СОГЛАСОВАНО

Директор

ФГБУЗ Центр крови ФМБА России

_____

УТВЕРЖДЕНО

Начальник Департамента здраво-

Охранения Ивановской области

_____

М.А. Ратманов

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

НА ЗАКУПКУ КОМПЬЮТЕРНОГО И СЕТЕВОГО ОБОРУДОВАНИЯ С ЛИЦЕНЗИОННЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ДЛЯ СОЗДАНИЯ ЕДИНОЙ ИНФОРМАЦИОННОЙ БАЗЫ ДАННЫХ В ЦЕЛЯХ РЕАЛИЗАЦИИ МЕРОПРИЯТИЙ, СВЯЗАННЫХ С ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ ДОНОРСКОЙ КРОВИ И ЕЕ КОМПОНЕНТОВ, И ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ЭТОЙ БАЗЫ

Иваново
2014

Оглавление

Введение 5
Перечень принятых сокращений 6
1. Общие требования к условиям поставки 7
1.1. Условия поставки 7
1.2. Место поставки 7
1.3. Комплектация оборудования 7
1.4. Условия эксплуатации 7
1.5. Требования к документации 8
1.6. Требования к протоколированию выполненных работ 8
1.7. Требования к надежности 9
1.8. Требования к ремонту, техническому и гарантийному обслуживанию 10
1.9. Поддержка эксплуатации 10
1.10. Требования к закупаемому оборудованию 11
1.11. Требования к закупаемым лицензионным операционным системам и программам общего назначения 11
1.12. Требования к совместимости оборудования и программного обеспечения 11
1.13. Требования к надежности 11
1.14. Требования к поддержке эксплуатации 12
1.15. Требования по сохранности информации при авариях 12
1.16. Требования к патентной чистоте 12
1.17. Требования к обеспечению безопасности персональных данных 12
2. Технические требования к закупаемому оборудованию и программному обеспечению 15
2.1. Требования к АРМ тип 1 15
2.1.1. Требования к персональному компьютеру форм-фактора «все в одном» 15
2.1.2. Требования к веб-камере 15
2.1.3. Требования к сетевому фильтру 16
2.1.4. Требования к принтеру лазерному 16
2.1.5. Требования к штрих-кодовому сканеру 16
2.1.6. Требования к комплекту средств защиты информации 17
2.1.7. Требования к программному обеспечению общего назначения 17
2.2. Требования к АРМ тип 2 17
2.2.1. Требования к персональному компьютеру форм-фактора «все в одном» 17
2.2.2. Требования к сетевому фильтру 18
2.2.3. Требования к принтеру лазерному 18
2.2.4. Требования к штрих-кодовому сканеру 19
2.2.5. Требования к комплекту средств защиты информации 19
2.2.6. Требования к программному обеспечению общего назначения 20

2.3. Требования к АРМ тип 3 20
2.3.1. Требования к персональному компьютеру форм-фактора «все в одном» 20
2.3.2. Требования к сетевому фильтру 21
2.3.3. Требования к принтеру лазерному 21
2.3.4. Требования к штрих-кодовому сканеру 21
2.3.5. Требования к термотрансферному принтеру 22
2.3.6. Требования к комплекту средств защиты информации 23
2.3.7. Требования к программному обеспечению общего назначения 23
2.4. Требования к серверному оборудованию 23
2.4.1. Требования к серверам 24
2.4.2. Требования к программному обеспечению общего назначения 24
2.4.3. Требования к средствам защиты информации 24
2.4.4. Архитектура единого информационно-технологического пространства 25
2.4.4.1. Требования к службе каталога 25
2.4.4.2. Требования к подсистеме сохранения и восстановления данных 26
2.4.4.3. Требования к подсистеме мониторинга и инвентаризации 26
2.5. Требования к источникам бесперебойного питания (ИБП) 27
2.5.1. Требования к ИБП для АРМ тип 1, 2, 3 27
2.5.2. Требования к ИБП для серверного оборудования 27
2.5.3. Требования к ИБП для настенного шкафа 28
2.6. Заземление 28
2.7. Требования к комплекту оборудования для создания инфраструктуры 29
2.7.1. Активное сетевое оборудование 29
2.7.1.1. Требования к маршрутизатору 29
2.7.1.2. Требования к сетевому коммутатору 29
2.7.2. Требования к комплекту климатического оборудования 30
2.7.3. Требования к комплекту материалов СКС 30
2.7.3.1. Требования к настенному шкафу 31
2.7.4. Общие требования к структурированной кабельной системе 31
3. Технические требования к системе информационной безопасности 32
3.1. Серверная часть 32
3.2. Клиентская часть (персональные компьютеры) 33
3.3. Для использования на объекте Грузополучателей 33
4. Требования к содержанию и выполнению работ 34
4.1. Перечень работ по вводу в эксплуатацию 34
4.2. Требования к работам по внедрению и пуско-наладке компьютерного и сетевого оборудования с лицензионным программным обеспечением 34

