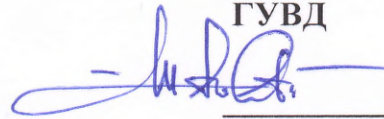


«УТВЕРЖДАЮ»

Заместитель начальника
ГУВД г. Ташкента



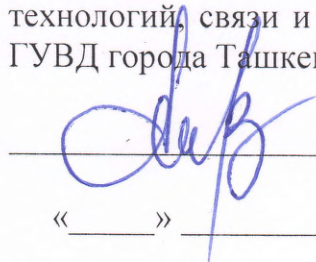
Т.Б. Холматов

« _____ » _____ 2022 г.

Техническое задание
на приобретение оборудования и программного
обеспечения для нужд ГУВД г. Ташкента
в рамках создания информационно-аналитической
системы мониторинга «Единый центр управления»
ГУВД г. Ташкента

«ВНЕСЕНО»

Начальник отдела информационных
технологий, связи и защиты информации
ГУВД города Ташкента

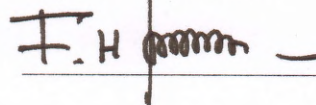


Б.П. Шакулов

« _____ » _____ 2022 г.

«СОГЛАСОВАНО»

Заместитель начальника
организационного управления ГУВД
города Ташкента



Ф.Ф. Хасанов

« _____ » _____ 2022 г.

1. ОБЩИЕ СВЕДЕНИЯ 5

Наименование.....	5
1.2. Наименование организаций заказчика.....	5
1.3. Основание и цель приобретения оборудования	5
1.4. Сроки.....	5
1.5. Порядок оформления и предъявления заказчику результатов работ по созданию ИС	5
2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ	9
2.1. Назначение.....	9
2.2. Цели создания системы.	9
3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	10
3.1. Краткие сведения об объекте автоматизации.....	10
3.2. Сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды	10
4. ТРЕБОВАНИЯ К СИСТЕМЕ	12
4.1. Требования к ИС в целом.....	12
4.1.1. Требования к структуре и функционированию ИС.....	12
4.1.1.1. Перечень систем, подсистем, их назначение	12
4.1.1.2. Требования к взаимодействию со сторонними информационными системами	13
4.1.1.3. Требования к режимам функционирования системы.....	14
4.1.1.4. Перспективы развития, модернизации системы.....	16
4.1.1.5. Общая архитектура системы	16
4.1.2. Требования к характеристикам взаимосвязей создаваемой системы со смежными системами17	
4.1.2.1. Требования к способам подключения и средствам связи	17
4.1.3. Требования к численности и квалификации пользователей	17
4.1.4. Показатели назначения.....	18
4.1.4.1. Значения параметров, характеризующих степень соответствия системы по назначению 19	
4.1.4.2. Степень приспособляемости системы к изменению процессов и методов управления, к отклонениям параметров объекта управления	21
4.1.4.3. Допустимые пределы модернизации и развития Системы	21
4.1.4.4. Вероятностно-временные характеристики, при которых сохраняется целевое назначение Системы.....	21
4.1.5. Требования к надежности.....	21
4.1.6. Требования безопасности	23
4.1.7. Требования к эргономике и технической эстетике	24
4.1.8. Требования к защите информации от несанкционированного доступа	25
4.1.9. Требования по сохранности информации при авариях.....	27
4.1.10. Требования к патентной и лицензионной чистоте	29
4.1.11. Требования по стандартизации и унификации.....	29
4.1.12. Дополнительные требования.....	30
4.1.12.1. Требования к оснащению системы устройствами для обучения персонала	30
4.2. Требования к функциям (задачам), выполняемым системой и вспомогательному оборудованию.....	32
4.2.1. Требование к модулю интеграции распознавания и регистрация номерных знаков автотранспортных средств.....	32
4.2.2. Требование к модулю интеграции видеонаблюдения	33
4.2.3. Требование к модулю интеграции видеоаналитики.....	34

4.2.4. Требование к модулю интеграции распознавание лиц	34
4.2.5. Подсистемаинформационно-аналитическая.....	34
4.2.5.1. Задачами подсистемы в целом являются:	35
4.2.5.2. Реализуемые функции подсистемы:.....	36
4.2.5.3. Дополнительный функционал:	36
4.2.6. Геоинформационная подсистема	37
4.2.6.1. Основные задачи Подсистемы	37
4.2.6.2. Требования к организации Подсистемы	37
4.2.6.3. Функциональные требования к Подсистеме.....	38
4.2.6.4. Описание технологической реализации Подсистемы	40
4.2.7. Подсистема информационно-аналитическая.....	40
4.2.7.1. Требования к подсистеме видеонаблюдения и видеоанализа.....	42
4.2.7.2. Требования к аналитическим функциям подсистемы видеоанализа.....	42
4.2.7.3. Требования к клиентскому приложению подсистемы видеоанализа для операторов системы	42
4.2.7.4. Состав анализа видеоданных.....	43
4.2.8. Модуль видеоидентификации лиц (ВИ)	43
4.2.9. Модуль видеоаналитики (ВА).....	44
4.2.10. Модуль предоставления обзорного наблюдения.....	46
4.2.11. Серверное оборудование для информационно-аналитической подсистемы	46
4.2.11.1. Дополнительные специальные требования к подсистеме хранения данных Системы	47
4.2.12. Требования к транспортированию	49
4.2.13. Гарантийные обязательства.....	49
4.2.14. Требования по ремонтпригодности.....	50
4.2.15. Требования к сервисному обслуживанию	50
4.2.16. Экологические и санитарные требования.....	50
4.3. Требования к видам обеспечения.....	50
4.3.1. Требования к математическому обеспечению.....	50
4.3.2. Требования к информационному обеспечению.....	50
4.3.3. Требования к лингвистическому обеспечению	51
4.3.4. Требования к программному обеспечению	51
4.3.5. Требования к общему программному обеспечению	52
4.3.6. Требования к техническому обеспечению.....	54
4.3.6.1. Сервер структурирования видео	54
4.3.6.2. Сервер анализ поведения человека	55
4.3.6.3. Сервер интеграции.....	57
4.3.6.4. СерверМРР база данных	58
4.3.6.5. Коммутатор на 24 порт	59
4.3.6.6. Коммутатор на 16 порт	60
4.3.6.7. Источники бесперебойного питания.....	61
4.3.6.8. Серверная стойка 42U.....	61
4.3.6.9. Серверная стойка 22U.....	61
4.3.6.10. Межсетевой экран.....	62
4.3.6.11. Экран (монитор) для видеостены	62
4.3.6.12. Матрица.....	63
4.3.6.13. Карта кодирования.....	64
4.3.6.14. Джойстик.....	64

4.3.6.15. Видеодекодер	65
4.3.6.16. Жесткий диск	66
4.3.6.17. Оптическая распределительная панель.....	66
4.3.7. Требования к метрологическому обеспечению	66
4.3.8. Требования к организационному обеспечению.....	67
4.3.9. Требования к методическому обеспечению	67
5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС.....	70
6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС	71
7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ИС К ВВОДУ В ДЕЙСТВИЕ	75
8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ.....	76

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование

Техническое задание на приобретение программного обеспечения и оборудования для нужд ГУВД г. Ташкента

Условное обозначение: ИС, Система, situation center ИС для ситуационного центра.

1.2. Наименование организаций заказчика

Заказчик: ГУВД г. Ташкента.

Адрес: Мирабадский р. ул. С. Азимова д.87.

Пользователь(и): ГУВД г. Ташкента

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

1.3. Основание и цель приобретения оборудования

- Указа Президента Республики Узбекистан «О мерах по коренному повышению эффективности деятельности органов внутренних дел, усилению их ответственности за обеспечение общественного порядка, надежной защиты прав, свобод и законных интересов граждан» от 10.04.2017 года №УП-5005;

- Постановление Президента Республики Узбекистан от 12.04.2017 года №ПП-2883 «Об организационных мерах по дальнейшему совершенствованию деятельности органов внутренних дел»;

- Постановление Президента Республики Узбекистан от 19.06.2018 года №ПП-3786 «О дополнительных мерах по повышению эффективности обеспечения общественного порядка, профилактики правонарушений и борьбы с преступностью в городе Ташкенте»;

- Техническое задание на создание информационно-аналитической системы мониторинга «Единый центр управления» ГУВД г. Ташкента № Эз-07-8/2514 от 08.04.2021 г.

Протокол совещания по итогам визита Президента Республики Узбекистан в Алмазарский район города Ташкента 29 июня 2018 года.

1.4. Плановые сроки, начало и окончания работ

Сроки разработки и поставки ИС 30 дней.

1.5. Порядок оформления и предъявления заказчику результатов работ по созданию ИС

Результаты работ по созданию системы, после окончания пред. проектных работ, включающих в себя утверждаемую часть разработки системы – «Техническое задание», должны быть оформлены в соответствии с О'zDSt 1986:2018.

Работы по созданию системы, в соответствии с О'zDSt 1986:2018, производятся и принимаются поэтапно. По окончании каждого из этапов работ оформляется соответствующая документация.

Этапы создания проектной документации:

Инженерно-изыскательские работы. Формирование требований

к системе, не отраженных в данном Техническом задании включают в себя:

- инженерно-изыскательские работы, результат которых собран в отчет и приведены соответствующие выводы с обосновывающими расчетами, схемами, описанием предполагаемых технических средств (решений), того или иного оборудования, техническими условиями, предоставленными заказчиком (пользователем) системы. Результат работ данного этапа - оформленный «лист(ы) согласования» как приложение к заданию на проектирование;

- предварительный технико-экономический расчет.

Создание проектной документации включает в себя:

- создание документации эскизного проекта (см. содержание О'zDSt 1986:2018) и технического проектов (см. содержание О'zDSt 1986:2018), проектно-сметной документации на монтажные, электротехнические, общестроительные работы, при этом этапы, объемы и стадии определяются заданием на проектирование, составленном на этапе инженерно-изыскательских работ;

- согласование материалов проекта (во взаимодействии с заказчиком (пользователем), получение необходимых экспертных заключений (во взаимодействии с заказчиком (пользователем)). Утверждение материалов проекта (во взаимодействии с заказчиком (пользователем)).

Этапы реализации проекта:

Организационно-технические мероприятия включают в себя:

- Зона ответственности Исполнителя распространяется только на поставку оборудования до места назначения Заказчика.

- получение исполнителем товаров и оборудования, по заказной спецификации проекта производится с обязательным оформлением актов в монтаж и актов входного контроля оформленными комиссионно представителями: заказчика (пользователя), генпроектировщика (POWER CONSTRUCTION PLANET), поставщика (исполнителя);

- перед началом инсталляционных и монтажных работ производится оформление разрешительной документации на проведение работ (оформление актов готовности зданий, сооружений и т.д., получения нарядов и допусков к производству монтажных, пуско-наладочных работ).

Этап внедрения включает в себя:

- постепенчатое внедрение системы, включая необходимые монтажные, инсталляционные работы (с оформлением каждого этапа актами и протоколами приемки службами эксплуатации заказчика (пользователя));
- разработку эксплуатационной документации и ее оформление (см. содержание О'zDSt 1986:2018; О'zDSt ISO/IEC 25051). В состав эксплуатационной документации входят: инструкция по установке, руководство пользователя, программа и методика испытаний и т.д.;

Этапы закупки оборудования:

Оборудование должно быть новым, не бывшим в употреблении, не снятым с производства и произведено не ранее 2021 года. Не допускается поставка выставочных образцов, а также оборудования, собранного из восстановленных узлов. Оборудование должно быть поставлено комплектно и обеспечивать конструктивную и функциональную совместимость.

Этап ввода в действие включает в себя:

- подготовку к вводу в действие Системы (см. содержание О'zDSt 1986:2018);
- подготовку персонала (см. содержание О'zDSt 1986:2018). Подготовка учебных материалов и плана обучения (О'zDSt ISO/IEC 12207 7.4);
- обеспечивается получение и ревизия представителями поставщика (исполнителя) программно-технических комплексов у заказчика оформляется актом соответствия и пригодности (с указанием количества и сроков действия лицензий, если таковые имеются);
- производится необходимый комплекс пуско-наладочных работ (см. содержание О'zDSt 1986:2018. Оформляется актом начало и окончание этапов (индивидуального и комплексного). Приводится описание техно-рабочей части с описанием достигнутых показателей и значений);
- производятся предварительные испытания (тестирование) (см. содержание п О'zDSt 1986:2018) узлов, подсистем, систем. Сроки и объемы испытаний, устанавливаются в отдельном задании заказчика. Оформляется протокол предварительных испытаний с указанием неисправностей и сбоев, указанием причин, внесение изменений в документацию на ИАС в т.ч. эксплуатационную;
- ввод всей системы в опытную эксплуатацию (результаты оформляются актами совместно со службой эксплуатации) (см. содержание О'zDSt 1986:2018). Сроки проведения опытной эксплуатации, устанавливаются в отдельном задании заказчика. На весь срок опытной эксплуатации будет создана специальная комиссия, представители которой будут участвовать в процессе пробной эксплуатации, вести журналы учета и участвовать в приемке отдельных комплексов;
- доработка и доводка системы до проектных величин и значений с выделением периода наработки на отказ. Ведется табель работы системы;

- проведение приемочных испытаний (см. содержание О'zDSt 1986:2018).
Оформление акта о приемке системы ИАС в постоянную эксплуатацию оформляется комиссионно, с привлечением независимых экспертов, участвовавших в работе комиссии предыдущего этапа.

Этап сопровождения системы включает в себя:

- создание концепции сопровождения системы согласно О'zDSt ISO/IEG14764.

Должен быть составлен план, сопровождения системы,
(см. содержание О'zDSt 1986:2018);

- выполняются работы в соответствии с гарантийными обязательствами поставщика (исполнителя, производителя), (см. содержание О'zDSt 1986:2018).

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение

Система предназначена для автоматизации и контроля процессов определения и выявления факторов, создающих риски возникновения чрезвычайных ситуаций, нарушения общественной безопасности, угрозы жизни и здоровья граждан и террористических актов.

Целевое назначение Системы - значительное повышение уровня оперативного реагирования, выявление и значительное расширение возможностей по обнаружению разыскиваемых лиц и прочих лиц, находящихся в базах, данных существующих АИС МВД РУ.

2.2. Цели создания системы.

Целью создания является:

- своевременное обеспечение оперативных и дежурных сил и служб достоверной визуальной и аналитической информацией, необходимой для выполнения возложенных на них задач;
- предоставление информации смежным автоматизированным информационным системам МВД РУ для дальнейшего анализа или производства других операций;
- повышение эффективности оперативно-служебной деятельности подразделений охраны общественного порядка, обеспечения общественной безопасности, следственных и оперативных действий подразделений органов внутренних дел города Ташкента, при раскрытии преступлений и правонарушений;
- использования видеоматериалов, полученных с помощью оборудования видеонаблюдения, для проведения следственных действий;
- своевременное выявление лиц, находящихся в розыске. Реагирование и задержание. Профилактические действия.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1. Краткие сведения об объекте автоматизации

Объектом автоматизации при разработке Системы являются объекты подразделений органов внутренних дел города Ташкента и объекты массового пребывания людей.

Разрабатываемая Система относится к новым создаваемым комплексам автоматизации, являющимся важным инструментом для осуществления органами внутренних дел своих непосредственных обязанностей. По архитектуре, конструктивному исполнению, функционалу Система не имеет аналогов среди существующих информационных систем в структуре ГУВД г. Ташкента и в Республике в целом, но может быть использована по назначению сразу после внедрения, взаимодействуя с существующими АИС МВД РУ, принося положительные результаты.

3.2. Сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды

Общие требования:

При обследовании объектов автоматизации на предмет размещения в них элементов Системы, при инженерно-изыскательских работах и техническом проектировании должны быть учтены следующие условия:

- на объектах автоматизации должны отсутствовать такие воздействия, как: механический резонанс, синусоидальная вибрация, механические удары, атмосферное пониженное давление, плесневые грибы, рабочие растворы, агрессивные среды и другие негативные факторы;
- электропитание на стационарных объектах эксплуатации Системы осуществляется от электрической сети напряжением 380/220В, частотой 50 Гц с глухо заземленной или изолированной нейтралью;
- серверы, активное сетевое оборудование (вычислительные мощности и средства «окружения» Системы, а также рабочие станции должны размещаться в кондиционируемых специализированных помещениях, в отдалении от отопительных приборов;
- кондиционируемые помещения должны быть оборудованы системами электроснабжения, связи, телекоммуникаций, вентиляции, поддержки климатических условий и поддержки противоположных условий эксплуатации;
- оборудование, устанавливаемое вне помещений, должно удовлетворять следующим требованиям:

*внешние устройства, монтируемые вне помещений, должны быть защищены корпусами, шкафами, кожухами или располагаться в запирающихся шкафах, обеспечивающих степень защиты не ниже IP 54.

Внешние устройства должны сохранять работоспособность при следующих значениях климатических факторов:

- рабочая температура окружающей среды - от минус 30 до плюс 50°С, если в настоящем техническом задании или в ЧТЗ не указано иное;
- относительная влажность - до 98% при 35°С, если в настоящем техническом задании или в ЧТЗ не указано иное.

