«УТВЕРЖДАЮ»

_____

_____

Организация

_____

Подпись ФИО

«___ » _____ 20___г.

Требования Заказчика
на внешнюю разработку и внедрение ИС Единая Система противопожарной защиты АВК (Рубеж)

Версия 1.00

Дата 13.03.2024

Оглавление

Часть	Цвет MS Word	Комментарии
Внешняя разработка СУБД		

1. Введение.

ИС Система противопожарной защиты АВК предназначена для централизованного мониторинга из ОСС пожарной безопасности здания АВК сегмента первой очереди.

В рамках реконструкции АВК возникла необходимость в оснащении новых зон системами пожарной безопасности. При этом масштабирование текущей системы, построенной на платформе EBI от Honeywell невозможна.

В рамках проекта для новых зон внедряется система пожарной безопасности на платформе Global Рубеж.

Далее будет разработан план миграции системы пожарной безопасности АВК на платформу Global.

2. Термины.

АРМ – Автоматизированное рабочее место;

АПК – Аэропортовый комплекс;

СПЗ – Система противопожарной защиты;

1С АСУ ОСП – 1С: Автоматизированная система управления обслуживанием средств производства (АСУ ОСП);

СЦ – Ситуационный центр;

ССОИ – Система сбора обработки и отображения информации;

ИС – Информационная система.

3. Назначение и цели разработки ИС.

3.1. Назначение ИС.

ИС необходима для осуществления непрерывного мониторинга состояния пожарной безопасности объектов.

3.2. Цели разработки ИС.

- Развертывание верхнего уровня системы противопожарной защит на базе ПО Global Monitor

4. Требования к ИС.

4.1. Бизнес требования.

4.1.1. Описание бизнес процесса.

Диспетчер осуществляет мониторинг состояния противопожарной безопасности, а также состояние готовности оборудования противопожарных инженерных систем. При формировании сигнала класса Alarm и Warning и попадании сигнала отказа в журнал событий при отказе оборудования противопожарных инженерных систем, диспетчер осуществляет квитирование сигнала и первичную диагностику неполадки и определяет причину отклонения параметров работы оборудования инженерной системы от нормы.

При получении и подтверждении сигнала «Пожар» Диспетчер действует согласно действующему описанию процесса Противопожарное обеспечение объектов ПК.

4.1.2. Описание АРМов.

АРМ	Возможности	Количество
АРМ «Администратор»	Предоставляет возможность чтения и редактирования всех документов ИС, доступ ко всем интерфейсных элементам ИС, доступ к настройкам ИС, доступ на администрирование ИС.	***2***
АРМ «Суперчитатель»	Предоставляет доступ на чтение всех документов	***2***
АРМ «Управление справочниками»	Предоставляет возможность чтения и редактирования всех справочников в ИС.	***1***
АРМ «Разработчик мнемосхем»	Предоставляет возможность формирования, редактирования визуальных представлений (мнемосхем) работы технологического оборудования.	***2***
АРМ «Диспетчер пожарной безопасности»	По всем объектам: - Контроль параметров работы противопожарных систем. - Получение сигналов и отчетов обо всех критических событиях/авариях противопожарных систем, регистрируемых ИС - Ведение электронного журнала возникновения неисправностей на оборудовании противопожарных систем. - Информация о режимах работы основных агрегатов противопожарных систем - Информация о текущих режимах автоматического управления противопожарных систем объекта/группы объектов	***2***

	- Переключение режимов автоматического управления противопожарных систем объекта/группы объектов - Формирование отчетов - Квитирование ALARM и WARNING по любому объекту - Переход по ALARM и WARNING на соответствующий экран объекта	