4.3. Требования к внедрению и пуско-наладке технологического программного обеспечения (АИСТ) 35

4.4. Требования по обеспечению передачи данных из АИСТ Грузополучателя в Единую информационную базу данных. 35

4.5. Требования к составу передаваемых данных в ЕИБД. 35

4.6. Требования к частоте передачи данных в ЕИБД. 37

4.7. Требования к мониторингу передачи данных в ЕИБД 37

4.8. Консультационные услуги по подготовке и вводу данных для обеспечения функционирования системы АИСТ на объектах эксплуатации и в едином информационном центре. 37

4.9. Консультационные услуги из единого информационного центра по информационному обеспечению удаленного мониторинга и администрирования программного обеспечения на местах.....38

4.10. Консультационные услуги по подготовке и вводу данных при инструктаже и консультировании Пользователей, в том числе удаленно из ЕИЦ. 38

4.11. Обеспечение функционирования программного обеспечения общего назначения для АРМ 38

4.12. Техническая поддержка системы защиты информации 39

4.12.1. Серверная часть 39

4.12.2. Клиентская часть и отдельные АРМ....39

4.12.3. Техническая поддержка прочих программных средств....39

4.13. Задачи Поставщика 40

5. Список нормативно-технических документов и правовых актов....41

5.1. Нормативно-технические документы....41

5.2. Нормативные правовые акты 42

Приложение 1. Потребность в оборудовании, программном обеспечении, материалах 44

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Ивановский-1 филиал....44

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Ивановский-2 филиал....45

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Шуйский филиал 46

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Кинишемский филиал 47

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Вичугский филиал 48

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Фурмановский филиал 49

Приложение 2. Перечень грузополучателей 50

Введение

Целью настоящего технического задания является определение требований к закупке компьютерного и сетевого оборудования с лицензионным программным обеспечением, осуществлению монтажа компьютерного и сетевого оборудования с лицензионным программным обеспечением, пусконаладочных работ, установке и внедрению лицензионного программного обеспечения и программно-технических средств защиты информационной базы по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, а также проведению инструктажа медицинского и технического персонала по эксплуатации компьютерного оборудования для развития единого информационного пространства службы крови России, ее единой информационной базы и внедрения типовой автоматизированной информационной системы трансфузиологии (далее – АИСТ) в филиалы Областного бюджетного учреждения здравоохранения «Ивановская областная станция переливания крови» (далее – Грузополучатели), в соответствии с Федеральным законом №349-ФЗ от 2 декабря 2013 г. «О федеральном бюджете на 2014 год и на плановый период 2015 и 2016 годов» (Приложение №34).

В 2010г. в соответствии с постановлением Правительства Российской Федерации от 31 декабря 2009 г. № 1145 «О финансовом обеспечении за счет бюджетных ассигнований федерального бюджета мероприятий по развитию службы крови», для областного бюджетного учреждения здравоохранения «Ивановская областная станция переливания крови» (далее ОБУЗ «Ивановская ОСПК») были проведены работы по закупке компьютерного и сетевого оборудования с лицензионным программным обеспечением и программно-техническими средствами защиты и обеспечению информационного взаимодействия ОБУЗ «Ивановская ОСПК» с единым информационным центром и ведения единой информационной базы данных службы крови России. В рамках выполнения указанных работ в Государственном учреждении здравоохранения ОБУЗ «Ивановская ОСПК» был создан региональный информационный центр (РИЦ) информационной системы Службы крови.