Линии связи и оборудование должны сохранять требуемую работоспособность в условиях грозы и других неблагоприятных природных явлений.

Зданиям и помещениям, в которых будет располагаться оборудование, входящее в состав Системы, должны удовлетворять всем действующим стандартам в республике Узбекистан.

Режим эксплуатации – круглосуточный круглогодичный. Использование технических средств и выполнение периодического обслуживания и сервисных работ должно производиться в соответствии с требованиями производителей оборудования. Точный регламент, сроки и периодичность проведения техобслуживания должен быть определен после инсталляции оборудования Поставщиком на основании технической документации к оборудованию.

4. ТРЕБОВАНИЯ К СИСТЕМЕ

4.1. Требования к ИС в целом

Проектируемый комплекс автоматических информационных аналитических систем мониторинга будет уникальным, ввиду централизованной обработки видеопотоков, построенной на единой базе данных биометрических фотографий высокого качества.

Данная система является комплексом систем автоматизации (КСА МВД РУ).

Комплексные решения по построению Системы должны включать в себя следующие мероприятия:

- системную организацию аналитических алгоритмов обнаружения в автоматическом режиме в реальном времени и в режиме off-line;
- вывод видеоизображения с камеры видеонаблюдения в телекоммуникационную систему;
- вывод видеоизображений с ближайших к месту происшествия существующих камер, существующих систем;
- внедрение программно-аппаратных средств, для реализации методов и алгоритмов сбора и обработки видеоинформации.

Внедрение данных решений позволит Системе:

1. Осуществлять мониторинг контролируемых объектов (входные группы объектов) в реальном масштабе времени;
2. Собирать, анализировать и фиксировать видеоинформацию, работать с базами данных разыскиваемых лиц;
3. Выдавать и фиксировать тревожные сообщения в Систему, поступающих от аналитических функций системы видеонаблюдения;

Система видеонаблюдения должна функционировать в непрерывном круглосуточном режиме и быть в постоянной готовности к обеспечению экстренного реагирования на тревожную информацию, поступающую от подсистемы видеонаблюдения.

4.1.1. Требования к структуре и функционированию ИС

4.1.1.1. Перечень систем, подсистем, их назначение

Система включает в свой состав следующие функциональные подсистемы:

- подсистема информационно-аналитическая;
- геоинформационная подсистема;
- подсистема ЦОД;
- подсистема мониторинга и визуализации;
- подсистема терминальных пунктов видеонаблюдения;
- подсистема распознавание ГРЗ ТС, регистрации и нарушение ПДД;

В состав системы также должны входить следующие обеспечивающие подсистемы:

- транспортная подсистема локальная объекта и подсистема каналов доступа, предоставленная национальным провайдером АК «Узбектелеком»;
- подсистема информационной безопасности Системы.

4.1.1.2. Требования к взаимодействию со сторонними информационными системами

При создании Системы, предлагается использовать централизованную схему построения топологии Системы, определяющую техническую и системную архитектуру. Пример построения системы представлен на рисунке 1.

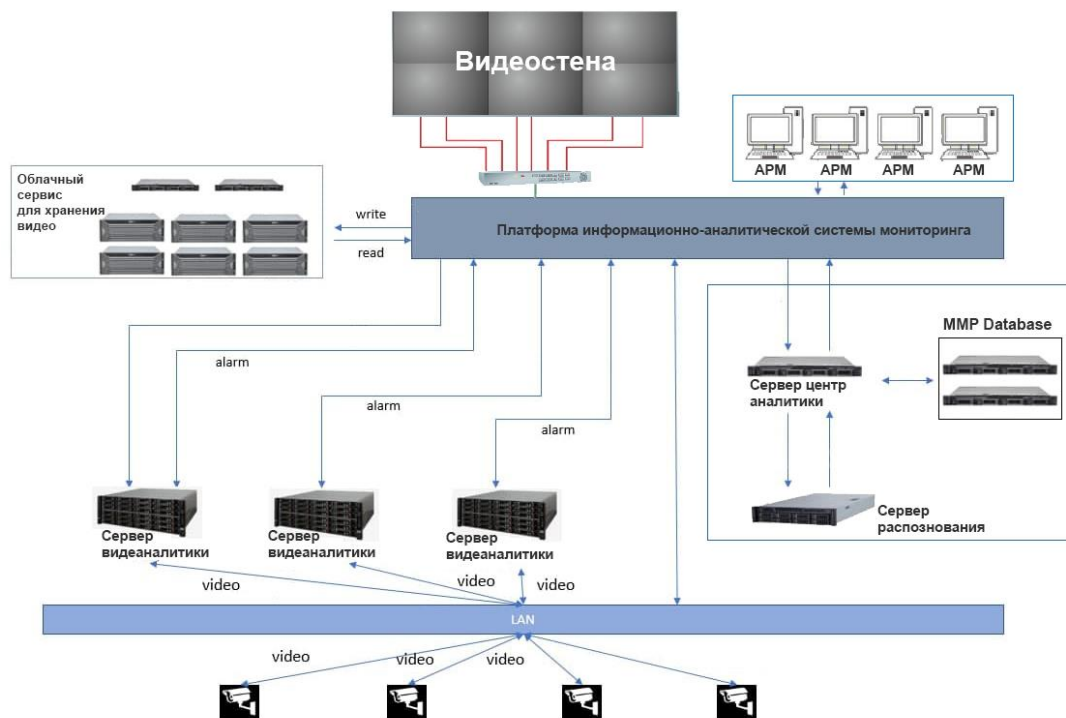


Рисунок 1. - Предполагаемая структура построения

Централизованная схема построения топологии Системы предполагает размещение вычислительных мощностей и системы хранения информации в ЦОДе с агрегированием сетевой части в центре топологии типа «звезда» и распределенной клиентско-административной части системы.

Система должна состоять из:

1. Ядра системы, расположенного в ЦОД. На уровне ядра системы поддерживается функционал Системы:

- потоковое распознавание лиц, сверка с базами данных, информирование;

- отложенный поиск по лицам, зафиксированным системой потокового распознавания;
- поиск лиц по Бадам граждан;
- видео аналитика;
- управление/обновление Баз данных;
- хранение видео контента по тревожным событиям;
- геоинформационный;
- опциональный функционал, включающий в себя: подключение к дополнительным базам данных, интеграция с системой 102, интеграция с другими системами МВД РУ.

2. Диспетчерских наблюдения включает в себя следующий функционал:

- Мониторинг в заданном территориальном секторе, который включает в себя:
 - управление событиями;
 - просмотр изображения с выбранных видеокамер;
 - просмотр видео контента;
 - получение результатов системы потокового распознавания лиц, получение автоматических сигналов тревоги, управление реагированием, силами и средствами;
 - получение доступа к просмотру видео контента с существующих систем на объектах;
 - доступ к информации в ядре Системы заданного диапазона, для получения определенной информации из Системы по сектору ответственности подразделения основного пользователя.
 - технический мониторинг, администрирование, включая компоненты интеграции с источниками внешних систем;
 - геоинформационная система (ГИС).
 - Управление видеопотоками, включая СХД и СУБД информации, содержащих все события, сгенерированные системой по всем событиям;
 - Управление аналитической системой;
 - Автоматизированные рабочие места СВН (АРМ СВН);
 - Рабочие места сетевых администраторов и системных администраторов СВН (АРМ СВН).

4. Терминальные пункты видеонаблюдения (объекты) - комплексно установленные IP видеокамеры с коммутатором доступа и маршрутизаторами, подключенным в зашифрованный канал данных VPN (опорной сети) национального провайдера АК «Узбектелеком».

Интеграция со всеми информационными системами МВД.

4.1.1.3. Требования к режимам функционирования системы

Система имеет следующие основные режимы функционирования:

- Штатный (режим повседневной деятельности) – основной режим функционирования. В данном режиме система выполняет свои функции в соответствии с техническими и организационными инструкциями. При этом:

- система функционирует в круглосуточном ежедневном режиме, с перерывами на запланированное техническое обслуживание;
- система поддерживает весь перечень предоставляемых услуг;
- исправно работает оборудование, составляющее комплекс аппаратных средств;
- исправно функционирует системное, базовое и прикладное программное обеспечение системы.

Сервисный режим - необходим для проведения обслуживания, реконфигурации и пополнения новыми компонентами Системы и ее компонентов. При этом несанкционированные работы и несогласованные остановки работы оборудования Системы, а также любые действия, которые могут привести к остановке или к задержкам работы ИТ и телекоммуникационной инфраструктуры МВД РУ, недопустимы.

Нештатный режим функционирования – режим, который позволяет использовать доступные ресурсы системы для сохранения информации, правильного закрытия информационных массивов, работающих приложений и операционных систем. Нештатный режим используется для выполнения минимально необходимых операций в условиях аварийного энергоснабжения компонентов системы или выхода из строя части оборудования.

В случае если в результате программного или аппаратного сбоя, отказа электроснабжения или возникновения других внутренних или внешних факторов система не может обеспечить решения своих задач в полном объеме и на надлежащем уровне, то происходит переход системы в нештатный режим функционирования.

Основные усилия персонала системы в нештатном режиме ее функционирования направлены на обеспечение приема видеоинформации, организации реагирования на эти события и возвращение системы в штатный режим функционирования.

При этом информация о каждом отказе или сбое записывается в системе и передается обслуживающему персоналу для принятия мер по поддержанию работоспособности и штатного режима функционирования системы.

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

Аварийный режим функционирования Системы - характеризуется отказом одного или нескольких компонентов программного и (или) технического обеспечения. В аварийном режиме системы:

- в режиме реального времени должны передаваться сведения о состоянии системы и ее отдельных компонентов в отделы внутренней технической поддержки Заказчика.

- в случае задымления или возгорания составляющих систем должна срабатывать система автоматического газового пожаротушения в соответствии с ШНК 2.04.09-2007 «Пожарная автоматика зданий и сооружений».

- Система должна обеспечить сохранность всех базовых конфигураций программно-аппаратных средств и не допустить утерю и/или повреждение данных систем хранения и резервирования информационных ресурсов Заказчика.

4.1.1.4. Перспективы развития, модернизации системы

Все компоненты Системы должны быть обеспечены возможностью масштабирования не менее 25% от требуемых параметров, согласно данного ТЗ.

4.1.1.5. Общая архитектура системы

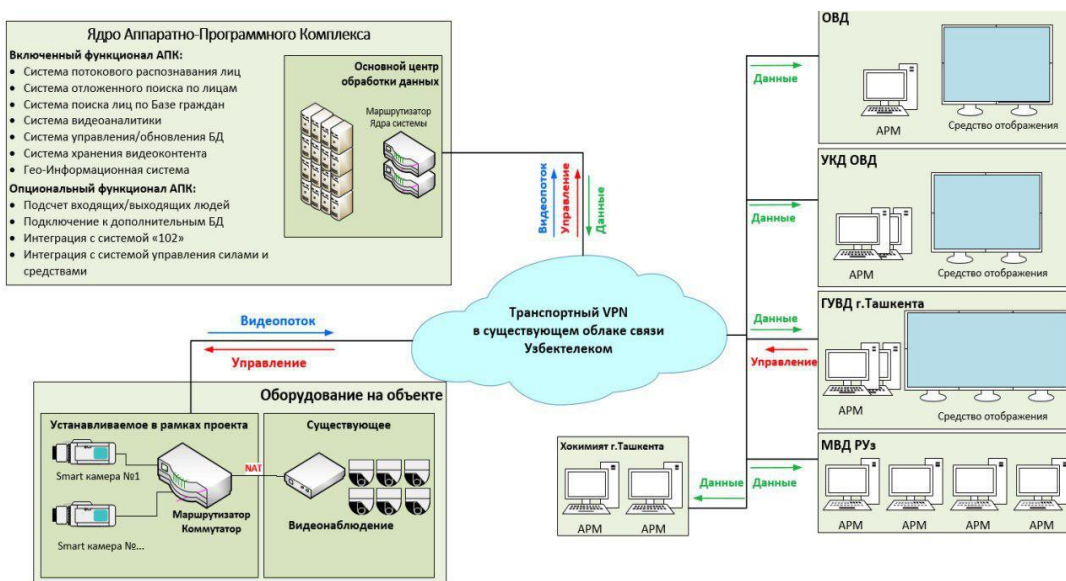


Рисунок 2 - Предполагаемая технологическая схема комплекса систем автоматизации

Технологическая схема комплекса систем автоматизации представлена на рисунке 2. Данная схема, примененная в создании Системы, оправдана, с точки зрения оптимального распределения ресурсов Системы. Выход из строя центра обработки данных маловероятен, если все условия настоящего ТЗ будут выполнены участниками реализации проекта. Резервирование других функций ЦОД ГУВД г. Ташкент МВД РУ, не затрагивающих данное решение, будет осуществляться на следующих этапах реализации построения структуры ИКТ МВД РУ в целом. Временный выход из строя любого другого объекта Системы,

не будет являться критичным для всей Системы, при этом сохраняется работоспособность всей Системы.

4.1.2. Требования к характеристикам взаимосвязей создаваемой системы со смежными системами

При создании и реализации системы предусмотреть возможность поддерживать информационное взаимодействие с разрабатываемыми и существующими информационными системами МВД РУ по аналогу с тестовой площадкой.

Информационная совместимость системы с другими информационными системами должна обеспечиваться возможностью использования в них одних и тех же форматов данных и протоколов обмена данными.

4.1.2.1. Требования к способам подключения и средствам связи

Для функционирования Системы все сетевые компоненты в рамках одного объекта автоматизации должны быть объединены в локальную вычислительную сеть с использованием транспортного протокола IP.

Другим важным компонентом системы, является транспортная телекоммуникационная инфраструктура, обеспечивающая связь камер видеонаблюдения с серверами видео аналитики и хранения данных.

Для создания корпоративной сети передачи данных следует предусмотреть использование арендуемых каналов передачи данных опорной сети АК «Узбектелеком».

4.1.3. Требования к численности и квалификации пользователей

Персонал, эксплуатирующий и обслуживающий Систему должен состоять из: пользователей Системы;

персонала, осуществляющего эксплуатацию (обслуживающего персонала/администратора)

Численный состав пользователей является переменным и определяется руководством объекта автоматизации.

Все пользователи должны быть разделены по группам (ролям) в соответствии с функциональностью, которую они используют при работе с Системой.

Каждый пользователь должен иметь одну (единую) учетную запись в Системе.

Численность обслуживающего персонала Системы должна определяться с учетом следующих требований:

- структура и конфигурация Системы должны быть спроектированы и реализованы с целью минимизации количественного состава обслуживающего

персонала и обеспечения работоспособности Системы во всех режимах функционирования;

- аппаратно-программные средства Системы не должны требовать круглосуточного обслуживания и постоянного присутствия администраторов у консоли управления;

- структура Системы должна предоставлять возможность управления всем доступным функционалом Системы как одному администратору, так и предоставлять возможность разделения ответственности по администрированию между несколькими администраторами;

- для администрирования Системы к администратору не должны предъявляться требования по знанию всех особенностей функционирования элементов, входящих в состав администрируемых компонентов Системы.

Для обслуживающего персонала Системы должны быть определены следующие основные роли:

- системный администратор;

- инженер по обслуживанию средств сетевой и вычислительной техники, а также периферийного оборудования;

- администратор информационной безопасности.

Требования к численности и составу обслуживающего персонала Системы подлежат уточнению при техническом проектировании и должны быть включены в эксплуатационную документацию на каждый сегмент.

Основными квалификационными требованиями к персоналу Системы является возможность самостоятельной работы:

- наличие соответствующих юридически правильно оформленных документов с необходимыми квалификационными характеристиками (допуски для работы);

4.1.4. Показатели назначения

Интегральным параметром, характеризующим степень соответствия системы ее назначению, должна являться полнота реализации требований настоящего Технического Задания.

Целевое назначение системы должно сохраняться на протяжении всего срока эксплуатации системы. Срок эксплуатации системы определяется сроком устойчивой работы аппаратных средств вычислительных комплексов, своевременным проведением работ по замене (обновлению) аппаратных средств, по сопровождению программного обеспечения системы и его модернизации.

При проектировании архитектуры программного комплекса должны быть реализованы следующие основные показатели назначения, отвечающие требованиям к автоматизированным информационным системам подобного класса:

- Масштабируемость - должна достигаться путем замены оборудования на более производительное и перераспределением нагрузки от вычислительных

процессов за счет использования ресурсов подключаемого другого оборудования. Система должна допускать не менее чем 3-кратное увеличение объемов обрабатываемой информации.

- Интегрированность - система должна состоять из интегрированных модулей, построенных на основе стандартных настраиваемых комплексов программного обеспечения.

- Информационная безопасность - система должна обеспечить использование механизмов, автоматизации режима ограничения доступа к информационным ресурсам Заказчика. Программный комплекс должен обеспечивать минимизацию риска некорректного использования информационных ресурсов Заказчика за счет следующих мероприятий:

- предоставления доступа только после идентификации пользователя;

- разграничения прав доступа по категориям пользователей.