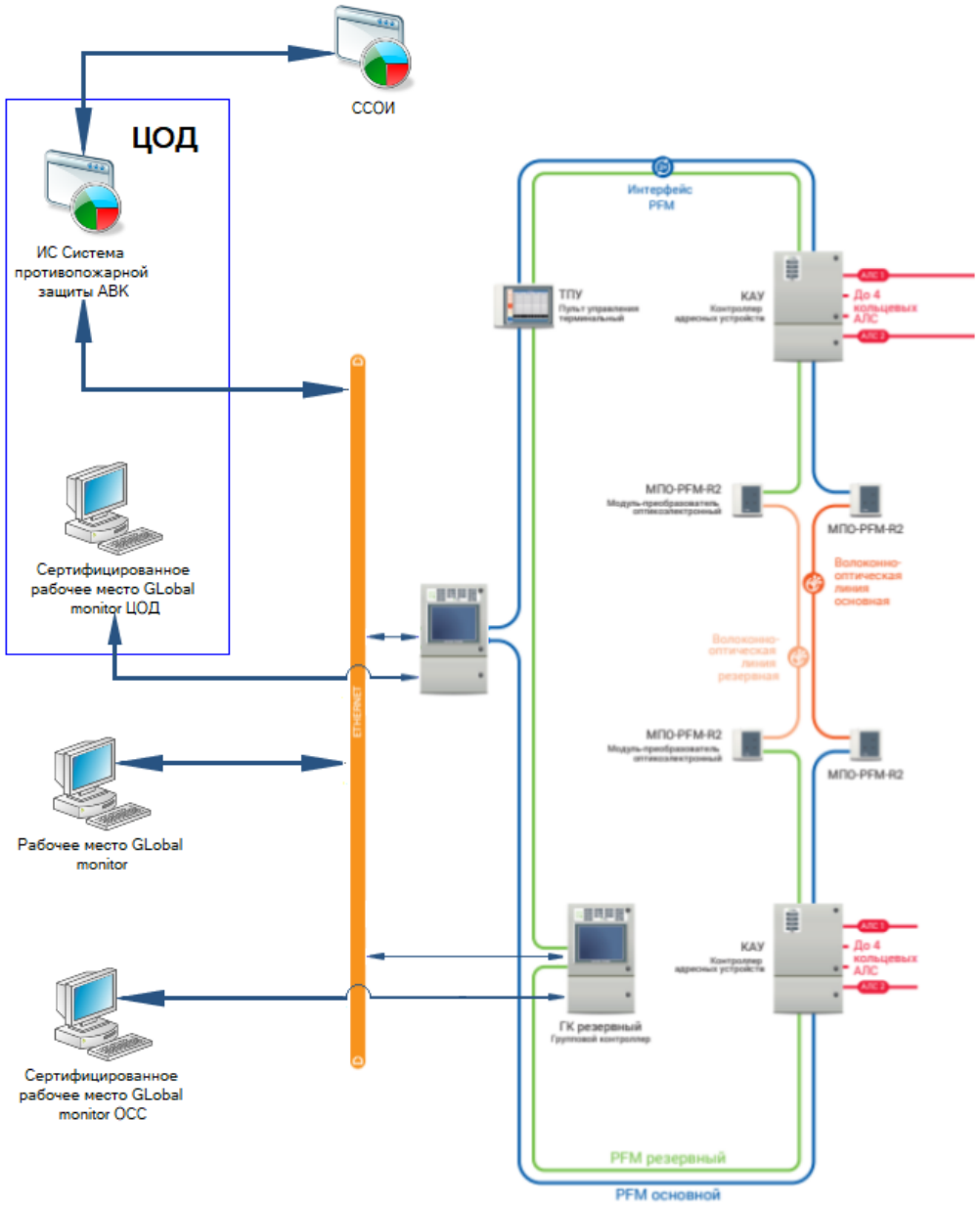
4.1.3. Описание структуры данных ИС.

Система противопожарной защиты представляет собой набор адресных приборов и устройств, предназначенных для создания централизованной адресно-аналоговой пожарной сигнализации, системы управления оповещением, противодымной вентиляции, пожаротушения, а также инженерным оборудованием. Логика работы как отдельных элементов, так и всей системы в целом является гибко программируемой. Кроме этого, все адресные устройства и приборы системы имеют возможность настройки целого ряда параметров для выполнения тех или иных функций. Главным управляющим прибором является групповой контроллер (ГК), который объединяет всю систему в единое целое. Он содержит в себе информацию обо всех устройствах, логиках и режимах их работы, обеспечивает связь компонентов системы, обрабатывает происходящие события и принимает решения о необходимых действиях согласно запрограммированной логике. С группового контроллера также производится настройка параметров всех адресных устройств. В зависимости от исполнения, ГК имеет десяти дюймовый сенсорный дисплей, на котором отображается состояние всей системы, а также производится ручное управление любым устройством системы. В качестве верхнего уровня используется ИС Система противопожарной защиты на базе ПО «GLOBAL Монитор». Связь с групповым контроллером осуществляется через интерфейс Ethernet без преобразователей. С помощью ИС производится первоначальное конфигурирование системы, создается база данных всей системы, закладываются алгоритмы управления устройствами, а также производится запись созданной базы в групповой контроллер. Кроме первоначальной настройки, важной функцией ИС является мониторинг системы – визуальное отображение на планировках объекта состояния зон, направлений и устройств в режиме реального времени с оповещением оператора.