В 2014 году в соответствии с Федеральным законом №349-ФЗ от 2 декабря 2013 г. «О федеральном бюджете на 2014 год и на плановый период 2015 и 2016 годов» (Приложение №34) необходимо выполнить поставку компьютерного и сетевого оборудования и лицензионным программным обеспечением, монтаж закупаемого оборудования, пусконаладочные работы, установку и внедрение лицензионного программного обеспечения и программно- технических средств защиты для Грузополучателей.

Особенностью настоящего Технического задания является формирование требований к закупаемому компьютерному и сетевому оборудованию с лицензионным программным обеспечением и лицензионному программному обеспечению для полной совместимости с созданным единым информационным пространством Службы крови Российской Федерации, единой информационной базы Грузополучателей, с техническими решениями предыдущих этапов по созданию единой информационной базы службы крови России.

Перечень принятых сокращений

АРМ	Автоматизированное рабочее место
АИС	Автоматизированная информационная система
АИСТ	Автоматизированная информационная система трансфузиологии
БД	База данных
ЕДЦ	Единый донорский центр
ИБП	Источник бесперебойного питания
ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть
ЛПУ	Лечебно-профилактическое учреждение
ОПК	Отделение переливания крови
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
РИЦ	Региональный информационный центр
СЗПДн	Система защиты персональных данных
СЗИ	Средства защиты информации
СКС	Структурированная кабельная сеть
СПИД	Синдром приобретенного иммунодефицита
СПК	Станция переливания крови
СУБД	Система управления базами данных
ЕИЦ	Единый информационный центр службы крови России
ФМБА России	Федеральное медико-биологическое агентство России
ФСТЭК	Федеральная служба по техническому и экспортному контролю
CD-ROM	Compact Disc read-only memory, лазерный диск для хранения данных
FTP	File Transfer Protocol — протокол передачи файлов
RAID	redundant array of independent disks — избыточный массив независимых жёстких дисков
NBD	next business day, следующий рабочий день

1. Общие требования к условиям поставки

1.1. Условия поставки

Автоматизированная информационная система трансфузиологии (далее – «система», АИСТ) – программный комплекс, предназначенный для автоматизации технологической деятельности учреждений Службы крови и создания единой информационной базы в рамках реализации мероприятий, связанных с обеспечением безопасности донорской крови и её компонентов.

Техническое задание содержит требования к закупаемому в 2014 году Грузополучателями для внедрения системы оборудованию и программному обеспечению, а также информационным сервисам, создаваемым на закупаемом оборудовании и программном обеспечении с целью обеспечения бесперебойного и надежного функционирования единой информационной базы.

Прикладное программное обеспечение для автоматизации технологического процесса СПК (система АИСТ) передается в учреждения Службы крови России Федеральным медико-биологическим агентством (ФМБА России). Обладателем исключительных прав на систему АИСТ является Федеральное государственное бюджетное учреждение здравоохранения «Центр Крови Федерального медико-биологического агентства России» (далее – Центр крови ФМБА России). Система АИСТ передается в учреждения Службы крови на безвозмездной основе.

Внедрение системы АИСТ и поддержка работоспособности ИС АИСТ обеспечивается Поставщиком в объеме, предусмотренном настоящим Техническим заданием и Государственным контрактом.

1.2. Место поставки

Поставка оборудования и программного обеспечения (далее – оборудование) осуществляется по адресам Грузополучателей, указанным в Приложении 2 к настоящему Техническому заданию. Перечень оборудования, программного обеспечения, материалов для поставки Грузополучателям указан в Приложении 1 к настоящему Техническому заданию.

1.3. Комплектация оборудования

Поставка оборудования осуществляется комплектно. Комплект включает в себя оборудование для работы персонала (АРМ, принтеры лазерные, штрих-кодовые сканеры, термотрансферные принтеры, веб-камеры), серверное оборудование, ИБП и комплект оборудования для создания инфраструктуры (активное сетевое оборудование, климатическое оборудование, материалы СКС).

Спецификация оборудования и материалов приведена в разделе 2 настоящего Технического задания.

В целях организации исполнения Государственного контракта Поставщик в течение 10 рабочих дней после даты заключения Государственного контракта представляет Заказчику календарный план-график выполнения работ.