- Система должна соответствовать требованиям, предъявляемым к информационной безопасности государственных информационных ресурсов (систем), и в том числе Политике безопасности Заказчика, отражающей подход Заказчика к защите своих информационных ресурсов.

- Расширяемость - система должна поддерживать работу неограниченного числа рабочих пользовательских мест, обеспечивая при этом их объединение в единую информационную инфраструктуру.

- Модульность - система должна состоять из отдельных взаимодействующих между собой модулей, построенных на основе сопряжения, путем настройки стандартных комплексов программного обеспечения, реализующего функции системы. Состав модулей может дополняться с соблюдением единых принципов организации.

- Унификация - Методы описания, представления, передачи и обработки данных в электронной форме должны быть унифицированы;

- Клиентский интерфейс - Все основные функции и действия должны быть понятны интуитивно обычному пользователю при условии знания предметной области. Структура входных и выходных форм, расположение меню, кнопок, и другой управляющей информации должны быть спроектированы с учетом обеспечения высокой скорости ввода данных и соответствия существующей технологии обработки информации.

4.1.4.1. Значения параметров, характеризующих степень соответствия системы по назначению

Система должна быть построена таким образом, чтобы обеспечивалось отсутствие потерь информации при информационном обмене внутри Системы, между подсистемами, а также и при информационном обмене с внешними источниками/потребителями информации.

Кроме того, Система должна:

- Обеспечивать функционирование в штатном режиме круглосуточно, без выходных («режим 24/7») с допустимыми регламентными перерывами на сервисное обслуживание суммарной длительностью не более 2 часов в месяц.
- Поддерживать изменения алгоритмов работы телекоммуникационной инфраструктуры. Отказоустойчивость ИТ-систем и систем, не входящих в объем настоящего ТЗ, обеспечивается средствами Заказчика и не рассматривается в текущем ТЗ.
- Поддерживать модернизацию (до пределов, установленных производителем оборудования, входящего в состав Системы) и наращивание системы (исходя из требований Заказчика) за счет добавления новых модульных блоков в соответствующие технические компоненты Системы.
- Обеспечивать требуемые параметры электроснабжения, температурно-климатического режима для непрерывной работы оборудования систем Системы.
- Обеспечивать защиту установленного оборудования от повреждения или кражи, от пожара и иных негативных внешних воздействий.
- Обеспечивать удобную и эффективную эксплуатацию оборудования ИТ и телекоммуникаций, установленного в машинных залах ЦОД Системы, а также всего комплекса вспомогательного оборудования.
- Обеспечивать требуемый уровень надежности, количественные и качественные характеристики электроснабжения оборудования ИТ и телекоммуникаций, вспомогательного оборудования.
- Обеспечивать требуемый уровень надежности, количественных и качественных характеристик вентиляции, кондиционирования и отопления для оборудования ИТ и телекоммуникаций, вспомогательного оборудования.
- Обеспечивать возможность проведения регламентных и ремонтных работ без остановки работы оборудования ИТ и телекоммуникаций, размещаемого в машинных залах ЦОД Системы.
- Обеспечивать интерактивный мониторинг и управление телекоммуникационной инфраструктурой Системы и инженерной инфраструктурой как с рабочего места оператора ЦОД, расположенного непосредственно в ЦОДе Системы, так и в удаленном режиме.
- Обеспечивать уровень информационной безопасности телекоммуникационной инфраструктуры Системы в соответствии с требованиями Заказчика.
- Обеспечивать унификацию структурированной кабельной сети всех уровней Системы и удобство подключения нового оборудования к телекоммуникационной инфраструктуре Системы.

4.1.4.2. Степень приспособляемости системы к изменению процессов и методов управления, к отклонениям параметров объекта управления

Система управления техническими средствами Системы должна быть гибкой в отношении любых возможных изменений оборудования и изменений архитектуры Системы, добавления нового оборудования.

4.1.4.3. Допустимые пределы модернизации и развития Системы

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

Порядок возможной модернизации Системы уточняется в процессе разработки проекта и согласовывается протоколом на стадии проектирования с Заказчиком;

Модернизация и развитие системы должна осуществляться в пределах, обеспечивающих экономическое обоснование производимых затрат и сроков их окупаемости с учетом существующего функционала Системы и периода морального старения оборудования, входящего в состав Системы. Минимально допустимый срок эксплуатации технических средств Системы при этом должен быть не менее 5 лет.

4.1.4.4. Вероятностно-временные характеристики, при которых сохраняется целевое назначение Системы

Минимальный срок эксплуатации:

- Системы в целом - не менее 5 лет;
- модулей функциональных подсистем - не менее 5 лет;
- комплекса технических средств - не менее 5 лет (при проведении соответствующего технического обслуживания и соответствующей технической модернизации);
- телекоммуникационной подсистемы - не менее 5 лет (при проведении соответствующего технического обслуживания и соответствующей технической модернизации).

4.1.5. Требования к надежности

При размещении на технической площадке, удовлетворяющей требованиям эксплуатационной документации, в целевой конфигурации Системы должны обеспечивать необслуживаемое функционирование в круглосуточном режиме с допустимыми перерывами на профилактику и перенастройку с простоями в

связи с неисправностью не более 24 часов в год, при среднем времени устранения неисправности, вызвавшей простой, не более 4 часов.

Показатели надежности включают:

- показатели надежности комплекса оборудования должны достигаться комплексом организационно-технических мер, обеспечивающих доступность ресурсов, их управляемость и обслуживаемость;
- организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок персонала при проведении работ по обслуживанию оборудования Системы, минимизацию времени ремонта или замены вышедших из строя компонентов за счет:
- регламентации проведения работ и процедур по обслуживанию и восстановлению подсистемы;
- своевременного оповещения пользователей о случаях нештатной работы компонентов подсистемы;
- своевременной диагностики неисправностей.
- перечень аварийных ситуаций, по которым должны быть регламентированы требования по времени восстановления работоспособности подсистемы:
- выход из строя одного из узлов оборудования Системы;
- выход из строя компонента одного из узлов;
- выход из строя источника бесперебойного питания;
- выход из строя камеры видеонаблюдения.
- срок восстановления работоспособности подсистемы - не более 1-х суток с момента поступления заявки о неисправности.

Надежность должна обеспечиваться, как минимум, следующими методами:

- применением высоконадежного и отказоустойчивого оборудования;
- использованием оборудования с аппаратной избыточностью элементов и возможностью «горячей» замены отдельных элементов (блоки питания, вентиляторы и т.п.);
- принятием специальных технологических решений, обеспечивающих высокую отказоустойчивость наиболее ответственных и жизненно важных компонентов;
- обеспечением сохранности накопленной информации при авариях электропитания любой продолжительности и продолжением работы после восстановления электропитания без дополнительной настройки;
- сохранением работоспособности инженерных систем при некорректных действиях пользователя;
- реализацией подсистемы бесперебойного электроснабжения;
- использованием оборудования с встроенными средствами самодиагностики и самотестирования состояния;
- организацией технически грамотной эксплуатации всех подсистем.

При возникновении сбоев в аппаратном обеспечении, включая аварийное отключение электропитания, Система в целевой конфигурации должна

автоматически восстанавливать свою работоспособность после устранения сбоев и корректного перезапуска аппаратного обеспечения (за исключением случаев повреждения рабочих носителей информации с исполняемым программным кодом).

Надежность системы рассчитывает Разработчик в соответствии с «TSt 45.037:2003 Надежность технических средств телекоммуникаций. Методика расчета среднего времени восстановления технических средств телекоммуникаций». К надежности электроснабжения предъявляются следующие требования:

- с целью повышения отказоустойчивости системы в целом необходима обязательная комплектация Системы источниками бесперебойного питания с возможностью автономной работы системы не менее 15 минут и резервным питанием от дизель-генератора не менее 24 часов;
- система должны быть укомплектована системой оповещения Администратора о переходе на автономный режим работы
- в случае длительного отключения энергоснабжения функция автоматического безопасного и корректного завершения работы ИБП должна предотвратить потерю информации серверного оборудования Системы, безопасно его отключить и обеспечить минимальное время восстановления (включения).

Гарантийный срок эксплуатации системы должен составлять:

- на все поставляемые компоненты системы: не менее 1 года с даты подписания акта приемки системы в эксплуатацию.

Вся произведенное и поставленное оборудование должно быть надежным в эксплуатации и обеспечено всеми необходимыми сертификатами соответствия согласно международным стандартам.

4.1.6. Требования безопасности

Требования по безопасности включают требования по обеспечению безопасности при монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств системы (защита от воздействий электрического тока, электромагнитных полей, афотических шумов и т. п.), по допустимым уровням освещенности, вибрационных и шумовых нагрузок.

Монтаж оборудования производить в строгом соответствии с инструкцией «МКН 03:2006 Инструкция по монтажу сооружений и устройств связи, радиовещания и телевидения».

Оборудование обеспечить электропитанием и заземлением в строгом соответствии с ГОСТ 464-79, ВСН 1-77, МКМ 02:1999 и ПУЭ. Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ

12.1.030-81 и ПУЭ. Использование металлических конструкций в качестве заземляющих проводок недопустимо.

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

В случае возгорания не должно выделяться ядовитых газов и дымов. Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих санитарных правил и норм (СанПиН) РУ.

Технические средства, входящие в состав Системы, должны удовлетворять требованиям ГОСТ 12.1.002-84 по уровням напряженности электрических полей.

Уровень шума на рабочих местах операторов Системы, создаваемый оборудованием, должен соответствовать требованиям, установленным ГОСТ 12.1.003-83.

К эксплуатации оборудования Системы должен допускаться персонал, имеющий достаточную теоретическую и практическую подготовку. Эксплуатационная документация должна содержать указания по безопасности при эксплуатации и техническом обслуживании.

Условия эксплуатации и характеристики окружающей среды определяются в соответствии с Гигиеническими требованиями к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы (Санитарные правила и нормы. СанПиН 2.2.2/2.4.1340-03).

4.1.7. Требования к эргономике и технической эстетике

Компоновка технических средств на рабочих местах персонала должна отвечать условиям удобства обслуживания и работы с ними и соответствовать общим эргономическим требованиям по ГОСТ 23000-78.

Поверхности пультов, мониторов и консолей управления должны обладать покрытием, исключающим появление бликов в поле зрения диспетчера.

Взаимное расположение рабочих мест персонала должно отвечать требованиям ГОСТ 21958-76.

Внешнее оформление технических средств должно отвечать требованиям технической эстетики по ГОСТ 30.001-83.

Графический интерфейс Системы должен отвечать следующим требованиям:

- отображение на экране преимущественно необходимой для решения текущей прикладной задачи информации;
- использование функциональных и «горячих» клавиш, при этом на экране должна находиться подсказка о назначении таких клавиш;

- отображение на экране хода длительных процессов обработки.

Процедуры ввода данных должны отвечать следующим требованиям:

- пользователь должен иметь возможность гибко контролировать ввод данных: просматривать введенные данные на мониторе, производить их корректировку или отказаться от ввода;
- обеспечение возможности ввода значений по умолчанию.

Интерфейс должен обеспечивать корректную обработку ситуаций, вызванных неверными действиями, неверным форматом или недопустимыми значениями входных данных. В указанных случаях должны выдаваться соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

4.1.8. Требования к защите информации от несанкционированного доступа

До начала этапа эксплуатации Системы ее системные пользователи, а также руководящий и обслуживающий персонал должны быть ознакомлены под роспись с перечнем сведений ограниченного пользования и подлежащих защите, в части, их касающейся, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации ограниченного распространения. Создание перечня информации ограниченного распространения и инструкции пользования данными ограниченного распространения – прерогатива Заказчика.

Комплекс технических (аппаратно-программных) средств защиты Системы должен включать:

- Средства аутентификации пользователей, в том числе с помощью ЭЦП и элементов Системы (рабочих станций, систем управления инженерной инфраструктурой и т.п.).
- Средства разграничения доступа к ресурсам рабочих станций управления и мониторинга.
- Средства реагирования на обнаруженные попытки несанкционированного доступа, как в помещения, так и в технические средства.
- Средства защиты от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ в Системы, подверженные данным уязвимостям.

Оснащение Системы прочими техническими средствами, за исключением описанных в настоящем ТЗ, обеспечивает Заказчик.

Вместе с тем, целью защиты информации и программных средств от несанкционированного доступа и действия вредоносных программ (компьютерных вирусов) при разработке и эксплуатации Системы необходимо предпринять организационные, правовые, технические

и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.

При разработке Системы необходимо учесть действующие требования политики информационной безопасности учреждения Заказчика, чтобы избежать возникновения конфликтных ситуаций при проведении мероприятий по обеспечению информационной безопасности.

Доступ к информации должен быть строго регламентирован и обеспечен на уровне:

- администратора системы - в части доступа на выполнение функций системы на уровне модулей системы и функциональных возможностей каждого отдельного модуля;
- сетевого администратора - в части доступа к разделенным файлам локальной сети.

Доступ пользователей к информации, хранящейся в базе данных, должен быть возможен только через соответствующие пункты меню режимов работы Системы.

Вход в систему и доступ пользователей к различным режимам работы должен быть строго регламентирован в зависимости от потребностей Заказчика и обеспечен Администратором системы путем настройки доступа к модулям и функциям системы. Вход в систему должен осуществляться по уникальным именам и закодированным паролям для каждого пользователя системы. Установка и смена паролей, прав доступа должна осуществляться пользователями информационной системы через интерактивный программный модуль по истечению срока действия пароля или по запросу Администратора.

Информационная безопасность системы должна обеспечиваться за счет централизованного хранения данных на серверах и разграничения доступа с использованием двухуровневой защиты:

- на уровне системы управления базами данных (СУБД), обеспечивающей механизмы аутентификации и авторизации доступа к объектам системы;
- на уровне приложения, обеспечивающего доступ к функциям системы.

Каждый пользователь должен быть однозначно идентифицирован в системе, для обеспечения строгого выполнения своих обязательств и предотвращения раскрытия информации.

Система должна поддерживать управление политиками разграничения доступа на уровнях «пользователь» и «пользовательская группа».

Система не должна предоставлять возможность пользователям получать доступ к информации помимо предусмотренных процедур, определенных на уровне разработки технического проекта.

Каждый пользователь системы, имеющий зарегистрированный в системе ЭЦП, при регистрации должен получать соответствующий пароль, который проверяется при авторизации.

Для каждого авторизированного пользователя будут сохраняться:

- учетное имя (логин);
- пароль;
- персональные данные - ФИО, должность, телефон;
- пользовательская группа.

Для получения гибкой системы настроек будут вводиться следующие понятия:

- право - составляет минимальный набор логически связанного функционала;
- роль - минимальный набор прав для получения доступа к функционалу системы в соответствии с должностными обязанностями пользователя.

При запуске любого АРМ, после процедуры авторизации пользователя, система должна формировать меню АРМ в соответствии с ролью, которой обладает пользователь.

В зависимости от роли пользователя будут определяться вертикальные ограничения на уровне таблиц, полей и процедур. В зависимости от региональной или структурной принадлежности пользователя будут определяться горизонтальные ограничения на уровне записей.

Доступ к файлам и базам данных должен осуществляться по специальному паролю. Пароль должен быть известен только ответственным за эксплуатацию базы данных администраторам.

Все действия, предусмотренные функционалом для участников системы, результат этих действий, точная дата и время должны записываться в журналы действий (logs) с обязательным указанием пользователя, выполнившего операцию. Никто не должен иметь права на изменение/удаление записей журналов. Архив логов должна храниться в течение 5 лет. После истечение срока хранения должно проходить циклический запись логов.

Помимо регламентированного доступа к информации на уровне пользователей, а также защиты от несанкционированного доступа необходимо предусмотреть корпоративную антивирусную защиту, т.е. установка серверной части антивирусной защиты, клиентской части, с выводением отчетов на рабочее место администратора, а также для предотвращения сетевых атак рекомендуется использование сетевых экранов.

4.1.9. Требования по сохранности информации при авариях

В процессе функционирования информационной системы возможны следующие аварийные ситуации:

- отсутствие электропитания;

- отсутствие (обрыв) линии связи;
 - отказ технических средств;
 - наличие «вирусов»;
 - отказ программного обеспечения из-за ошибок Разработчика, не обнаруженных на этапах тестирования и опытной эксплуатации;
 - потеря информации после некорректных действий обслуживающего персонала.
- Полный перечень отказов и их критериев, среднее время восстановления работоспособности после возникновения аварийной ситуации и другие количественные значения показателей надежности будут уточнены на стадии разработки рабочей документации и согласованы с Заказчиком.

Сохранность информации при авариях должна обеспечиваться на уровне БД и на уровне оборудования, а также путем создания резервных копий.

Вместе с тем сохранность информации в Системе должна обеспечиваться при следующих аварийных ситуациях:

- нарушения внешнего электропитания;
- провалы внешнего напряжения - кратковременные понижения при резком увеличении нагрузки в электрической сети;
- высоковольтные импульсы - кратковременные значительные увеличения внешнего напряжения;
- полное отключение внешнего поступления электроэнергии - полное отключение электроэнергии вследствие аварий, перегрузок;
- слишком большое внешнее напряжение - кратковременное увеличение напряжения в сети;
- нестабильность частоты питающего внешнего напряжения.
- нарушение или выход из строя каналов связи локальной сети Системы;
- полный или частичный отказ инженерных средств системы;
- сбой общего или специального программного обеспечения инженерных систем;
- ошибки в работе управляющего или технического персонала;
- выход из строя элемента сетевой инфраструктуры системы.