Для прямого управления любым исполнительным устройством системы, в том числе и дымоудалением и пожаротушением используется сертифицированное рабочее место Global monitor (ЦПИУ «Рубеж-АРМ исп.3) представляющий собой промышленный компьютер, имеющий сертификат соответствия ТР ЕАЭС 043/2014.

В рамках данного проекта внедряется ИС Система противопожарной защиты, закупается Сертифицированное рабочее место.

На верхнем уровне ИС Система противопожарной защиты АВК в рамках отдельного проекта будет интегрироваться в ИС ССОИ на базе R-Платформа, которая позволит интегрировать ИС СПЗ АВК с ИС 1С АСУ ОСП и ИС СЦ.


ССОИ
ЦОД
ИС Система противопожарной защиты АВК
Сертифицированное рабочее место GLobal monitor ЦОД
Рабочее место GLobal monitor
Сертифицированное рабочее место GLobal monitor ОСС
ETHERNET
Интерфейс PFM
ТПУ
КАУ
До 4 кольцевых АЛС
МПО-PFM-R2
МПО-PFM-R2
Волоконно-оптическая линия основная
Волоконно-оптическая линия резервная
МПО-PFM-R2
МПО-PFM-R2
КАУ
До 4 кольцевых АЛС
ГК резервный
PFM резервный
PFM основной

4.1.4. Требования к характеристикам взаимосвязей разрабатываемой ИС с эксплуатируемыми / внедряемыми ИС.

Не предъявляются.

Интеграция с ИС ССОИ будет осуществляться отдельным проектом после ввода ИС ССОИ в опытную эксплуатацию.

Интеграция будет осуществляться с помощью API, которое предоставит контрагент: 

.

4.2. Функциональные требования.

4.2.1. Требования к функциям, выполняемым ИС.

- получение в реальном времени текущих параметров работы противопожарных систем объектов;
- агрегация данных в серверах и отображение данных на соответствующих мнемосхемах;
- получении событий (ALARM, WARNING) и оповещение Диспетчера;
- генерация собственных событий (ALARM, WARNING) по заложенным правилам и оповещение Диспетчера;
- оповещение об отказах элементов системы управления (диагностика линий связи, контролеров, шлюзов, серверов объектовых систем и т.п.);
- формирование исторического массива исходных данных для проведения плановых предупредительных работ с основным оборудованием;
- мониторинг режимов работы оборудования противопожарных систем;
- ведение краткосрочных и долгосрочных архивов данных;
- экспорт текущих значений Точек I/O, исторических значений Точек I/O и событий ALARM/WARNING во внешние системы;
- оповещение об отказах оборудования инженерных систем.

4.2.2. Требования к программному обеспечению.

Программное обеспечение должно соответствовать СП484.1311500.2020.

4.2.3. Требования по техническому обеспечению.

Необходимо закупить ЦПИУ «Рубеж-АРМ исп.3 – 2 шт.

Требование к серверному оборудованию:

- ЦП: 4 потока 2.8 ГГц;
- Оперативная память: 16 Гб;
- Хранилище приложений и баз данных: 50 Гб;
- Хранилище системное: 50 Гб;
- Сетевой интерфейс – 100 Mb/s и выше.

4.2.4. Требования к техническим характеристикам.