1.4. Условия эксплуатации

Поставщик при выполнении работ, указанных в настоящем Техническом задании, должен обеспечить поддержку бесперебойной работы прикладного программного обеспечения автоматизированной информационной системы трансфузиологии (АИСТ), установленного на АРМ в технологических подразделениях Грузополучателей.

Характеристики технических средств должны обеспечивать их надежную эксплуатацию при следующих условиях:

- параметры электропитания (220 В +/- 20 В, 50 Гц +/- 1 Гц);
- резкие скачки напряжения;
- температура окружающей среды: от + 5^0 С до +35^0 С;
- относительная влажность от 15% до 80% при температуре +23^0 С.

Наличие вводов электропитания достаточной мощности, а также действующей шины заземления, на местах инсталляции АРМ, серверного оборудования, активного сетевого оборудования обеспечивают Грузополучатели.

Серверы баз данных системы должны работать в непрерывном круглосуточном режиме. Регламентные работы на серверном оборудовании должны проводиться в соответствии со сроками

проведения регламентных работ, определенными в технической документации на закупаемое оборудование, но не реже одного раза в шесть месяцев. При проведении регламентных работ серверное оборудование системы должно быть остановлено не более чем на 4 часа. Копирование данных системы и обновление исполняемых кодов прикладных программ системы должно проводиться без перезапуска серверного оборудования. После установки обновлений программного обеспечения общего назначения (update) серверное оборудование должно быть перезапущено.

1.5. Требования к документации

Каждая единица закупаемого оборудования должна поставляться с комплектом технической документации, включая руководство пользователя. Состав и содержание технической документации должны быть достаточны для выполнения пусконаладочных работ, гарантийного и послегарантийного обслуживания системы.

Каждая единица оборудования должна сопровождаться формуляром или паспортом (если такой документ предусмотрен производителем оборудования) в соответствии с государственным стандартом Российской Федерации ГОСТ 2.601-95.

Документация может быть передана грузополучателям на бумажных носителях и в электронном виде (при наличии) на оптическом диске (CD-ROM или DVD-ROM).

В течение 10 (десяти) рабочих дней после подписания Контракта Поставщик должен предоставить Заказчику по 1 (одному) экземпляру надлежаще удостоверенных проектов документов:

- описание обеспечения присутствия на объекте информатизации и полный перечень оказываемых услуг. Необходимо описать доступ к этим услугам, максимальное время ответа на заявку Пользователя, а также процедуры приоритетов запросов;

- эксплуатационную документацию на систему с регламентом и процедурами резервного копирования, восстановления данных и программного обеспечения с учетом времени их актуальности;

- описание комплекса средств поддержки предлагаемой участником системы защиты персональных данных;

- проекты документов для подсистемы защиты информации, в том числе:

  - документы, определяющие структуру СЗПДн;
  - документы, определяющие требования, состав и содержание организационно-технических мероприятий по обеспечению безопасности информации на объектах информатизации;

- документ «Пояснительная записка по службе каталогов и инфраструктурным сервисам» с описанием службы каталогов, которая будет реализована на объектах Грузополучателей в соответствии с настоящим Техническим заданием;

- документ «Пояснительная Записка по подсистеме сохранения и восстановления данных (подсистеме резервного копирования)»;

- документ «Пояснительная Записка по подсистеме мониторинга и инвентаризации»;

- календарный план – график работ;

- документ "Паспорт инфраструктуры" Грузополучателя, включающий следующие сведения:

  - детальный перечень закупленного компьютерного и сетевого оборудования (включая спецификацию и схему размещения на поэтажном плане объекта);
  - наименование учетных записей и паролей доступа пользователей к программному обеспечению и оборудованию;
  - план IP-адресации;
  - описание аппаратно-программных средств подсистемы защиты персональных данных, схема и текстовое описание их расположения и взаимодействия;
  - схема размещения данных (и установленного программного обеспечения) на серверах;
  - регламенты, схемы, протоколы и средства информационного обмена между Получателем и ЕИЦ;
  - перечень регламентных работ (включая план резервного копирования) и описание механизмов резервного копирования и программно-аппаратного комплекса для обеспечения резервного копирования.