В случае полного выхода из строя одного из компонентов Системы (физическое разрушение, полное отключение каналов связи и т.д., в том числе любые аварии, приводящие к остановке предоставления услуг, возложенных на оборудование и программное обеспечение) все вычислительные и телекоммуникационные функции должны автоматически перейти на второй дублирующий соответствующий компонент Системы. Ответственность за настройку и эксплуатацию систем, не рассматриваемых настоящим ТЗ, несет Заказчик. Сохранность информации в ИТ системах настоящим проектом не

рассматривается, ответственность за восстановление информации при авариях в ИТ инфраструктуре несет Заказчик.

4.1.10. Требования к патентной и лицензионной чистоте

В отношении всех составляющих Системы, должно быть обеспечено недопущение нарушения действующих документов исключительного права третьих лиц (патентов, лицензионных соглашений и других охранных документов).

Проектные решения построения Системы должны отвечать требованиям по патентной и лицензионной чистоте, согласно действующему законодательству и распорядительным документам, регламентирующим создание ЦОД. Уточнение требований по патентной чистоте должно производиться в договорах на проведение работ по созданию компонентов Системы. При этом Разработчику необходимо привести сведения о наличии лицензий на используемое программного обеспечения, СУБД и другие программные продукты третьих сторон. В случае использования собственных разработок необходимо указывать наличие документальных свидетельств на владение интеллектуальной собственностью и авторскими правами, в том числе на конструкторскую документацию и чертежи. Все программно-технические средства общего программного обеспечения, обеспечивающие работоспособность Системы, должны иметь разрешение на использование (лицензию) с требуемым количеством пользователей.

Все используемое оборудование должно быть сертифицировано и разрешено к применению на территории РУ.

4.1.11. Требования по стандартизации и унификации

Технические средства Системы, подлежащие обязательной сертификации в соответствии с действующим законодательством Республики Узбекистан, должны иметь соответствующие сертификаты.

Технические средства Системы, должны использовать стандартные электрические стыки, интерфейсы, технологии и протоколы передачи данных.

Одним из условий эффективного функционирования Системы должно быть использование стандартных комплексов технических и программных средств, унифицированных форм документов, единых международных, отраслевых классификаторов, единых международных стандартов.

На всех стадиях разработки АПК система должна обеспечиваться унификация проектных решений, что должно обеспечиваться единообразным подходом к решению однотипных задач, унификацией технического, информационного, лингвистического, математического, информационного и организационного

обеспечения Единообразный подход к решению однотипных задач должен достигаться:

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

Унификация технических средств Системы должна достигаться за счет:

1. Применения серийных технических средств, соответствующих международным стандартам;
2. Минимизации применяемых типов вычислительных машин и других компонентов;
3. Использования типовых автоматизированных рабочих мест, компонентов и комплексов.

В системе будут использоваться стандартные процедуры для выполнения функций обслуживания системы, таких как резервное копирование, восстановление, архивирование, импорт и экспорт данных, обеспечение целостности данных и индексов.

4.1.12. Дополнительные требования

4.1.12.1. Требования к исполнителю

- Исполнитель должен предоставить информацию по:
 - методам достижения минимального уровня ТСО (Total Cost of Ownership) за счет предлагаемого технологического решения, функционала, и т.п. уникальных решений производителя сроком на не менее 5 лет;
 - сервисам и подпискам (включая по стоимости послегарантийной поддержки);
 - условиям лицензирования (объем предоставления, порядок взимания платы, срок действия лицензий и др.) при наличии;
 - перечню осуществляемых работ (услуг) с конкретизацией объема и привлекаемых специалистов (обоснование формирования стоимости оказываемых услуг);
- Исполнитель в рамках выделенного бюджета:
 - должен предоставить полностью укомплектованное и работоспособное решение необходимое для обеспечения полноты использования запрашиваемой конфигурации;
 - может предложить свое аналогичное решение/оборудование (в том числе с превосходящими характеристиками), которое выполняет все поставленные цели и задачи, указанные в настоящем техническом задании (с учетом целевого назначения и показателей).

Также, необходимо отметить, что в соответствии с постановлением Президента Республики Узбекистан от 02.04.2021 года № ПП-5050, одним из основных задач

Единого центра оперативного управления при Главном управлении внутренних дел города Ташкента, является осуществление непрерывного мониторинга криминогенной и социальной обстановки на территории столицы, управление соответствующими силами и средствами органов внутренних дел, Национальной гвардии, Министерства по чрезвычайным ситуациям и хокимията города Ташкента, привлеченными для обеспечения общественной безопасности.

В связи с чем, а также, принимая во внимание то, что в рамках данного проекта возможно взаимоинтеграция информационных систем (ИС) сторонних ведомств и организаций, инициатору необходимо согласовать данное техническое задание в соответствии с постановлением Президента Республики Узбекистан от 18.04.2018 г. № ПП-3673.

Помимо этого, в целях расширения круга потенциальных поставщиков/производителей (исполнителей) инициатору рекомендуется рассмотреть возможность приобретения аппаратных средств и программного обеспечения по отдельным лотам.

4.1.12.2. Требования к страхованию

Поставщик обеспечивает страхование закупаемого оборудования до момента доставки на территорию, указанную в договоре.

4.1.12.3. Требования к упаковке и отгрузке товара

В соответствии с НТД завода–изготовителя. Товар должен упаковываться в упаковку обеспечивающую полную сохранность продукции при перевозке, с учётом возможных перегрузок и длительного хранения. Упаковка должна обеспечивать сохранность оборудования и защиту его от механических повреждений, прямого атмосферного воздействия и коррозии.

4.1.12.4. Требования по передаче заказчику технических и иных документов при поставке товаров

Техническая документация должна быть выполнена на русском языке:

- счёт-фактура (инвойс) на сумму общей стоимости отгруженного товара на имя Заказчика;
- сертификаты качества;
- технический паспорт или др.;
- сертификаты происхождения и качества;

4.1.12.5. Требования к оснащению системы устройствами для обучения персонала

Комплекты и составные части системы должны быть укомплектованы методической литературой, обеспечивающей обучение персонала как самостоятельно, так и в методических классах, при групповых занятиях или аттестации.

Разрабатываемая Система должна быть обеспечена документацией для обучения персонала. В состав документации входят:

- руководство пользователя;
- руководство системного администратора.

4.2. Требования к функциям (задачам), выполняемым системой и вспомогательному оборудованию

Функции (задачи) Системы реализуются функциональными компонентами Системы и входящими в их состав функциональными подсистемами.

Определенные настоящим техническим заданием требования к функциям (задачам), выполняемым Системой, уточняются на этапах технического проектирования и разработки проектной документации на Систему.

В комплект поставки Системы должны входить необходимые инструменты диагностирования и обслуживания оборудования и материалов для штатной работы Системы. При возникновении аварийной ситуации инструменты диагностирования должны позволить определить возникшие неисправности. В объем поставки ЦОД должны войти следующие инструменты, но не ограничиваясь:

- набор инструментов для осуществления монтажа медных;
- набор инструментов для осуществления монтажа электрических кабелей;
- набор портативных тестеров для осуществления тестирования соединительных кабельных линий связи и тестирования параметров электрической сети.

Все активное оборудование Системы должно в режиме реального времени предоставлять удобный интерфейс для мониторинга и диагностирования, а также поддерживать стандартные протоколы управления и мониторинга используя

протокол IP.

Все измерительное оборудование должно быть аттестовано в соответствии с ГОСТ РУ.

4.2.1. Требование к модулю интеграции распознавания и регистрация номерных знаков автотранспортных средств

Отображение на картографическом фоне мест размещения комплексов фото-видео фиксации ТС и нарушения правил дорожного движения в виде пиктограмм;

Ведение статистики перемещения транспортных средств по данным камер фото-видео фиксации с возможностью поиска любого ТС за указанный промежуток времени;

Построений маршрута ТС по данным комплексов фото-виде фиксации ТС;

Должен быть интегрирован с база данных учета ТС для получение оперативной информации по запросу о владельца ТС;

Модуль должен быть интегрирован с база данных разыскиваемых ТС;

Автоматическое создание карточки происшествия при проезде разыскиваемым транспортным средством любой камеры фото-видео фиксации со звуковым и визуальным оповещением.

построение маршрута ТС на карте по данным комплексов фото-видео фиксации ТС;

представление данных на аналитических панелях в виде различных графических представлений данных показателей;

автоматическое обновление информационных панелей при поступлении новых данных в модуль хранилище данных;

фильтрация данных как в целом по всей информационной аналитической панели, так и в каждом отдельном отчете;

детализация при клике по объекту на графике, карте, интерактивной схеме, в таблице с сохранением фильтрации;

просмотр дополнительных материалов (файлов, при наличии в среде пользователя соответствующих приложений), прикрепляемых к элементам информационной панели;

4.2.2. Требование к модулю интеграции видеонаблюдения

Отображение на картографическом фоне мест размещения камер видеонаблюдения в виде пиктограмм;

Просмотр изображения с выбранных камер видеонаблюдения;

Просмотр видеоархива с камер видеонаблюдения за указанный период времени;

Вывод списка камер видеонаблюдения, наблюдающих место происшествия, просмотр изображения в реальном времени.

Возможности сортировку, группировку камер видеонаблюдение по назначению;

Возможности экспортировать фрагменты видеоархива на внешней носитель (USB, HDD);

Функции снимков (Snapshot);

На карте местности внесение в базу данных основных сведений о камеры видеонаблюдение;

Отображение на карте местности состояние (о наличии связи) камер в виде пиктограмм для визуальной оценки;

Должно поддерживать протокол Onvif;

Все функционалы должна внедрена в отдельном слое ГИС;

4.2.3. Требование к модулю интеграции видеоаналитики

Модуль должен обеспечить обмен данными между сервером видеоаналитики и ГИС

На карте местности назначит функционал камер или групп камер;

Возможности передачи IP адреса камер или групп камер на сервер видеоаналитики для дальнейшей работа с групп камерой.

Возможности поиска события по заданным атрибутам и вывести результаты за указанный период времени;

Проигрывать виде фрагменты по выбранном критерием;

Экспорт видео фрагмента на внешней носитель (USB, HDD)

Все функционалы должна внедрена в отдельном слою ГИС;

Все действия, связанный с сервером видеоаналитики должны сохранено в хронологическом порядке для восстановления действия оператора

Все тревожный сигналы поступающий от севера видеоаналитики должно сопровождается со звуковым и визуальным оповещением;

4.2.4. Требование к модулю интеграции распознавание лиц

Модуль должен обеспечить обмен данными между сервером распознавание и ГИС

На карте местности назначит функционал камер или групп камер;

Возможности передачи IP адреса камер или групп камер на сервер распознавание для дальнейшей работа с групп камерой.

Возможности поиска события по заданным атрибутам и вывести результаты за указанный период времени;

Проигрывать виде фрагменты по выбранном критерием;

Экспорт видео фрагмента на внешней носитель (USB, HDD)

Все функционалы должна внедрена в отдельном слою ГИС;

Все действия, связанный с сервером распознавание должны сохранено в хронологическом порядке для восстановления действия оператора

При обнаружение разыскиваемого человека на карте местности отображать фотографии с возможностью цифрового увеличение;

Все тревожный сигналы поступающий от севера распознавание должно сопровождается со звуковым и визуальным оповещением;

Возможности загрузки видеофрагмента для поиска определенного лица в видеофайле;

4.2.5. Подсистема информационно-аналитическая

Подсистема информационно-аналитическая – основной профессионально-ориентированный компонент Системы. Данная подсистема предназначена для

потокowego распознавания и оперативного выявления лиц, находящихся в розыске в местах массового скопления людей, путем автоматической процедуры сравнения лиц в видеопотоке с камер видеонаблюдения с лицами, хранящимися в базе данных МВД. Взаимодействие с базами данных осуществляется посредством системы интеграции. Результаты идентификации доступны оператору, находящемуся в ситуационном центре с возможностью передачи информации о совпадении сотруднику правоохранительных органов на мобильное устройство. Для минимизации времени реагирования система использует географические координаты (GPS). Все сигнатуры передаются в СУБД для хранения.

Подсистема строится на уровне ядра Системы и состоит из ресурса аппаратно-программного комплекса, реализующего:

- потокowego распознавания лиц, сверка с базами данных, информирование;
- отложенный поиск по лицам, зафиксированным системой потокowego распознавания;
- поиск лиц по Базам граждан;
- видеоаналитика;
- управление/обновление Баз данных;
- хранение видеоконтента;
- геоинформационная система.

4.2.5.1. Задачами подсистемы в целом являются:

- визуальная фиксация и документирование оперативной обстановки в поле обзора видеокамер;
- выявление лиц, находящихся в розыске, на основе мониторинга потока людей с использованием оперативной портретной идентификации;
- выявление лиц, находящихся в розыске по загруженным фотографиям в систему или фотографиям отправленным через мобильные устройства;
- идентификация лиц по загруженным фотографиям в систему или фотографиям отправленным через мобильные устройства и верификация по общегражданской базе данных лиц;
- хранение и обработка видеoinформации, предоставление удаленного санкционированного доступа к видеоархиву, обеспечение возможности и восстановления хода событий на основе архивированных видеоматериалов;
- дистанционное управление видеокамерами;
- диагностика всех компонентов системы видеонаблюдения;
- унификация создаваемой системы, возможность подключения широкого спектра оборудования (видеокамер) разных производителей, в целях обеспечения надёжности за счет построения модульной, отказоустойчивой системы;

- возможность подключения локальных существующих систем видеонаблюдения на объектах, при соответствии техническим требованиям, предъявляемым в системе;
- отображение на карте, быстрый поиск, принятие решений и передача информации адресно с использованием ресурсов геоинформационной подсистемы;
- создание ресурса для дальнейшей модернизации.

4.2.5.2. Реализуемые функции подсистемы:

Подсистема должно в режиме реального времени определить и распознавать лиц находящий в поле зрения камер, при условии не более 20 лиц в кадре и проводит сравнение по базе данных «Розыск» (не более 20 000 единиц информации). Вероятность положительного обнаружения лица по отклонению от анфаса до 45 градусов (крен, рыскание, тангаж) составляет не менее 90%, вероятность положительной идентификации при условии межзрачкового расстояния не менее 50 пкс составляет не менее 90%, вероятность ложноположительной идентификации должна составлять не более 0,5%.

- потоковое распознавание лиц, поиск по базам данных, уведомление в случае совпадения;
- поиск по базе данных всех лиц, зафиксированными системой распознавания лиц. (Объем базы данных 300 Млн. лиц);
- поиск по общегражданской базе данных лиц. (Объем базы данных 25Млн записей);
- аналитическая обработка видео фрагментов в целях установления личности по общегражданской базе данных. (Объем базы данных 25 Млн);
- аналитическая система видеонаблюдения. Поиск по видеоархиву (глубина архива не менее 30 суток);
- управление, хранение и автоматическое обновление баз данных из источников данных;
- возможность создания списков для наблюдения за иностранными гражданами и построения трекинга в случае оперативной необходимости;
- аналитика и поиск по видеоконтенту;
- отображение камер на карте при помощи геоинформационной системы;

4.2.5.3. Дополнительный функционал:

- демографический анализ;

По запросу:

- внутреннее расследование инцидентов по видеоархиву, таких как: забытые и оставленные предметы, конфликтные ситуации на входе;

- создание отдельных списков и категорий с возможностью уведомления сотрудников о посещении объекта (магазинные воры, скандалисты, асоциальные личности);

Доступ пользователей к информационной системе, осуществляется используя персональные данные для доступа: логин, пароль (или еще более защищенный доступ с помощью ЭЦП) и ограничением по IP адресу.

Программное обеспечение АПК предоставляется Заказчику, как единое комплексное решение с возможностью доработки (внесение программных и настроечных изменений).

4.2.6. Геоинформационная подсистема

Подсистема должен обеспечить пользователей едиными пространственными данными, с учетом разграничения доступа к формированию данных и их чтения.

Подсистема предназначен для выполнения следующих функций:

формирование единого электронного оперативного плана города для отслеживания текущей обстановки;

отображение на единой электронной карте города значимых объектов инженерной, транспортной и социальной инфраструктуры;

наглядное отображение данных, содержащихся в паспортах безопасности объектов и территории;

4.2.6.1. Основные задачи Подсистемы

Основными задачами создания подсистемы являются:

обеспечение разделения доступа к формированию данных и получению данных в соответствии с действующими регламентами ведомственного и межведомственного взаимодействия;

визуализация хранимой информации:

совокупной информации на электронной карте (объекты, события), связанной с задачами решаемыми ведомствами

обеспечение получение «статичных» пространственных данных из органов государственной власти, уполномоченных на её ведение;

обеспечение механизмов обмена пространственными данными со смежными Сервисами.

4.2.6.2. Требования к организации Подсистемы

Организационная структура Подсистемы определить на этапе проектирования.