- *Максимальное количество рабочих мест (пользователей) на момент внедрения - 5*
- *Ожидаемый годовой прирост количества рабочих мест (пользователей) – 0%*
- *Планируемый объем основных объектов данных (документов и др.) в первый год эксплуатации от максимально-возможного (требуемого) объема (%) – 20%*
- *Предполагаемый ежегодный прирост объема объектов данных от максимально-возможного (требуемого) объема (%) – 20%*
- *Предполагаемое среднесуточное количество обрабатываемых объектов данных на одно рабочее место (пользователя) - 1000;*
- *Доступность: 7дн / 24 час;*

4.2.5. Требования к надежности.

Для каждого возможного вида аварийной ситуации, должны быть сформированы инструкции для пользователя и администратора, которые должны быть доступны в Руководстве пользователя ИС, Руководстве администратора ИС.

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

- при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке ОС, восстановление программы должно происходить после перезапуска ОС, запуска исполняемых файлов и служб Системы;
- при ошибках в работе аппаратных средств (кроме носителей данных и программ) восстановление функции системы возлагается на ОС;
- при ошибках, связанных с программным обеспечением (ОС и драйверы устройств), восстановление работоспособности возлагается на ОС.

4.2.6. Требования к информационной безопасности.

Максимальный уровень конфиденциальности данных, хранимых, обрабатываемых и передаваемых в ИС - 5.

Сеть передачи данных комплекса программно аппаратных средств должна быть изолирована от других сегментов на логическом или физическом уровне.

1. Общие требования.

1.1. Ни одно действие в рамках IT-решения не происходит без участия подсистемы безопасности.

2. Требования к аутентификации и учетным записям.

2.1. При получении запроса на доступ к объекту, подсистема безопасности требует от субъекта идентифицировать себя, проводит процедуру аутентификации и выполняет процедуру авторизации с использованием параметров хранящихся в таблицах управления доступом. Субъекты имеют доступ только к разрешенным объектам системы.

2.2. Учетные записи IT-решения персонализированны (ставятся в однозначное соответствие конечному пользователю IT-решения). Допускается использование неперсонализированных учетных записей при условии выполнения ими служебных функций (регламентные задания, интеграция со смежными IT-решениями, автоматизированные выгрузки и т.п.).

2.3. Создание и удаление учетных записей субъектов доступа доступно только администратору IT-решения.

2.4. Учетные записи IT-решения соответствуют требованиям Стандарта "на продукт Выполненные требования корпоративных норм информационной безопасности (требования ИБ, предъявляемые к паролям учетных записей пользователей)"

2.5. В части обеспечения управления жизненным циклом учетных записей путем автоматической обработки запросов на создание, удаление, блокировку, разблокировку учетной записи, предусмотрена интеграция с ИС "Управление доступом". Использование IT-решением учетных записей Active Directory является одним из возможных вариантов интеграции данного IT-решения с ИС "Управление Доступом".

2.6. Для информационных систем не поддерживающих сквозную аутентификацию с использованием учетной записи AD должен быть создан шаблон приложения в ИС "Single Sing-On".

2.7. В документах, инициирующих разработку/модернизацию описаны требования, а в проектной/эксплуатационной документации реализация интеграционных механизмов, их структура и цели, которые должны быть достигнуты.

2.8. Информация о служебных и пользовательских учетных записях (логин, пароль) в файлах конфигурации, настроечных файлах, полях БД, реестре и т.п., как на клиентских, так и на серверных компонентах IT-решения храниться в зашифрованном виде.

3. Требования к авторизации и разграничению прав доступа.

3.1. Основная модель разграничения доступа - дискреционная. Для каждой тройки субъект – объект - состояние объекта (в соответствии с жизненным циклом объекта в IT-решении) есть возможность задать явное и недвусмысленное перечисление допустимых типов доступа, при этом суммарные права проверяются на непротиворечивость, а также применяется принцип поглощения более широкими разрешительными правами более узких и принцип преимущества запретительных прав над разрешительными (при наличии запретительных прав). При

использовании интерфейсов, отличных от типовых, права доступа к объектам IT-решения не отличаются от предоставляемых на основе типовых интерфейсов.