1.6. Требования к протоколированию выполненных работ

По результату внедрения системы Поставщик должен предоставить комплект документации с перечислением выполненных работ по настройке комплекса, в том числе:

- протокол пуско-наладки закупленного компьютерного и сетевого оборудования, включая описание настроек и размещения оборудования;
- протокол настройки закупленного компьютерного и сетевого оборудования, включая подтверждение приема указанных настроек в Едином информационном центре ФГБУЗ «Центр крови ФМБА России», осуществляющем эксплуатацию базы данных донорства крови и ее компонентов;
- протокол установки и настройки АИСТ, включая описание справочников и настроек;
- протокол настройки телекоммуникационного оборудования и каналов связи в объеме, необходимом для организации возможности осуществления передачи данных от Грузополучателя в Единый информационный центр, включая подтверждение обмена данными с Единым информационным центром ФГБУЗ «Центр крови ФМБА России», и РИЦ;
- протокол о создании системы защиты персональных данных (СЗПДн), включая согласование с ФГБУЗ «Центр крови ФМБА России» настроек компонент СЗПДн и порядка подключения в защищенный информационный контур базы данных донорства крови и ее компонентов в целях обеспечения совместимости с единым информационным пространством Службы крови;
- протокол подключения локальной вычислительной сети Грузополучателя к существующей ведомственной сети передачи данных базы данных донорства крови и ее компонентов с целью обеспечения информационного взаимодействия между объектами системы и ЕИЦ с соблюдением требований Указа Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», включая подтверждение обмена данными с Единым информационным центром ФГБУЗ «Центр крови ФМБА России».

1.7. Требования к надежности

Время работы персональных компьютеров определяется действующими регламентами деятельности Грузополучателей.

Работа закупаемого серверного и телекоммуникационного оборудования должна быть организована по схеме 7x24x365 (7 дней в неделю, 24 часа в сутки, 365 дней в году).

Поставщиком должны быть предусмотрены организационно-технические мероприятия по защите от заражения вредоносными программами, как в части сохранности данных, так и в части обеспечения работоспособности АИС Грузополучателей.

Сохранность данных должна быть реализована за счет функции резервного копирования и восстановления из резервных копий.

Сохранность информации на сервере должна обеспечиваться в следующих аварийных ситуациях:

- пропадание электропитания;
- отказ технических средств;
- ошибки в работе системного ПО;
- ошибки в прикладном программном обеспечении;

В эксплуатационной документации должен быть приведен регламент и определены процедуры резервного копирования, восстановления данных и программного обеспечения с учетом времени их актуальности.

Необходимо обеспечить сохранность информации и восстановление функционирования системы без потери информации в аварийных ситуациях.

Сохранность информации на сервере системы должна обеспечиваться при следующих аварийных ситуациях:

- отказ комплекса программно-технических средств системы в результате сбоя или выхода из строя его технических средств;
- отказ комплекса программно-технических средств системы в результате сбоя его общесистемного программного обеспечения или программного обеспечения общего назначения;
- сбой или отказ комплекса программно-технических средств системы в результате ошибки в прикладном программном обеспечении системы;

В системе должна быть обеспечена сохранность конфигурационной информации системы.

В системе должно быть предусмотрено резервное копирование всей централизованно сохраняемой и критической для функционирования системы информации. Процедуры резервного копирования должны соответствовать п.2.4.4.2. « Требования к подсистеме сохранения и восстановления данных» настоящего Технического задания.

1.8. Требования к ремонту, техническому и гарантийному обслуживанию

Поставщик должен обеспечить следующие сроки гарантийных периодов (Гарантийный срок) на закупаемое серверное и сетевое оборудование, оборудование АРМ и иное оборудование:

- Гарантия производителя – не менее 12 (двенадцати) месяцев;
- Гарантийный срок – не менее 12 (двенадцати) месяцев от даты подписания Сторонами акта выполненных работ;
- Срок гарантийного обслуживания – не менее 12 (двенадцати) месяцев.

Срок гарантии исчисляется с момента подписания сторонами Акта выполненных работ.

Для бесперебойной работы системы АИСТ, в случае возникновения неисправности на Оборудовании в течение гарантийного срока, Поставщик обеспечивает восстановление неисправности путем ремонта/замены на идентичное в сроки не превышающий 24 часов.

В Гарантийный срок Поставщик должен обеспечить различные способы доступа к системе технической поддержки («горячей линии») для приема обращений персонала Грузополучателей и оказания технических консультаций.