На этапе ввода в эксплуатацию Сервиса Исполнитель должен разработать регламенты информационного взаимодействия с «поставщиками» и

«потребителями» пространственных данных в соответствии с действующими нормативными актами.

Предусмотреть в регламентах процедуры инициации создания новых слоев, в рамках комплекса, ведомства. Ведомство иницирует создание нового слоя и правила доступа к нему. Оператор Сервиса предоставляет доступ к данным иным ведомствам и организациям, на основе разрешений, сформированных ведомством-инициатором.

4.2.6.3. Функциональные требования к Подсистеме

Геоинформационная подсистема должна обеспечивать выполнение следующих основных функций:

обеспечение разделения доступа к данным на уровне протокола запроса данных; возможность получения и передачи данных в форматах, используемых в органах государственной власти;

возможность получения и передачи данных в форматах, используемых в смежных системах в режимах полной поставки данных и частичного обновления информации;

выведение краткой семантической информации по объектам на карте;

создание, отображение данных, копирование и удаление выбранного объекта или электронного документа;

управление семантическими данными (просмотр и редактирование полей карточки объекта в соответствии с установленными правами доступа);

установка связей между объектами различных типов по заданным параметрам в соответствии с информационной моделью данных и установленными правами доступа пользователя Комплекса «Безопасный город»;

реализация и настройка корректности заполнения полей (ограничения, подстановки), и уведомление об отсутствии или наличии связей между объектами, в т. ч. пространственными и непространственными;

настройка корректности заполнения полей (ограничения, значения по умолчанию, вычисляемые значения) и уведомление о некорректности заполнения;

заполнение значений полей пространственных объектов на основе их геометрических характеристик (площадь, длина, периметр);

группировка и сортировка списка объектов по значению их атрибутов или группы атрибутов;

хранение истории изменения данных по слоям и объектам;

ведение журнала изменений по каждому объекту с возможностью отката изменений и отображением информации кто, когда и какие внес изменения.

Геоинформационная подсистема должна обеспечивать картографические функции:

получение информации об объектах, расположенных в выбранной точке карты;

проверка площадных объектов на предмет корректности геометрии перед сохранением в БД;

поиск пространственных объектов на карте по координатам точки;

настройка стилей оформления для типов пространственных объектов (точечных, линейных, площадных, растровых) применяющихся при выполнении условий на атрибуты;

управление видимостью данных в зависимости от масштаба и позиционирования карты (обеспечение динамической подгрузки данных и работы с большим количеством объектов на слоях);

экспорт и печать фрагментов карты с качеством не менее 300 точек на дюйм, возможностью задавать фактический размер области печати карты и масштаб карты, поддержкой различных форматов бумаги и сохранением точности заданного масштаба;

экспорт графических данных в векторные и растровые форматы (*.tab, *.shp, *.pdf, *.jpg), создание шаблонов для экспорта, экспорт набора данных, в том числе строго определенного, необходимого для подготовки графического отчета;

управление видимостью и порядком отображения слоев;

отображение картографической легенды;

создание тематических карт, конфигурационные инструменты настройки тематических карт, сохранения настроек, сохранение и редактирование тематических шаблонов;

работа с растровыми изображениями (подключение геопривязанного растра в виде слоя карты, просмотр растра под векторным изображением);

вывод на просмотр семантической информации выбранного пространственного объекта;

построение ведомости координат поворотных точек, экспликационной ведомости, как части отчета;

формирование графических отчетов. Печать подготовленных графических отчетов в произвольном формате вплоть до А0.

Геоинформационная подсистема должна позволять расширять количество хранимых слоев и обеспечивать хранение следующих пространственных данных:

цифровые ортофотопланы с линейным разрешением на местности до 0,6 м;

единую цифровую картографическую основу (ЕЦКО).

Цифровой топографический план М 1:2 000;

номенклатуры планшетной сетки масштаба 1:2000 и 1:10000, в основе своей имеющие местную систему координат;

документы территориального планирования, градостроительного зонирования и проектов планировки территории в следующих масштабных рядах соответственно:

1:25000 или 1:10000, 1:25000 или 1:10000, 1:5000 или 1:2000;

учет земель и объектов недвижимости в масштабах 1:5000 или 1:2000;

ведение реестров прав, привязанных к карте;

ведение адресного реестра;

улично-дорожную сеть;

жилые и нежилые кварталы;

адресную систему жилых домов, нежилых зданий и сооружений населенных пунктов;

границы населенных пунктов РУз. и прилегающих территорий;

кадастровое деление на кадастровые кварталы с привязкой к улично-дорожной сети;

имущество и земельный кадастр;

информация об объектах туризма и спорта;

информация об объектах социальной сферы;

тематические слои, включающие: функциональное зонирование территории, историко-культурное наследие, санитарно-защитные зоны, объекты здравоохранения, объекты образования, территории и объекты, подверженные риску возникновения чрезвычайных ситуаций природного и техногенного характера и прочие, необходимые для обеспечения безопасности города.

Геоинформационная подсистема должна обеспечивать хранение в адресном справочнике (совместно и отдельно) названий объектов альтернативными наименованиями, закрепившимися в «просторечном» обиходе.

4.2.6.4. Описание технологической реализации Подсистемы

На этапе проектирования Подсистемы исполнителем должен быть составлен исчерпывающий перечень слоев необходимых для обслуживания задач ведомств.

4.2.7. Подсистема информационно-аналитическая

Программное обеспечение подсистемы видеонаблюдения и видеоанализа, должно обладать следующими функциями:

Потоковое распознавание лиц, поиск по базам данных, уведомление в случае совпадения;

Поиск по базе данных всех лиц, зафиксированных системой распознавания лиц.

Поиск по общегражданской базе данных лиц.

Аналитическая обработка видео фрагментов в целях установления личности по общегражданской базе данных.

Аналитическая система видеонаблюдения

Поиск по видеоархиву, глубина хранения которого составляет 30 дней;

Управление, хранение и автоматическое обновление баз данных из источников данных;

Возможность создания списков для наблюдения за иностранными гражданами и построения трекинга в случае оперативной необходимости;

Аналитика и поиск по видеоконтенту;

Отображение камер на карте при помощи геоинформационной системы;

12. Предоставление информации по интересующим лицам для заинтересованных ведомств.

13. Иерархическая организация видеоисточников. Распределение прав пользователей по доступу к источникам видео и событий по аппаратному или логическому принципу. Каждый дежурный должен иметь полномочия по доступу к источникам на просмотр, модернизацию параметров, получение текущего состояния, просмотр архива с указанием глубины и т.д. в соответствии с его служебными полномочиями;

14. Установка степени важности тревог с определением группы операторов-получателей;

15. Оперативное уведомление оператора об инциденте с предоставлением информации о времени, месте, характере ситуации, автоматическим предоставлением видеoinформации одновременно в записи и реального времени, а также поддержкой режима оценки оператором каждой из ситуаций;

16. Мониторинг состояния всех элементов системы в реальном времени из любой точки сетевой среды. Операторы должны получать информацию о работоспособности системы в реальном времени. При отказе узла должны получать тревожное сообщение;

17. Унифицированный интерфейс настройки сетевых источников видеосигнала с возможностью оперативного доступа. Система должна позволять из единого центра администрировать все распределенные источники видеосигнала;

16. Формирование в режиме реального времени базы данных распознанных целей;

17. Привязка зон обзора неподвижных видеокамер к карте охраняемого объекта, проекции мнемоник движущихся целей на карту объекта;

18. Выдача аудиовизуального сигнала оператору в случае возникновения тревожной ситуации;

19. Обеспечение круглосуточного наблюдения за ситуацией в зонах наблюдения;

20. Обеспечение просмотра архива с возможностью поиска видеофрагментов по определенным условиям (дата, время, камера, тип цели и т.д.).

4.2.7.1. Требования к подсистеме видеонаблюдения и видеоанализа

Видеокамеры или кодеры (преобразователи аналогового сигнала в цифровой) должны поддерживать интерфейс ONVIF. Передатчики сетевого видео, включая камеры и видеосервера, должны поддерживать компрессию H.264 (или выше).

4.2.7.2. Требования к аналитическим функциям подсистемы видеоанализа

Подсистема видеоанализа должна обладать возможностью реализации следующих нижеперечисленных аналитических функций в режиме реального времени и в режиме offline.

1. Идентификационные:

- сравнительная идентификация людей по биометрическим признакам лица;

2. Классификационные:

- определение пола, возраста и расы человека;

3. Ситуационные:

- обнаружение скопления людей, в том числе в несанкционированных местах;

- детектор оставленных предметов;

- реагирование на проход людей в заданном направлении (входы, выходы, переходы, коридоры и т.п.);

4. Сервисные:

- расфокусировка видеокамеры;

- загрязнение объектива видеокамеры;

- изменение фона;

- изменение зоны обзора, отворачивание камеры;

- заслонение объектива камеры.

4.2.7.3. Требования к клиентскому приложению подсистемы видеоанализа для операторов системы

Клиентское приложение подсистемы видеоанализа для операторов системы должно обеспечивать следующее:

- прием и обработку потока информации, поступающей от ядра Системы;

- обработку цветного изображения;

- управление отображением видеоинформации;

- формирование мультиэкранного изображения;

- вывод сигнальной информации оператору в случае обнаружения тревожной ситуации;

- вывод сигнальной информации оператору в случае положительного результата идентификации;

- возможность экспорта или распечатки выбранного кадра («стоп-кадр»);
- взаимодействие со средствами архивирования видеoinформации для просмотра архивов;
- возможность просмотра изображения с видеокамер или архива в полноэкранном режиме;
- возможность просмотра архивного изображения в выбранных зонах наблюдения при одновременном контроле текущей ситуации в других зонах;
- просмотр архива событий (фильтрация по типу событий, дате и другим параметрам);
- аутентификацию оператора;
- протоколирование всех действий оператора;
- сохранение работоспособности при кратковременном пропадании электропитания.

4.2.7.4. Состав анализа видеоданных

Анализ видеоданных состоит из:

- программного обеспечения;
- аппаратно-программного комплекса.

Программное обеспечение может состоять условно из нескольких модулей:

- модуль видеоидентификации лиц (ВИ);
- модуль видеоаналитики (ВА);
- модуль предоставления обзорного наблюдения.

4.2.8. Модуль видеоидентификации лиц (ВИ)

Условно система идентификации лиц может иметь модульную архитектуру и включать в состав следующие программные модули, но не ограничиваясь:

1. Программный модуль детектирования лиц;
2. Программный модуль вычисления биометрических шаблонов;
3. Функционал сравнения шаблонов с эталонами, хранящимися в базе данных;

Программный модуль детектирования лиц предназначен для обнаружения и выделения изображений лиц людей в видеопотоке, регистрируемом камерами из состава ВН.

Для каждой камеры модуль должен обеспечивать одновременное выделение не менее 4-х лиц в случае их нахождения в зоне регистрации.

Программный модуль вычисления биометрических шаблонов предназначен для формирования векторов признаков изображений лиц, выделенных модулем детектирования лиц.

Модуль вычисления биометрических шаблонов обеспечивает обработку данных, поступающих от модулей детектирования лиц.

Модуль вычисления биометрических шаблонов предназначен для формирования векторов признаков изображений лиц, выделенных модулем детектирования лиц.

Функционал сравнения шаблонов с эталонами, хранящимися в базе данных, должен обеспечивать сравнение векторов признаков изображений лиц, поступающих от модулей вычисления биометрических шаблонов, с векторами признаков изображений эталонных лиц, занесенных БД.

Программное обеспечение системы должно обладать следующими эксплуатационными характеристиками:

- вероятность детектирования лица в видеопотоке - не менее 90%, из выборки лиц, положительно зафиксированной детекторами видеоанализа;

Указанные характеристики должны обеспечиваться при следующих условиях:

- стабильной освещенности области лица в зоне регистрации от 150 до 10000лк;

- неравномерности освещенности области лица не более 50%;

- скорости движения людей до 5 км/ч;

- вероятность положительного обнаружения лица по отклонению от анфаса до 45 градусов (крен, рыскание, тангаж) составляет не менее 90%;

- вероятность положительной идентификации при условии межзрачкового расстояния не менее 50 пкс составляет не менее 90%;

- вероятность ложноположительной идентификации должна составлять не более 0,5%.

4.2.9. Модуль видеоаналитики (ВА).

ПО видеоаналитики предназначено для обнаружения и распознавания тревожных ситуаций в видеопотоке, зарегистрированном камерами из состава СВН.

ПО видеоаналитики должно иметь модульную архитектуру.

ПО должно обеспечивать возможность конфигурирования задач видеоаналитики для каждой камеры или групп камер.

ПО видеоаналитики должно включать в состав следующие программные модули:

- программный модуль видеоаналитики;

- интерфейс пользователя.

Программный модуль видеоаналитики предназначен для обработки видеопотока и решения в режиме реального времени следующих задач видеоаналитики:

- обнаружение объекта (человека) в запрещенной зоне;

- сервисный мониторинг и оценка работоспособности системы видеонаблюдения.

К задачам сервисного мониторинга относятся:

- потеря видеосигнала;
- затемнение изображения (в том числе отключение освещения);
- засветка изображения (в том числе поломка автоматической регулировки диафрагмы объектива);
- потеря контрастности (в том числе загрязнение объектива);
- изменение ориентации камеры.

Интерфейс пользователя должен обеспечивать выполнение следующих функций с использованием АРМ:

- настройку и конфигурирование ПО видеоаналитики;
- выборочный просмотр видеопотока, регистрируемого камерами из состава СВН в режиме реального времени;
- вывод результатов работы ПО с отображением текущих результатов видеоанализа;
- вывод сигнальной информации оператору в случае обнаружения тревожной ситуации;
- просмотр и редактирование архива тревожных ситуаций;
- просмотр видео архива;
- поиск события в архиве видеозаписей по заданию оператора: по дате и времени, типу тревожной ситуации.

ПО должно предусматривать разграничение прав доступа к функциям системы для различных групп пользователей.

В состав ПО видеоаналитики могут входить другие дополнительные модули, обеспечивающие функционирование ВА.

Окончательный состав и конфигурация СПО определяется на этапе проектирования системы.

ПО видеоаналитики должно обеспечивать следующие эксплуатационные характеристики:

- доля истинно положительных срабатываний от общего числа событий, которые требовалось обнаружить, - не менее 90%;
- доля истинно положительных срабатываний от общего числа срабатываний - не менее 90%.

Указанные характеристики должны обеспечиваться при следующих условиях регистрации:

- освещенность в зоне регистрации от 100 до 10000 лк;
- дистанция съемки от 5 до 30 м;
- плотность потока людей не более 1 чел./м²;
- скорость движения людей не более 5 км/ч;
- объем оставленного предмета от 0,001 м³.

В состав подсистемы могут входить другие дополнительные технические средства, обеспечивающие размещение и функционирование подсистемы ВА.

Точный состав, конфигурация и технические характеристики оборудования в составе подсистемы ВА, не определенные настоящими требованиями, уточняются на этапе проектирования системы в зависимости от условий эксплуатации на конкретном объекте.

4.2.10. Модуль предоставления обзорного наблюдения.

Данное ПО предназначено для приема и обработки (кодирование, сжатие) видеопотока от камер из состава ВН и его отображения на АРМ оператора с использованием интерфейса пользователя.

ПО должно удовлетворять следующим требованиям:

1. Поддержка форматов сжатия видео: Motion JPEG и H.264.;
2. Получение видеоданных по протоколам: RTP/RTSP и HTTP.;
3. Поддержка доступа пользователей к изображению с видеокамер в режиме реального времени и видеоархиву с:
 - АРМ с предустановленным специальным программным обеспечением способным работать под управлением операционной системы Windows.
4. Возможность получения видеоданных со сторонних систем видеонаблюдения с использованием технологии NAT;
6. Система должна поддерживать следующие индивидуально задаваемые для каждой видеокамеры режимы записи в видеоархив: непрерывно, по расписанию, по событию, по команде от внешней системы;
8. Поддержка резервирования системы таким образом, чтобы выход из строя одного из компонентов не привел к полной неработоспособности Системы;
9. Ведение единого реестра устройств видеонаблюдения, расположенных на определенной территории (города);
10. Отображение на цифровой карте местности мест установки камер видеонаблюдения с возможностью вывода на экран видеоизображения с выбранного (выбранных) устройств видеонаблюдения;
11. Отображение на экранах монитора оператора служебной информации: текущее время, текущая дата, номер и/или имя видеокамеры.

ПО должно предусматривать разграничение прав доступа к функциям системы для различных групп пользователей.

Для обеспечения функционирования СВН могут использоваться дополнительные прикладные программы. При этом все используемое ПО должно быть лицензировано.

Взаимодействие систем в составе СВН должно осуществляться на основе открытых стандартов сетевого видео.

4.2.11. Серверное оборудование для информационно-аналитической подсистемы

Серверное оборудование предназначено для приема и обработки видеопотока, регистрируемого видеоканерами, с помощью устанавливаемого на него программного обеспечения.

Сервера располагаются централизованно в ЦОД и объединяются ресурсами как единый комплекс.

