администратора Системы – документ, определяющий порядок установки, настройки и администрирования Системы.

На стадии ввода Системы в действие должны быть разработаны следующие документы:

1. Программа и методика приемочных испытаний;
2. Протокол испытаний;
3. Акт выполненных работ на этапе ввода Системы в эксплуатацию;
4. Акт о сдаче-приеме Системы в эксплуатацию.

Данный состав технической и эксплуатационной документации может быть дополнен или изменен в зависимости от разрабатываемого компонента ИС «Антитеррор».

**Перечень организаций, с которыми должен быть согласован
проект технического задания**

Наименование предприятия	Адрес
Министерство цифровых технологий Республики Узбекистан	г. Ташкент, ул. Иброхима Муминова, 4 Тел.: (998) 71-238-41-07 факс: (998) 71-239-87-82 E-mail: info@digital.uz
ГП «Центр кибербезопасности»	г. Ташкент, Мирабадский р-н, ул. Тараса Шевченко, 20 Тел.: (998) 71-203-55-11, E-mail: info@infosec.uz

СПИСОК ИСПОЛНИТЕЛЕЙ

Ответственные исполнители:

Начальник отдела УЦИиЗИ МВД
РУ

М. Мукумжонов