3.2. Подсистема безопасности IT-решения обеспечивает следующий минимальный перечень уровней доступа:

- нет доступа к объекту;

- доступ к объекту только на чтение;

- доступ к объекту только на создание/изменение;

- удаление информационного объекта;

- изменение прав доступа субъектов к объекту;

3.3. Существует один выделенный субъект - администратор, имеющий полномочия устанавливать права доступа для всех остальных субъектов IT-решения. Требование не распространяется на случаи, когда в IT-решении автоматизируются процедуры предоставления доступа ко вновь создаваемым информационным объектам пользователями уже являющихся субъектами доступа этих IT-решений и имеющими доступ к родительским объектам доступа (например, доступ к комментарию в ИС "Согласование" определяется пользователем).

3.4. Организация предоставления/лишения доступа к группам/ролям IT-решения:

- IT-решение интегрировано с ИС "Управление Доступом" в части обеспечения автоматической обработки Заявок на изменение доступа (предоставление доступа, лишение доступа).

- Использование IT-решением групп безопасности MS Active Directory является одним из возможных вариантов интеграции данного IT-решения с ИС "Управление Доступом".

3.5. Предусмотрена возможность предоставления доступа к информационным объектам, содержащим конфиденциальную информацию, через группы / роли. При включении субъекта в группу, он получает доступ к информационным объектам, назначенным для группы. Предоставление доступа к информационным объектам через учетные записи субъектов доступа допускается только при наличии в IT-решении механизма лишения доступа субъекта ко всем объектам, а также механизма передачи прав доступа одного субъекта другому.

3.6. Разграничение прав доступа к персональным данным:

- Персональные данные сотрудников DME, а именно, личные контактные данные (телефон, электронная почта), должны быть выделены в отдельный бизнес объект. Доступ к данному бизнес объекту предоставляется через отдельную роль/группу/АРМ.

- Системой владельцем указанных персональных данных является только ИС Кадры. Информационный обмен личными контактными данными между IT-системами запрещен. Допускается размещение ссылки на личные контактные данные из системы владельца.

3.7. В IT-решении предусмотрен доступ Суперпользователя в соответствии с требованиями п.2.7 Стандарта на продукт Учтённый\актуальный объект информационного доступа (Перечень обязательных ресурсов/АРМ учтённых объектов информационного доступа).

4. Требования к криптографической защите информации.

4.1. В IT-решении обеспечивается криптографическая защита конфиденциальной информации от несанкционированного изменения и доступа при организации хранения сведений конфиденциального характера, относящихся к 1-й, 2-й и 3-й категории конфиденциальности в соответствии со Стандартом на средства защиты информации от несанкционированного доступа.

4.2. Для защиты сведений конфиденциального характера от несанкционированного доступа при её хранении и передаче по каналам связи, относящихся к 1-й, 2-й и 3-й категории конфиденциальности, по требованию владельца или Сотрудников ГИБ дополнительно используется асимметричная система криптографической защиты, где владельцем секретного ключа асимметричной пары является субъект доступа.

4.3. В IT-решении обеспечена криптографическая защита информации, относящейся к сведениям 1-й и 2-й категории конфиденциальности от несанкционированного изменения и доступа при ее передаче по каналам связи в пределах КИС (как между модулями системы (серверами), так и между терминалами пользователей и серверами).

4.4. В IT-решении обеспечена криптографическая защита информации, относящейся к сведениям 1-й, 2-й, 3-й и 4-й категории конфиденциальности от несанкционированного изменения и доступа при ее передаче по каналам связи за пределы КИС (как между модулями системы (серверами), так и между терминалами пользователей и серверами).

4.5. Длина симметричных (сессионных) ключей, используемых для криптографической защиты информации, не менее 128 бит.

4.6. Длина асимметричных ключей, используемых при криптографической защите информации, не менее 1024 бит.

4.7. Ключи, используемые для криптографической защиты информации и находящиеся в открытом состоянии, размещаются только в защищенных сегментах оперативной памяти, исключающих доступ к ним программных модулей, не входящих в подсистему безопасности.

5. Требования к целостности информации.

5.1. IT-решение поддерживает логическую целостность информации. В случае поддержки платформой транзакционно-ориентированного механизма, изменения носят характер транзакционно-ориентированных, выполняющихся в целом от начала до конца либо, в случае сбоя, не выполняющихся совсем.