Количество специализированных серверов определяется, исходя из требований к производительности системы:

- загрузка процессоров не более 80% при одновременном выполнении всех функций системы;
- количество ядер на обработку одного видеопотока - не более 2;
- время, затрачиваемое системой на идентификацию лица, т.е. с момента обнаружения лица в кадре до отображения на АРМ оператора положительного результата идентификации, не должно превышать 3 секунд.
- время, затрачиваемое системой на обнаружение тревожной ситуации, не должно превышать 5 секунд.

4.2.11.1. Дополнительные специальные требования к подсистеме хранения данных Системы

Данная подсистема предназначена для хранения как видеоинформации с камер видеонаблюдения, так и всей проанализированной информации в базе данных. База данных информации распознанных лиц и событий располагается централизованно в ЦОДе.

Количество серверов с общим объемом дискового пространства для системы хранения данных определяется исходя из количества видеоканер и требованиям к хранимой информации:

Требования к БД системы видео идентификации (ВИ) лиц:

БД в составе ВИ предназначена для хранения изображений лиц, относительно которых производится идентификация, их биометрических шаблонов и установочных данных. Базы данных располагаются по месту расположения серверов видео аналитики в ЦОДе и хранят метаданные о всех распознанных лицах с определенными метками от маркированными по «участкам».

Объем информации, хранимой в БД:

- объем биометрического шаблона – определяется в соответствии с характеристиками СПО;
- объем установочных данных – не более 10 кб;

Должно быть предусмотрено разделение лиц в БД по категориям.

Должна быть обеспечена возможность удаленной актуализации БД.

Требования к системе хранения системы видеоидентификации (ВИ) лиц:

Должно быть обеспечено архивирование следующих результатов работы ВИ:

1. Сжатого видеопотока от каждой из камер в составе ВИ:

- алгоритм сжатия – MJPEG, H.264;
- степень сжатия – не более 30%;
- частота – не менее 16 кадров/с;
- разрешение – не менее 2 мегапикселей;
- глубина архива – не менее 30 суток.

2. Выделенных изображений лиц (с исходным разрешением, без потери качества):

- формат - *.PNG, *.JPEG;
- объем - не более 150 кб;
- разрядность - 8 бит/пиксель;
- метаданные - дата, время, номер камеры, метка для поиска соответствующего видеофрагмента в архиве.
- глубина архива - не менее 30 суток.

Примечание - допускается хранение более одного выделенного изображения лица каждого прошедшего человека.

3. Изображений полных видеокадров, содержащих лицо, по которому была произведена идентификация (с исходным разрешением, без потери качества):

- формат - *.PNG, *.JPEG;
- объем - не более 1200 кб;
- разрядность - 8 бит/пиксель;
- глубина архива - не менее 30 суток.

4. Данных о результатах идентификации:

- дата, время, номер камеры;
- ссылка на изображения лиц в архиве;
- метка для поиска соответствующего видеофрагмента в архиве;
- идентификаторы записей в базе данных, относительно которых было принято решение об идентичности обнаруженного лица, и значения степени схожести (количество идентификаторов определяется значением ранга).

Требования к системе хранения системы видеоаналитики (ВА):

Должно быть обеспечено архивирование следующих результатов работы подсистемы ВА:

1. Сжатого видеопотока от каждой из камер:

- алгоритм сжатия - MJPEG, H.264;
- степень сжатия - не более 30%;
- частота - не менее 16 кадров/с;
- разрешение - не менее 2 мегапикселей;
- глубина архива - не менее 30 суток.

2. Метаданные - дата, время, номер камеры, тип ситуации, метка для поиска соответствующего видеофрагмента в архиве.

Требования к архивированию системы предоставления обзорного наблюдения.

Должно быть обеспечено архивирование сжатого видеопотока, регистрируемого видеокамерами из состава подсистемы ВН:

- алгоритм сжатия - MJPEG, H.264;
- степень сжатия - не более 40%;
- частота - не менее 12 кадров/с;
- разрешение - исходное;
- глубина архива - не менее 30 суток.

4.2.12. Требования к транспортированию

Оборудование может быть поставлено авиатранспортом, автотранспортом или железнодорожным транспортом в соответствии с Инкотермс – 2010 с условием поставки DDP.

4.2.13. Гарантийные обязательства

Гарантийный срок на поставляемое оборудование должен составлять не менее 12 месяцев со дня подписания Акта приемки-передачи на выполненную услугу. Гарантийная техническая поддержка осуществляется по месту эксплуатации оборудования. Если в течение гарантийного срока продукция окажется дефектной, неукомплектованной и не будет соответствовать требованиям настоящего технического задания, либо ТУ изготовителя, Исполнитель обязан устранить дефекты, документировать, а случае невозможности заменить продукцию на новую после получения письменного уведомления Заказчика. Все расходы, связанные с устранением дефектов, доукомплектованием и заменой относятся за счёт Исполнителя. В случае сбоя или неправильного функционирования оборудования или программного обеспечения в течение гарантийного периода, произошедший из-за самой Продукции, Исполнитель гарантирует бесплатную наладку (ремонт) или восстановление оборудования или программного обеспечения в течение пятнадцати (15) дней с даты уведомления. Исполнитель гарантирует наступление даты окончания поддержки EOS (end of support/service) аппаратного обеспечения (всех комплектующих) не ранее чем через 5 лет с момента заключения договора поставки аппаратного обеспечения. Поддержка аппаратного обеспечения подразумевает доступность сервисного обслуживания всех блоков и компонентов аппаратного обеспечения. Исполнитель гарантирует наступление даты окончания приема заказов, производства и поставки отдельных плат и модулей EOM (end of market for expansion) не ранее чем через 5 лет с момента заключения договора поставки аппаратного обеспечения. Т.е. Исполнитель гарантирует возможность размещения заказов, производства и поставки на территорию Республики Узбекистан отдельных плат и модулей для расширения емкости аппаратного

обеспечения в течение всего срока поддержки аппаратного обеспечения Исполнителем до даты EOS.

4.2.14. Требования по ремонтпригодности

Поставщик должен обеспечить консультирование по вопросам поддержки поставленного оборудования в работоспособном состоянии в течение всего гарантийного срока.

4.2.15. Требования к сервисному обслуживанию

Поставщик должен иметь на территории Республики Узбекистан, авторизованный сервисный центр по ремонту и обслуживанию поставленного оборудования. Срок выполнения сервисных, ремонтных работ не должен превышать 10 календарных дней с момента передачи оборудования.

4.2.16. Экологические и санитарные требования

Оборудование должно соответствовать действующим стандартам и нормам по пожарной, санитарной и электрической безопасности, а также электромагнитной совместимости, в соответствии с номенклатурой продукции, в отношении которой законодательными актами Республики Узбекистан предусмотрена обязательная сертификация с документальным подтверждением.

4.3. Требования к видам обеспечения

4.3.1. Требования к математическому обеспечению

Вне зависимости от типа математических моделей, алгоритмов и методов математическое обеспечение должно обеспечивать возможность, вместе с другими видами обеспечения, реализовывать весь комплекс функций, принятых для Системы.

Все алгоритмы должны быть разработаны с учетом возможности получения некорректной входной информации и предусматривать соответствующую реакцию на такие события, с целью проинформировать пользователей и администраторов, избежать простоев, выход из строя, отказ в обслуживании Системы в целом и отдельных подсистем. Способы использования математических методов и моделей определяются в процессе проектирования.

4.3.2. Требования к информационному обеспечению

Информационное обеспечение Системы должно удовлетворять следующим требованиям:

- сохранность данных от искажения, утечки и преднамеренного уничтожения;
- минимально необходимое дублирование и достоверность данных;
- создание различных отчетных форм (при необходимости).

Вне зависимости от использованных программных средств, уровень хранения данных в Системе должны быть построены на основе современных реляционных или объектно-реляционных СУБД. Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД.

Средства СУБД, а также средства используемых операционных систем должны обеспечивать документирование и протоколирование обрабатываемой в системе информации.

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

Структура базы данных должна быть организована рациональным способом, исключающим единовременную полную выгрузку информации, содержащейся в базе данных системы.

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

4.3.3. Требования к лингвистическому обеспечению

Лингвистическое обеспечение Системы должно быть достаточным для общения различных категорий пользователей в удобной для них форме со средствами автоматизации Системы и для осуществления процедур преобразования и машинного представления обрабатываемой в Системе информации.

В лингвистическом обеспечении должны быть:

1. Предусмотрены языковые средства для описания любой используемой в Системе информации;
2. Унифицированы используемые языковые средства;
3. Стандартизованы описания однотипных элементов информации и записи синтаксических конструкций;
4. Обеспечены удобство, однозначность и устойчивость общения пользователей со средствами автоматизации Системы.

Все прикладное программное обеспечение системы должно использовать русский или английский, или узбекский язык, либо комбинации двух перечисленных языков.

4.3.4. Требования к программному обеспечению

Программное обеспечение Системы должно представлять собой совокупность общего программного обеспечения (ОПО) и специального программного обеспечения (СПО).

Программное обеспечение Системы должно обладать открытой, компонентной (модульной) архитектурой, обеспечивающей возможность эволюционного развития, в частности, с учетом включения в состав средств информатизации новых объектов Системы.

Программное обеспечение, технология (включая нормативно-техническую документацию) его разработки должны обеспечивать возможность согласованной разработки унифицированного (типового) программного обеспечения силами нескольких разработчиков.

Программное обеспечение должно быть сертифицировано по требованиям безопасности информации.

4.3.5. Требования к общему программному обеспечению

ОПО должно представлять собой совокупность программных средств со стандартными интерфейсами, предназначенных для организации и реализации информационно-вычислительных процессов в Системе. Состав ОПО формируется при проектировании конфигурации АПК интегрируемых информационных систем.

ОПО должно обеспечить:

- выполнение информационно-вычислительных процессов совместно с другими видами обеспечения;
- управление вычислительным процессом и вычислительными ресурсами с учетом приоритетов пользователей;
- коллективное использование технических, информационных и программных ресурсов;
- обмен неформализованной и формализованной информацией между компонентами Системы, а также между Системой и пользователями с протоколами информационно-логического взаимодействия;
- ведение учета и регистрации передаваемой и принимаемой информации;
- ввод в базы данных информации с клавиатуры АРМ и с машинных носителей, а также информации, поступающей через телекоммуникационные средства;
- автоматизированный контроль и диагностику функционирования технических и программных средств, а также тестирование технических средств;
- создание и ведение баз данных с обеспечением контроля, целостности, сохранности, реорганизации, модификации и защиты данных от несанкционированного доступа;
- создание и ведение словарей, справочников, классификаторов и унифицированных форм документов, параллельный доступ пользователей к ним;

- поиск по запросам информации в диалоговом режиме и представление ее в виде документов;
 - выполнение распределенных запросов к данным;
 - синхронизацию корректировки данных и контроль за изменением документов в базах документов;
 - разработку, отладку и выполнение программ, формирующих распределенные запросы к данным;
 - формирование и ведение личных архивов пользователей;
 - организацию решения функциональных задач СПО;
 - наращивание состава общего программного, а также специального программного, информационного и лингвистического обеспечения;
 - обработку (формирование, контроль, просмотр, распознавание, редактирование, выдачу на средства отображения и печати) текстовой, табличной и графической информации;
 - восстановление работоспособности ПО и баз документов (из резервных копий) после сбоев и отказов технических и программных средств.
- ОПО должно поддерживать функционирование выбранных типов ПЭВМ и периферийных устройств на уровне операционных систем (ОС), утилит и драйверов. Операционные системы должны выбираться исходя из перспектив развития аппаратно-программных платформ в мире, с учетом поддержания преемственности версий и редакций, условий и порядка их обновления, предлагаемых фирмой - разработчиком. Количество ОС, их версий и редакций в Системе должно быть минимизировано.

ОПО может включать следующие основные компоненты:

- графические 32 (64 и более) - разрядные многозадачные (многопроцессорные) операционные системы;
- сетевые операционные системы;
- системы управления базами данных;
- телекоммуникационные программные средства, включая средства электронной почты;
- средства архивирования файлов;
- инструментальные средства для создания и ведения текстовых и графических документов, электронных таблиц и т.д.;
- средства поддержки Internet и Intranet -технологий;
- средства управления выводом данных на устройства отображения информации группового и коллективного пользования;
- технологические программные средства.

Должно быть обеспечено ведение депозитария для всего ПО, а также создание дистрибутивов для любого ПТК Системы и распространение программного обеспечения на все компоненты Системы.

Поставляемое ПО, если это предусмотрено существующей нормативной правовой базой, должно быть сертифицировано (в том числе по требованиям безопасности информации) или иметь соответствующие сертификаты. Вопросы его использования и тиражирования должны регулироваться соответствующими соглашениями или сублицензионными договорами.

4.3.6. Требования к техническому обеспечению

Техническое обеспечение — это совокупность всех технических средств, используемых при эксплуатации Системы.

4.3.6.1. Сервер структурирования видео

Наименование	
Сервер структурирования видео – 2 шт.	
Система	
Форм-фактор	не более 4U подсерверную стойку 19”
Глубина шасси	не более 446 мм
Процессор	не менее Встраиваемый в промышленность микроконтроллер
Операционная система	Linux
Интерфейсные Порты	
Аудио выход	1 канал, выход на динамик
Входной сигнал тревоги	16 каналов
Выходной сигнал тревоги	8 каналов
eSATA	1 порт
SAS	2 порта SAS 3.0
RS-232	1 порт
RS-485	1 порт
USB	4 порта
HDMI	3 порта
VGA	1 порт
Сеть	4 порта RJ-45 10/100/1000 Мбит/с, с самоадаптацией Ethernet
Питание	2 порта
Применение искусственного интеллекта	
Свойства человеческого тела	пол, возраст, верхний цвет, нижний цвет, анализ маски для рта.
AI Search	Поддерживает поиск по метаданным людей и транспортных средств.
Максимальный входящий поток	Не менее 512 Мбит/с

256-канальный доступ к	С помощью обычной IP-видео
Поток защиты периметра	Не менее 96 каналов
Поток метаданных видео	Не менее 96 каналов
Место хранения	
Слоты для HDD	24 слоты, каждый слоты должен поддерживать не менее 8ТБ
RAID	RAID 0/1/5/6/10
Общие характеристики	
Источник питания	200–240 В, 50/60 Гц, 5 А
Резервирование питания	Двойное резервирование питания с возможностью горячей замены
Потребляемая мощность	Мощность блока питания должна быть достаточной для полноценного функционирования оборудования на максимальной нагрузке с учетом резерва
Рабочая Температура	От 10 до 35 ° С (от 50 до 95 ° F)
Влажность при эксплуатации	35–80% относительной влажности, максимальная относительная влажность 90% при 40°С без конденсата.

4.3.6.2. Сервер анализ поведения человека

Наименование	
Сервер анализ поведения человека -1шт	
Система	
Форм-фактор	не более 4U подсерверную стойку 19”
Основной процессор	Встраиваемый в промышленность микроконтроллер
Операционная система	Linux
Рабочий интерфейс	WEB (PCAPP), локальный графический интерфейс
Применение искусственного интеллекта	
Обнаружение	С помощью обычной IP камеры видеонаблюдения
Поток метаданных видео	Не менее 96 каналов
Обнаружение плотности толпы	Обнаружение боевых действий
Параметры видео	
Удаленное подключение	Не менее 96 каналов
Пропускная способность сети	Входящая пропускная способность: не менее 512 Мбит/с Пропускная способность записи: не менее 384 Мбит/с Исходящая пропускная способность: не менее 128 Мбит/с
Видео выход	1-канальный выход VGA, 3-канальный выход HDMI, выходы VGA 1 / HDMI 1 на тот же источник видео

	Поддержка вывода 4К
Сторонняя поддержка протоколов	Onvif; RTSP; Sony; Panasonic; Axis; Arecont; Pelco; Canon; Samsung
Рабочий интерфейс	WEB (PCAPP), локальный графический интерфейс
Сжатие	
Видео сжатие	Smart H.265+; Smart H.264+; H.265; H.264
Аудио сжатие	G.711A; G.711U; PCM; G726
Сеть	
Протокол	HTTP; HTTPS; TCP / IP; IPv4; RTSP; UDP; SMTP; NTP; DHCP; DNS; DDNS; P2P
Мобильный телефон	DMSS
Совместимость	ONVIF (Профиль S, T и G); CGI; SDK
Браузер	Chrome; PCAPP; IE9 или выше; Firefox
Сетевой режим	Режим привязки NIC, такой как многоадресный режим, балансировка нагрузки, отказоустойчивость и т. д.
Место хранения	
Слоты для HDD	24 слоты, каждый слоты должен поддерживать не менее 8ТБ
RAID	RAID 0/1/5/6/10
Периферийный интерфейс	
Аудио выход	1 канал, выход на динамик
Входной сигнал тревоги	16 каналов
Выходной сигнал тревоги	8 каналов
eSATA	1 порт
SAS	2 порта SAS 3.0
RS-232	1 порт
RS-485	1 порт
USB	4 порта
HDMI	3 порта
VGA	1 порт
Сеть	4 порта RJ-45 10/100/1000 Мбит/с, с самоадаптацией Ethernet
Питание	2 порта
Общие параметры	
Источник питания	100–240В переменного тока, 50 ± 2% Гц
Потребляемая мощность	Мощность блока питания должна быть достаточной для полноценного функционирования оборудования на максимальной нагрузке с учетом резерва
Рабочая Температура	От 10 до 35 ° C (от 50 до 95 ° F)
Влажность при эксплуатации	35–80% относительной влажности, максимальная относительная влажность 90% при 40°C без конденсата.

4.3.6.3. Сервер интеграции

Наименование	
Сервер интеграции -1 шт	
Система	
Форм-фактор	не более 4U подсерверную стойку 19"
Глубина шасси	не более 450 мм
Процессор	не менее двух 8-ядерных процессоров
Операционная система	LINUX
Оперативный память	не менее 256GB RDIMM, 3200 MT / c
HDD	не менее 4ТБ
SSD	не менее 1920Гб
RAID	H330
Интерфейсные Порты	
Сетевые порты	не менее 8 гигабитный портов
USB	не менее 2 порта USB 3.0 на передней панели и 3 порта USB 3.0 на задней панели
VGA	не менее 1 порта VGA
Другие порты	не менее 1 сериал порт
Общие характеристики	
Источник питания	110V–240V AC
Потребляемая мощность	Мощность блока питания должна быть достаточной для полноценного функционирования оборудования на максимальной нагрузке с учетом резерва
Рабочая Температура	От 10 до 35 ° C (от 50 до 95 ° F)
Влажность при эксплуатации	10–80% относительной влажности, максимальная относительная влажность 90% при 40°C без конденсата.
Программные компоненты должен отвечать не ниже следующего требование	
Назначение	<ul style="list-style-type: none"> - профессиональное и комплексное средство управления система. - взаимодействия с самыми передовыми технологиями такими как искусственный интеллект, облачные вычисления, большие данные; - должен обеспечивать возможность унифицированного доступа к устройствам, основным данным услуги и даже услуги по дальнейшему развитию для верхняя платформа для создания интегрированных продуктов общественной безопасности который в основном сосредоточен на наблюдении за общественной безопасностью на основе корреляционного анализа массивных данных.
Сервисы	· Сервис учетной записи

	<ul style="list-style-type: none"> · Сервис хранения · Сервиса системы правил · Облачная сервис базы данных · Сервис интеллектуального анализа · Сервис передачи мультимедиа · Сервис управления устройствами
Расширяемость	<ul style="list-style-type: none"> · Высокоэффективные условия обслуживания или легкость обновление с помощью распределенного аппаратного расширения и каскадный. · Быстрое расширение. · Резервное копирование и восстановление базы данных · Автоматическая балансировка нагрузки на соответствующий узел данных при добавлении устройства.
Лог	Системный, админский, клиентский журнал Поиск и экспорт журнала.
Управление ролями и пользователями	Управляет разрешениями пользователя через роль (устройство разрешение, управление разрешениями). Пользователю могут быть назначены роли для получения соответствующие разрешения. Пользователь может быть ограничен MAC-адресом и сроком действия.
Внешний интерфейс	Поддержка передачи данных и изображений на сторонние платформы
Каскадирование	Поддержка внутреннего агрегирования данных платформы нижнего уровня на платформу верхнего уровня.
Индивидуальная стыковка	Поддержка разработки пользовательских протоколов и стыковки

4.3.6.4. Сервер МРР база данных

Наименование	
Сервер МРРбаза данных-2 шт	
Система	
Форм-фактор	не более 1U подсерверную стойку 19"
Основной процессор	не менее двух 8-ядерных процессоров
Операционная система	Linux

Оперативный память	не менее 128G RDIMM
HDD	не менее 2ТБ
SSD	не менее 960Гб
Периферийный интерфейс	
SAS	не менее 2 порта SAS 3.0
USB	не менее 4 порта
VGA	не менее 1 порт
Сеть	не менее 8 порта RJ-45 10/100/1000 Мбит/с, с самоадаптацией Ethernet
Общие параметры	
Источник питания	115–230В переменного тока, $50 \pm 2\%$ Гц
Потребляемая мощность	Мощность блока питания должна быть достаточной для полноценного функционирования оборудования на максимальной нагрузке с учетом резерва
Рабочая Температура	$t + 10^{\circ} \text{C}$ до $+ 35^{\circ} \text{C}$ (от $+ 50^{\circ} \text{F}$ до $+ 95^{\circ} \text{F}$)
Программные компоненты должен отвечать не ниже следующего требование	
Хранение и управление метаданными	Data Storage: использует распределенную архитектуру без совместного использования, чтобы наилучшим образом использовать ЦП, память, сеть и емкость жесткого диска каждого хоста, а также поддерживает горизонтальное расширение и высокую надежность. Поддерживает несколько режимов хранения, таких как строка, столбец и смешанный режим строки и столбца, и предоставляет интерфейсы Restful и SQL для приложений верхнего уровня на основе различных сценариев.
Статистика потока данных	поддерживает статистику потока подключенных данных, включая как нормально, так и аномально сохраненные данные.
Доступ к данным	4000 единиц данных в секунду
Обработка данных	мощность обработки данных может составлять до 3 миллионов единиц данных в день. Расширение емкости доступно, если требуется большая мощность обработки.
Запрос данных	среднее время ответа 1 секунда для нечеткого запроса и точного запроса 100 миллионов данных.
Анализ данных	один сервер облачной базы данных может хранить и анализировать 500 миллионов единиц данных. Кластер поддерживает до 100 узлов.
Управление жизненным циклом данных	поддерживает управление жизненным циклом данных, к которым осуществляется доступ. Аварийная перезапись помогает избежать прерывания обслуживания, когда емкость диска достигает порогового значения.

4.3.6.5. Коммутатор на 24 порт

Наименование	
Коммутатор 24 порта-1шт	
Порты	
Интерфейсы	Не менее 20 портов 10/100BASE-TX Не менее 4 порта 10/100/1000BASE-T Не менее 4 порта 100/1000BASE-X SFP
Gigabit Ethernet:	Не менее 2000 Mbps (full-duplex)
Сетевые протоколы	IEEE 802.3, IEEE 802.3u, IEEE802.3ab, IEEE 802.3x
Коммутационная матрица	Не менее 20 Гб/с
Скорость перенаправления пакетов	Не менее 14Mpps
Приоритетные порты	1-8
Особенности	
Метод коммутации	Передача с промежуточным хранением
Размер таблицы MAC-адресов	Не менее 16К
Общие параметры	
Питание	В диапазоне AC: 100~240VAC, 50~60Hz DC: 11-13VDC
Защита от петли	Поддерживается (изоляция порта)

4.3.6.6. Коммутатор на 16 порт

Наименование	
Коммутатор системы -2шт	
Порты	
Интерфейсы	Не менее 16 порт 10/100/1000/10 000 Мбит/ Не менее 4 порта восходящими соединениями 1/10 GbE SFP+ Скорость порта - порта RJ-45 1000/10000 SFP+ 1/10GbE
Gigabit Ethernet:	Не менее 2000 Mbps (full-duplex)
Сетевые протоколы	веб-браузер / SNMP Manager / HTTPS / RMON1 /FTP
Коммутационная матрица	Не менее 20 Гб/с
Скорость перенаправления пакетов	Не менее 238 Mpps
Приоритетные порты	1-16
Особенности	
Метод коммутации	Передача с промежуточным хранением

Размер таблицы MAC-адресов	Не менее 16К
Общие параметры	
Питание	В диапазоне AC: 100~240VAC, 50~60Hz DC: 11-13VDC
Защита от петли	Поддерживается (изоляция порта)

4.3.6.7. Источники бесперебойного питания

Источники бесперебойного питания UPS-2шт	
Мощность	мощность ИБП должна быть достаточной для обеспечения автономной работы подключаемых к нему оборудования в течении не менее 30 минут
Тип	двойного преобразования, on-line
Управление	RS-232 порт, USB порт, LCD дисплей, ПО для управления
Наличие защиты	высоковольтных импульсов
Общие параметры	
Гарантия	не менее 1 год.

4.3.6.8. Серверная стойка 42U

Наименование	
Серверная стойка-2шт	
Тип	Металлическая, перфорированные передняя и задняя двери;
Высота	не менее 42U;
Ширина	не менее 600мм;
Глубина	не менее 1000мм;
Комплектация	о ригельный замок
Комплект	2 полки, 4 вентиляторы

4.3.6.9. Серверная стойка 22U

Наименование	
Серверная стойка-1шт	
Тип	Металлическая, перфорированные передняя и задняя двери;
Высота	не менее 22U;
Ширина	не менее 600мм;
Глубина	не менее 800мм;

Комплектация	о ригельный замок
Комплект	2 полки, 4 вентиляторы

4.3.6.10. Межсетевой экран

Наименование	
Межсетевой экран-2шт	
Порты	
Интерфейсы не менее	2x GE RJ45 Management/HA Ports • 2x GE RJ45 WAN Ports • 14x GE RJ45 Ports • 4x GE SFP Slots
Gigabit Ethernet:	Не менее 2000 Mbps (full-duplex)
Сетевые протоколы	веб-браузер / SNMP Manager / HTTPS / RMON1 /FTP
Коммутационная матрица	Не менее 20 Гб/с
Скорость перенаправления пакетов	Не менее 238 Mpps
Приоритетные порты	1-16
Производительность IPS	Не менее 2.2 Гбит/с
Производительность NGFW	Не менее 1.8 Гбит/с
Число одновременных SSL-VPN пользователей (максимум)	500
Производительность межсетевого экрана	Не менее (1518 / 512 / 64 byte) 20/ 20/ 9Гбит/с
Особенности	
Метод коммутации	Передача с промежуточным хранением
Размер таблицы MAC-адресов	Не менее 16К
Максимальное число устройств двухфакторной аутентификации	5000
Общие параметры	
Питание	100–240V AC, 50–60 Hz.
Защита от петли	Поддерживается (изоляция порта)

4.3.6.11. Экран (монитор) для видеостены

Экран (монитор) для видеостены-76 шт	
Тип экрана	LCD

ЖК матрица	PID
Размер экрана	не менее 55"
Размер пикселя	Не менее 40dpi
Разрешение экрана	Не менее 1920x1080
Яркость	Не менее 500кд/м2
Контраст	Не менее 4000:1
Время ответа	Не более 8мс
Цвет	Не менее 16.7Млн
Область обзора	Не менее 1018.08 x 572.67мм
Угол обзора	Горизонталь: не менее 178°, вертикаль не менее 178°
Шов экрана	3.5мм
Разъемы	Не менее 1 HDMI
	Не менее 1 BNC
	Не менее 1 DVI,
	Не менее 1 YPbPr
Выходы	Не менее 2 BNC
	Не менее 1 DVI
	Не менее 1 VGA
Источник питания	В диапазоне 90 ~ 264В AC
Рабочие условия	В диапазоне 0°С ~ 40°С, влажность 10%~85%
Время работы	не менее 60 000 часов
Крепление для видеостена 55" -76 шт	
Тип	Металл

4.3.6.12. Матрица

Матрица - 1 шт	
Видеовход VGA и DVI-I не менее	WSXGA: 1680×1050/60Гц WXGA: 1440×900/60Гц WXGA: 1280×800/60Гц, 1366×768/60Гц 1080p: 1920 × 1080@50/60Гц UXGA: 1600 ×1200@60Гц XVGA: 1280 ×960@60Гц 720p: 1280 ×720@50Hz/60Гц SXGA: 1280 ×1024@60Гц XGA: 1024 × 768@60Гц
Выход HDMI	Не менее 4 каналов
	1080p: 1920 × 1080@50/60Гц WSXGA: 1680×1050/60Гц UXGA: 1600 × 1200@60Гц (только для четных интерфейсов) 720p: 1280 × 720@50Гц/60Гц

	SXGA: 1280 × 1024@60Гц XGA: 1024 × 768@60Гц
ВНС выход	не менее 2 каналов, 2 DB 15
Разрешение	До 12 Мп
Каналы декодирования	120 каналов
Синхронное воспроизведение	12MP@20к/с 4 каналов 2MP@30к/с: 80 каналов D1 @30к/с: 160 каналов
Разделение экранов	1/4
Сетевой интерфейс	Не менее 1, RJ45 10М /100М/1000М управляемых сетевых интерфейса
Последовательный интерфейс	Не менее 1 RS-485 Не менее 1 RS-232
Удаленное преобразование аналогового	цифрового видео на видеостену
Поддержка матричного	Поддержка матричного коммутатора и выхода видеосигналов SD/HD
Поддержка жостик	Коммутатор с поддержкой через сетевую клавиатуру, клиентскую часть и т. д
Аудио выход	Не менее 4 каналов, 2 DB 15
Питание	АС100-240В
Рабочие условия	от -10°С до +55°С, влажность 10% ~ 90%

4.3.6.13. Карта кодирования

Плата для ПК отображения-1 шт	
Карта кодирования	Не менее 16CH HDMI UHD
Video Input	HDMI
Encoding Format	H.264/MPEG4
EncodingCapacity	16CH@1080P

4.3.6.14. Джойстик

Сетевая клавиатура-1шт	
Видео и управление	Управление поворотными камерами
Наружный интерфейс	
Интерфейс передачи	Не менее 1 RJ45 10/100 Mbps адаптивный Ethernet интерфейс; не менее 1 RS-232 интерфейс (для настройки параметров и тех. обслуживания); не менее 1 RS-422 интерфейс; не менее 1 RS-485 интерфейс; не

	менее 1 USB2.0 интерфейс (для хранения данных и обновления устройства)
Возможности	
Учетные записи	Не менее 16 учетных записей пользователей: Не менее 1 администратор и 15 операторов
Импорт/экспорт	Поддерживает импорт / экспорт с флэш-накопителя USB
Обновление системы	Поддерживается
Внешние интерфейсы	
USB	Не менее 4 шт USB 3.0 интерфейс Не менее 2 шт USB 2.0 интерфейс
Сеть	Не менее 2 шт 1000Mbps сетевой интерфейс
HDMI	Не менее 4 выхода
Общие	
Питание	Адаптер 12 V DC/4 A
Экран	10,1-дюймовое сенсорный экран

4.3.6.15. Видеodeкодер

Сетевой видеodeкодер - 1 шт	
Видеовход VGA и DVI-I	WSXGA: 1680×1050/60Гц WXGA: 1440×900/60Гц WXGA: 1280×800/60Гц, 1366×768/60Гц 1080p: 1920 × 1080@50/60Гц UXGA: 1600 × 1200@60Гц XVGA: 1280 × 960@60Гц 720p: 1280 × 720@50Hz/60Гц SXGA: 1280 × 1024@60Гц XGA: 1024 × 768@60Гц
Выход HDMI	Не менее 18 каналов 1080p: 1920 × 1080@50/60Гц WSXGA: 1680×1050/60Гц UXGA: 1600 × 1200@60Гц (только для четных интерфейсов) 720p: 1280 × 720@50Гц/60Гц SXGA: 1280 × 1024@60Гц XGA: 1024 × 768@60Гц
BNC выход	не менее 2 каналов, 2 DB 15
Разрешение	До 12 Мп
Каналы декодирования	Не менее 128 каналов
Синхронное воспроизведение	12MP@20к/с не менее 4 каналов 2MP@30к/с: не менее 16 каналов D1 @30к/с: не менее 64 каналов

Разделение экранов	1/4/9/16
Сетевой интерфейс	Не менее 1, RJ45 10М /100М/1000М управляемых сетевых интерфейса
Последовательный интерфейс	Не менее 1 RS-485 Не менее 1 RS-232
Тревожные вход/выход	Не менее 8/8
Двусторонний аудио вход	Не менее 1 канал, 3.5мм (2.0 Vp-p, 1 KΩ)
Двусторонний аудио выход	Не менее 1 канал, 3.5мм (2.0 Vp-p, 1 KΩ)
Аудио выход	Не менее 4 каналов, 2 DB 15
Питание	AC100-240В
Рабочие условия	от -10°C до +55°C, влажность 10% ~ 90%

4.3.6.16. Жесткий диск

Жесткий диск-72 шт	
Тип	HDD
Объем	Не менее - 7200 Гб
Объем буферной памяти	Не менее -256 Мб
Фактор формы	3,5"
Скорость передачи данных	Не менее -110 Мб/сек
Кэш	Не менее -64 Мб
Скорость вращения	(RPM) IntelliPower
Циклы загрузки / выгрузки	300
Рабочая температура	0°C ~ 65°C
Уровень шума	23 дБА

4.3.6.17. Оптическая распределительная панель

Оптическая распределительная панель (ODF) 1U-1шт	
Тип:	Оптическая патч панель (незагруженная)
Количество портов:	1-24
Массе (без полувиллок и розеток):	Не более 3 кг
Количество вводимых кабелей:	До 6 шт
Монтажные габариты:	19-дюймовые монтажные конструктивы

4.3.7. Требования к метрологическому обеспечению

При разработке и использовании системы специальные требования в метрологическом обеспечении отсутствуют.

При организации системы требуются стандартные измерительные приборы, не требующие поверок и сертификации.

4.3.8. Требования к организационному обеспечению

В состав системы должны входить программно-аппаратные средства обучения пользователей работе с системой.