5.2. Модификация и уничтожение системных файлов, модулей и информации недоступна для пользователей, не имеющих административных прав в IT-решении.

6. Требования к доступности информации.

6.1. С целью обеспечения устойчивой работы IT-решения при отказе оборудования, предусмотрена возможность организации кластера из нескольких географически распределенных вычислительных узлов. Некритическое количество узлов, выход из строя которых не сказывается на общей функциональности IT-решения, больше одного.

6.2. Вывод из строя рабочего места пользователя не сказывается на работе серверной части IT-решения.

6.3. Обеспечена возможность резервного копирования и восстановления информации без нарушения конфиденциальности и целостности, а также доступности сервисов, предоставляемых IT-решением пользователям. При восстановлении IT-решения из резервной копии, обеспечивается полное восстановление средств защиты информации.

7. Требования к регистрации и отображению событий в IT-решении.

7.1. Регистрации и отображению подлежат все события всех субъектов действия информационной системы, в том числе и администратора информационной системы.

7.2. Запись журнала аудита содержит следующую информацию:

- тип события;

- время возникновения события;

- субъект действия (учетная запись / идентификатор терминала);

- объект действия (в том числе и местоположение объекта);

- результат произведенного действия.

7.3. Система аудита позволяет осуществлять регистрацию следующих типов событий:

– регистрация входа в систему (идентификатор субъекта / терминала);
– создание информационного объекта;
– чтение объекта (для объектов, содержащих информацию, относящуюся ко 2-ой и выше категории конфиденциальности, а также по требованию владельца или Сотрудников службы информационной безопасности);
– изменение объекта;
– удаление объекта;
– изменение состава групп / ролей;
– изменение списка прав доступа объекта;
– запуск процедуры / функции, если он инициируется пользователем вручную;
– создание / удаление / изменение / активация / деактивация учетной записи;
– изменение конфигурационных настроек системы.

7.4. Журнал аудита обладает защитой от изменений со стороны любого субъекта, кроме процесса его формирования и администратора IT-решения, а также защитой от остановки IT-решения при переполнении журнала.

7.5. IT-решение имеет механизм передачи в удаленное хранилище системных событий, событий аудита.

7.6. IT-решение обеспечивает возможности мониторинга работы системы/ пользователей, включая:

- отображение текущих сессий пользователей в системе;

- диагностирование и отображение состояния каждого элемента системы;

- возможность генерации, регистрации в журналах событий и отправки сообщения при любом изменении состояния контролируемого параметра системы.

8. Требования к физическому размещению серверного оборудования и оборудования хранения данных.

8.1. Серверное оборудование и оборудование хранения данных размещается в ЦОД.

4.3. Нефункциональные требования.

4.3.1. Требования к пользовательскому интерфейсу.

Требования к внешнему виду ИС не предъявляются.

5. Требования к эксплуатационной документации.

- Руководство пользователя ИС - описание функциональности ИС, доступной пользователю (не требуется для Web-приложений и ИС, не взаимодействующих с пользователем в интерактивном режиме), разработанное в соответствии со Стандартом на форму Руководства пользователя IT системы.
- Руководство администратора ИС - описание стандартных процедур инсталляции и администрирования ИС, а также настраиваемых элементов, разработанное в соответствии со Стандартом на форму Руководства/ инструкции администратора IT системы.
- Инструкция администратора ИС - описание специфических настроек ИС и АРМ для работы с ней, разработанное в соответствии со Стандартом на форму Руководства/ инструкции администратора IT системы >

II. Руководство пользователя ИС должно содержать разделы:

1. "Введение", в котором указывается:
   - Область применения и назначение ИС (виды деятельности и функции, для автоматизации которых предназначена ИС);
   - Краткое описание возможностей ИС;
   - Рекомендуемый уровень подготовки пользователя ИС;
   - Используемые в документе термины и сокращения.
2. "Описание операций", в котором указывается:
   - Описание всех выполняемых функций, задач, комплексов задач, процедур;
   - Описание операций, необходимых для выполнения функций, задач, комплексов задач, процедур. При описании каждой операции указывается:
     - Наименование операции;
     - Условия, при соблюдении которых возможно выполнение операции;
     - Подготовительные действия;
     - Основные действия в требуемой последовательности;
     - Заключительные действия;
     - Ресурсы, расходуемые на операцию.