Должны быть разработаны и представлены пользователю комплекты наглядных пособий, инструкций и/или плакатов для обучения и подготовки пользователей системы (контингент: оперативный состав, служба администрирования системы, сотрудники по установке и ремонту оборудования и др.)

Обучение пользователей работе с программными средствами, оказание методической помощи, а также авторский контроль, в течение одного года после ввода программно-аппаратных средств в эксплуатацию, за функционированием разработанного программного обеспечения осуществляется исполнителем.

4.3.9. Требования к методическому обеспечению

Методическое обеспечение Системы должно включать совокупность документов, описывающих технологию функционирования Системы, методы выбора и применения пользователями технологических приемов для получения конкретных результатов при функционировании Системы.

Используемые правовые документы при создании Системы:

1. Закон Республики Узбекистан «Об информатизации».
2. Закон Республики Узбекистан «О Телекоммуникациях».
3. Постановление Президента Республики Узбекистан от 21 марта 2012 года. № ПП-1730 «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий».
4. Постановление Президента Республики Узбекистан от 27 июня 2013 года №ПП-1989 «О мерах по дальнейшему развитию Национальной информационно-коммуникационной системы Республики Узбекистан».
5. Постановления Президента Республики Узбекистан «О мерах по дальнейшему совершенствованию системы профилактики правонарушений и борьбы с преступностью» № ПП-2833 от 14 марта 2017 года.
6. Положение о порядке создания информационных систем государственных органов (приложение №2 к Постановлению КМ Республики Узбекистан от 22.11.2005г. № 256).
7. Постановления Президента Республики Узбекистан «О мерах по совершенствованию порядка проведения экспертизы предпроектной, проектной, тендерной документации и контрактов» №3550 от 20 февраля 2018 года.
9. Закон Республики Узбекистан «О государственных закупках» от 22.04.2021 г. № ЗРУ-684.
10. Внутриведомственные нормативно-правовые документы, регламентирующие процесс работы, соответствующих служб Министерства внутренних дел Республики Узбекистан.

Работы по созданию системы должны выполняться в рамках реализации единой государственной политики в области разработки и осуществлении комплексных программ по внедрению и развитию национальной информационно-коммуникационной системы, развития информационных технологий инфраструктуры МВД РУ., защиты и использования информации.

Используемые нормативные документы при создании Системы:

- O'zDSt 1986:2018 - Информационная технология. Информационные системы. Стадии создания;

- O'zDSt 1987-2018 - Информационная технология. Техническое задание на создание информационной системы;

- O'zDSt ISO/IEC 14764:2008 - Разработка программного обеспечения. Процессы жизненного цикла программного обеспечения. Сопровождение программных средств;

- O'zDSt 1985:2018 - Государственный стандарт Узбекистана. Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем;

- O'zDSt 2864:2014 - Государственный стандарт Узбекистана. Информационная технология. Информационные системы. Межведомственная интеграционная платформа. Общие технические требования;

Документы и система должны разрабатываться с учетом стандартов на создание автоматизированных систем:

- O'zDSt 1047:2018. Информационная технология. Информационные системы. Термины и определения.

- O'zDSt ISO/IEC TR 9294:2007. Информационная технология. Руководство по управлению документированием программного обеспечения.

- O'zDSt ISO/IEC/IEEE 12207:2018. Информационная технология. Процессы жизненного цикла программного обеспечения.

- O'zDSt ISO/IEC 25051:2018. Разработка программного обеспечения. Требования к качеству и оценка систем и программного продукта (square). Требования к качеству готового к использованию программного продукта (rusp) и инструкции по тестированию.

- O'zDSt 1135:2007. Информационная технология. Требования к базам данных и обмену информацией между органами государственного управления и государственной власти на местах.

- O'zDSt 2590:2012. Информационная технология. Требования к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы.

- O'zDSt ISO/IEC 15408:2016. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий, части 1, 2, 3.

- O'zDSt ISO/IEC 27002:2016. Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
- ИКН 15-2009 УзАСИ - Инструкция по проектированию устройств заземления персональных компьютеров Конструкции зданий;
- ИКН 16-2009 УзАСИ - Инструкция по проектированию устройств заземления персональных компьютеров;
- ИКН 17-2010 УзАСИ - Ведомственные строительные нормы. Проектирование структурированных кабельных систем и локальных вычислительных сетей;
- ИКН 05-2013 Ведомственные строительные нормы. Правила приемки в эксплуатацию законченных строительством объектов телекоммуникаций. Основные положения;
- ГОСТ 2.102-68 - Единая система конструкторской документации. Виды и комплектность конструкторских документов;
- ГОСТ 2.113-75 - Единая система конструкторской документации. Групповые и базовые конструкторские документы;
- ГОСТ 19.101-77 - Единая система программной документации. Виды программ и программных продуктов;
- РН 45-169:2004 - Руководящий документ. Основные требования к организации межведомственной компьютерной сети;
- РН 45-004-2008 - Система стандартизации в сфере связи и информатизации. Порядок планирования, разработки, согласования, утверждения и регистрации нормативных документов;
- РН 45-062:2012 - Инструкция по оформлению проектно-сметной документации в сфере связи, информатизации и телекоммуникационных технологий;
- РН 45-128:2012 - Руководящий документ Требования к оформлению технических проектов информационных систем органов государственной власти и управления;
- РН 45-170:2004 - Руководящий документ. Основные технические требования по созданию локальных и корпоративных ведомственных компьютерных сетей;
- РН 45-201:2011 - Руководящий документ. Технические требования к зданиям и сооружениям для установки средств вычислительной техники.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС

Стадии и этапы, выполняемые организациями – участниками работ по созданию ИС описаны в п.1.5. настоящего ТЗ, в целом содержание работ должно соответствовать требованию настоящего ТЗ, а также устанавливается в договорах с подрядчиками.

В рамках внедрения Проекта должны быть выполнены следующие виды работ (см. таблицу):

№	Наименование работ и их содержание	Сроки выполнения		Исполнители	Чем заканчивается этап (результат)
		Начало	Окончание		
1	Разработка технического задания на закупку оборудования	Январь 2022 года	Март 2022 года	ГУВД г. Ташкент	Утвержденное ТЗ
2	Объявление тендера	Январь 2022 года	Февраль 2022 года	ГУВД г. Ташкент	Выбор победителя тендера
3	Поставка необходимых технических средств, оборудования и информационной системы	Март 2022 года	Март 2022 года	Поставщик оборудования	Поставка необходимых технических средств, согласно Договоров, с поставщиками
4	Монтажные, инсталляционные, пуско-наладочные работы.	Март 2022 года	Март 2022 года	Исполнитель	Оформление документации завершения (акты окончания работ, индивидуальных испытаний, ведомостей установленного оборудования, техно-рабочая документация)
5	Инструктаж пользователей для работы в период опытной эксплуатации. Период пробной эксплуатации.	Март 2022 года	Май 2022 года	Исполнитель, Заказчик	Доработка функционала системы с учетом представленных предложений и замечаний.
6	Подготовка плана обучения и материалов для проведения обучения для пользователей и администраторов системы	Март 2022 года	Май 2022 года	Исполнитель	Разработанная документация
7	Введение информационной системы в промышленную эксплуатацию	Март 2022 года	Май 2022 года	Исполнитель	Запуск системы

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС

В соответствии с ГОСТ 34.603-92 для ИС устанавливают следующие основные виды испытаний:

- 1) предварительные;
- 2) опытная эксплуатация;
- 3) приемочные (промышленная).

Предварительные испытания следует выполнять после проведения разработчиком отладки и тестирования поставляемых программных продуктов ЦДУ и представления им соответствующих документов об их готовности к испытаниям, а также после ознакомления персонала с ее эксплуатационной документацией.

Опытную эксплуатацию системы проводят с целью определения соответствия функции системы к предъявляемым требованиям.

Приемочные испытания системы проводят для определения ее соответствия техническому заданию, оценки качества опытной эксплуатации и решения вопроса о возможности приемки ее в постоянную эксплуатацию.

При испытаниях системы проверяют:

- 4) качество выполнения комплексом программных и технических средств автоматических функций во всех режимах функционирования Системы, согласно Техническому заданию;
- 5) знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования системы, согласно Техническому заданию;
- 6) полноту содержащихся в эксплуатационной документации указаний персоналу по выполнению им функций во всех режимах функционирования системы, согласно Техническому заданию;
- 7) количественные и (или) качественные характеристики выполнения автоматических и автоматизированных функций системы в соответствии с Техническим заданием;
- 8) другие свойства системы, которым она должна соответствовать по Техническому заданию.

Критерии оценки достижения целей создания системы определяются функциональными возможностями системы, реализованных в рамках настоящего проекта.

Виды, состав, объем, методы испытаний и порядок приемки

В соответствии с O'z DSt 1986:2010 для Системы предусматриваются следующие виды проверок и испытаний:

- 1) предварительные испытания;
- 2) опытная эксплуатация;
- 3) приемочные испытания.

ИС должна быть подвергнута предварительным испытаниям в соответствии с «Программой и методикой испытаний». По положительным результатам предварительных испытаний она должна быть введена в опытную эксплуатацию. Опытная эксплуатация Системы должна осуществляться персоналом Заказчика из числа лиц, прошедших обучение по программе Исполнителя и проводиться в соответствии с программой и графиком (при необходимости) опытной эксплуатации. Продолжительность опытной эксплуатации должна быть не менее 15 и не более 45 рабочих дней. Оценка результатов опытной эксплуатации должна быть отражена в протоколе по результатам опытной эксплуатации.

По окончании «Опытной эксплуатации» на этапе ввода в промышленную эксплуатацию ИС должна быть подвергнута приемочным испытаниям в соответствии с «Программой и методикой испытаний». По результатам приемочных испытаний Система должна быть введена в эксплуатацию. Проверке на испытаниях должны быть подвергнуты:

комплекс программных средств ИС;

состав эксплуатационной документации, регламентирующей деятельность персонала при функционировании ИС;

степень ознакомления персонала с эксплуатационной документацией и его подготовленность к проведению опытной эксплуатации ИС.

При испытаниях комплекса программных средств ИС должны быть проверены: полнота соответствия подсистем входящим в систему функциональным требованиям соответствующих им частным техническим заданиям (ЧТЗ), с учетом изменений, документально оформленных в установленном порядке и утвержденных на момент испытаний;

выполнение комплексом программных средств автоматизированных функций в режимах функционирования ИС согласно функциональным требованиям на создание ИС.

При проверке эксплуатационной документации, регламентирующей деятельность персонала при функционировании ИС, должны быть проверены:

соответствие состава эксплуатационной документации требованиям настоящего Технического задания;

знание персоналом состава эксплуатационной документации и наличие у него навыков, необходимых для выполнения функций ИС согласно Техническому заданию на создание ИС;

полнота содержащихся в эксплуатационной документации указаний персоналу по выполнению им предписанных действий при работе с ИС, в рамках требований Технического задания на создание ИС.

Результаты проведения предварительных испытаний, опытной эксплуатации и приемочных испытаний должны быть зафиксированы в актах предварительных испытаний, опытной эксплуатации и приемочных испытаний соответственно.

При положительных результатах опытной эксплуатации и отсутствии в процессе ее проведения отклонений или их нефункциональном характере допускается не проводить приемочные испытания или проводить их в сокращенном объеме по выборочным параметрам на усмотрение экспертов Исполнителя и Заказчика. Положительные результаты испытаний, зафиксированные этими актами, являются основанием для подписания актов сдачи-приемки работ соответствующего этапа создания ИС.

Условия проведения испытаний

Общие требования к приемке работ по результатам предварительных испытаний, состав предприятий и организаций, участвующих в проведении приемки работ, а также сроки и место проведения приемки работ должны определяться Исполнителем работ по созданию ИС практика, согласовываться с Заказчиком и излагаться в «Программе и методике испытаний» и текущих оперативных организационно-распорядительных документах.

Общие требования к приемке работ в ходе и по результатам опытной эксплуатации, состав предприятий и организаций, участвующих в проведении приемки работ, а также сроки и место проведения приемки работ должны определяться Заказчиком, по представлению и согласовываться с Исполнителем работ по созданию Системы и отражаться в «Программе и методике предварительных испытаний».

В соответствии с О‘zDSt 1986:2010 испытания следует проводить на объекте Заказчика. По согласованию между Заказчиком и Исполнителем предварительные испытания и приемку программных средств допускается проводить на территории и технических средствах разработчика при создании условий получения достоверных результатов испытаний

В случае неготовности оборудования объекта (телекоммуникации, ЛВС, сервер, компьютеры) к началу проведения испытаний и контроля проведение всех стадий испытаний, контроля и приемки системы должны осуществляться на стенде, создаваемом Заказчиком и Исполнителем с использованием оборудования объекта или временно выделяемым Исполнителем. В составе стенда допускается использование одного компьютера (рабочей станции) с достаточным (более 1 Гб) объемом памяти и свободным дисковым пространством 40 Гб в качестве сервера, 2-х рабочих станций, временной ЛВС. В случае отсутствия на объекте Заказчика на момент проведения испытаний лицензионного базового программного обеспечения испытания должны проводиться с использованием испытательных версий программного обеспечения с ограниченным сроком лицензий, свободно распространяемого для проб и испытаний. Совокупная продолжительность всех видов испытаний в этом случае должна устанавливаться с учетом срока действия лицензии на такое программное обеспечение.

Данные, полученные при таких испытаниях, признаются объективными и достаточными для принятия решения по всем вопросам контроля и приемки Системы.

Порядок создания, состав и статус приемочной комиссии

Прием проводимых работ осуществляется комиссией Заказчика с обязательным участием Исполнителя работ по созданию ИС. Приемочная комиссия по приемке ИС создается Заказчиком. Руководителем приемочной комиссии назначается представитель Заказчика.

Допускается создание приемочной комиссии по приемке ИС руководством объекта внедрения. Руководителем приемочной комиссии при этом назначается руководитель (представитель) объекта внедрения.

В приемочную комиссию в обязательном порядке включается представитель Исполнителя и Заказчика.

Статус приемочной комиссии – ведомственная.

По результатам своей работы Приемочная комиссия оформляет Акт приемки работ, который подписывается всеми членами Приемочной комиссии и представляется на утверждение Заказчику.

Организационно-распорядительные документы:

- 1) акт завершения работ;
- 2) акт приемки в опытную эксплуатацию;
- 3) акт приемки в промышленную эксплуатацию;
- 4) план-график работ;
- 5) приказ о составе приемочной комиссии;
- 6) приказ о проведении работ;
- 7) программа работ;
- 8) протокол испытаний;
- 9) протокол согласования.

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

Перечень основных мероприятий и их исполнителей, которые следует выполнить при вводе ИС для ситуационного центра в действие:

- 1) приведение поступающей в систему информации к виду, пригодному для обработки с помощью ЭВМ;
- 2) проведение всех строительных и ремонтных работ;
- 3) создание условий функционирования объекта автоматизации, при которых гарантируется соответствие создаваемой системы требованиям;
- 4) определение сроков и порядка комплектования штатов и обучения персонала. Обучение специалистов Заказчика должно проводиться по следующим направлениям:

- 1) специалистов по сопровождению технических и общесистемных программных средств;
- 2) сотрудников, использующих систему в своей повседневной деятельности.

В ходе выполнения проекта на объекте информатизации требуется выполнить работы по подготовке к вводу системы в действие. При подготовке к вводу в эксплуатацию ИС заказчик должен обеспечить выполнение следующих работ:

- определить подразделение и ответственных должностных лиц, ответственных за внедрение и проведение опытной эксплуатации ИС;
- обеспечить присутствие пользователей на обучении работе с ИС, проводимом разработчиком;
- обеспечить соответствие помещений и рабочих мест пользователей в соответствии с требованиями ТЗ;
- обеспечить выполнение требований, предъявляемых к программно-техническим средствам, на которых должно быть установлено программное обеспечение ИС;
- совместно с разработчиком подготовить план установки ИС на технических средствах заказчика;
- провести опытную эксплуатацию ИС.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Комплектность, построение и оформление технической документации на оборудование ИС для ситуационного центра должно быть достаточным для понимания принципов работы, как составных частей, так и в целом ИС, а также для её настройки и обслуживания.

В соответствии с О`z DSt 1985:2018 в состав программной и эксплуатационной документации должны быть включены:

Спецификация;

Описание программы;

Инструкция по установке системы;

Руководство пользователя;

Руководство администратора;

Технологические инструкции взаимодействия со сторонними ИС.

Все документы должны, переданы в электронной форме и в случае необходимости предоставлены на бумажном носителе.

Для проведения тестовых испытаний со стороны исполнителя должна быть предоставлена - Программа и методика испытаний.

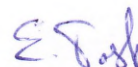
Подготовка указанных документов должна вестись и согласовываться с Заказчиком.

**Ведущий специалист информационных технологий,
связи и защиты информации ГУВД г.Ташкента**



А.Ч.Кадиров

**Главный специалист информационных технологий,
связи и защиты информации ГУВД г.Ташкента**



Е.Б.Ташманов

**Главный специалист отдела информационных технологий,
связи и защиты информации ГУВД г.Ташкента**



Д.В.Усманов