3. "Рекомендации по освоению" (включается при необходимости), в котором указываются рекомендации по освоению и эксплуатации ИС, включая описание контрольного примера, правила его запуска и выполнения.

4. "Рекомендации по устранению проблем использования" (включается при необходимости), в котором приводятся описания возможных проблем использования ИС и рекомендуемые действия по их устранению.

III. Руководство администратора ИС должно содержать разделы (допускается включать дополнительные разделы и/или объединять указанные разделы вместе):

1. "Введение", в котором указывается:

- Область применения и назначение ИС;
- Краткое описание возможностей ИС;
- Используемые в документе термины и сокращения.

2. "Состав и требования к ИС", в котором указывается:

- Перечень и назначение составных частей (модулей) ИС;
- Системные требования (к аппаратному и программному обеспечению рабочей станции, сервера / кластера серверов, на который устанавливаются части ИС), а также рекомендации по архитектуре / топологии технических средств и ее масштабированию;
- Общие требования и рекомендации по запуску ИС.

3. "Установка и настройка", в котором указывается:

- Описание рекомендуемых конфигураций (архитектур) ИС;
- Поэтапное, внутри каждого этапа - пошаговое, описание процедуры установки каждой части (модуля) ИС для каждой из рекомендуемых конфигураций;
- Описание выполняемых настроек каждой части (модуля) ИС (при необходимости приводится пошаговое описание той или иной настройки);
- Описание процедуры запуска ИС (частей ИС).

4. "Управление и доступ", в котором приводится описание всех доступных способов и средств управления ИС, включая:

- Перечень и описание способов управления с помощью стандартных средств администрирования;
- Перечень и описание команд управления и/или встроенных средств управления ИС;
- Перечень и описание типовых / стандартных (используемых по умолчанию) автоматизированных рабочих мест (АРМ) ИС;
- Описание действий по предоставлению доступа (в том числе настроек для получения доступа) к АРМ.

5. "Резервное копирование и восстановление", в котором указывается:

- Требования и рекомендации по резервному копированию ИС (ПО и данных);
- Подробное описание процедуры восстановления ИС (ПО и данных) из резервной копии;
- Описания возможных сбоев и аварийных ситуаций, возникающих в работе ИС, и рекомендуемые действия по их устранению.

6. "Обновление и удаление", в котором указывается:

- Поэтапное, внутри каждого этапа – пошаговое, описание процедуры обновления каждой части (модуля) ИС;
- Подробное описание процедуры удаления ИС (частей ИС).

7. "Приложения", в котором указываются (в виде отдельных приложений):

- Коды ошибок, выдаваемых ИС в сбойных ситуациях;
- Используемые порты, ключи, серийные номера и т.п.;
- Другая вспомогательная информация по администрированию ИС (например, по диагностированию сбоев и ошибок).

IV. Инструкция администратора ИС должна содержать разделы (допускается включать дополнительные разделы и/или объединять указанные разделы вместе):

1. "Структура", в котором указывается:

- Описание используемой (требуемой) конфигурации / архитектуры ИС;
- Описание (схема) используемой (требуемой) архитектуры / топологии технических средств (аппаратной части) ИС с указанием используемых IP-адресов, имен серверов и т.д.

2. "АРМ", в котором указывается:

- Перечень и описание используемых (в соответствии с ИС "Управление доступом") АРМ;
- Описание принципов формирования новых АРМ.

3. "Резервное копирование", в котором указывается порядок выполнения резервного копирования, в том числе:

- Периодичность резервного копирования;
- Особые требования по резервному копированию (например, параметры библиотеки резервных копий).

4. "Прочее", в котором указываются прочие особенности администрирования ИС, соблюдение которых является необходимым условием ее корректного использования, например:

- Правила присвоения имен учетным записям и группам пользователей;

- Ограничения по масштабированию и т.п.

6. Основные требования к Контрагенту.

Контрагенты должны иметь статус Дистрибьютора Эксперта компании Рубеж.

7. Требования к составу и содержанию работ по разработке ИС

Состав и содержание работ определяется согласно утвержденному План-графику.