Время регистрации заявки, направляемой Грузополучателями в техническую службу Поставщика посредством телефонной связи, электронной почты или факсимильной связи, не должно превышать:

- в рабочее время (в соответствии с распорядком работы Грузополучателей), не более – 30 минут;
- в вечерние часы (с момента окончания рабочего дня до 21 часа 00 минут по местному времени), не более – 60 минут;
- в выходные и праздничные дни с 08 часов 00 минут до 21 часа 00 минут местного времени, не более – 120 минут;

Время реагирования на направленные Грузополучателями заявки, в техническую службу Поставщика посредством телефонной связи, электронной почты или факсимильной связи, не должно превышать:

- в рабочее время (в соответствии с распорядком работы Грузополучателей), не более – 90 минут;
- в вечерние часы (с момента окончания рабочего дня до 21 часа 00 минут по местному времени), не более – 180 минут;
- в выходные и праздничные дни с 08 часов 00 минут до 21 часа 00 минут местного времени, не более – 240 минут;

1.9. Поддержка эксплуатации

Описание обеспечения присутствия в регионах по адресам Грузополучателей и полный перечень оказываемых услуг предоставляется Поставщиком Заказчику в течение 10 рабочих дней после даты заключения государственного контракта. Необходимо описать доступ к этим услугам, максимальное время ответа на заявку Грузополучателей, а также процедуры приоритетов запросов.

В предложении по поддержке эксплуатации системы Поставщик должен предусмотреть ежедневный мониторинг состояния оборудования и программного обеспечения. Поставщик должен предусмотреть поддержку запросов от Грузополучателей по обеспечению работоспособности и выполнению требований соглашений на гарантийное обслуживание системы.

Для поддержки эксплуатации системы Поставщик должен предусмотреть мониторинг состояния программного обеспечения. Поставщик должен предусмотреть поддержку запросов от пользователей по обеспечению работоспособности и обслуживанию системы. Поддержка эксплуатации на каждом из объектов осуществляется с момента ввода данного объекта в эксплуатацию по 31 декабря 2015 года (включительно).

1.10. Требования к закупаемому оборудованию

Автоматизированные рабочие места оборудуются в соответствии с ГОСТ (в части обязательного исполнения требований, установленных действующим законодательством): ГОСТ 27201-87, ГОСТ 27818-88, ГОСТ 24750-81, ГОСТ Р 50628-2000, ГОСТ Р 51318.24-99, ГОСТ Р 50839-2000, ГОСТ Р 50948-2001, ГОСТ Р 51318.22-99, ГОСТ Р МЭК 60950-2002, ГОСТ 26329-84.

Все закупаемое оборудование, подключаемое к сети электропитания, должно комплектоваться силовыми кабелями, имеющими разъём российского стандарта с заземлением. Оборудование, подключаемое к ЛВС, должно комплектоваться коммутационными шнурами RJ45-RJ45 кат. 5E, 4 пары длиной не менее 3м.

1.11. Требования к закупаемым лицензионным операционным системам и программам общего назначения

При поставке программного обеспечения должны быть выполнены требования части четвертой Гражданского Кодекса Российской Федерации.

Выполнение требований по обеспечению лицензионной чистоты программного обеспечения, обеспечивается Поставщиком.

Все оборудование должно обеспечивать возможность работы с кириллицей в соответствии со стандартами ISO в части, не противоречащей законодательству Российской Федерации.

Закупаемое программное обеспечение должно быть унифицировано по составу и версиям.

1.12. Требования к совместимости оборудования и программного обеспечения

Все программное обеспечение должно быть совместимым с аппаратным обеспечением.

Поставляемое оборудование и лицензионное программное обеспечение должно быть совместимым с прикладным программным обеспечением АИСТ, передаваемым Грузополучателю Центром крови ФМБА России на безвозмездной основе.

Поставляемое серверное оборудование и АРМ должны соответствовать системным требованиям ИС АИСТ.

Системные требования ИС АИСТ к оборудованию и программному обеспечению:

- Для серверной части ИС АИСТ
  - Аппаратная платформа x86-64
  - Операционная система Microsoft Windows Server 2003/Server 2003R2/ Server 2008/ Server 2008R2
  - Microsoft SQL Server 2008 для управления базами данных АИСТ
  - Процессор не менее 2.0ГГц на ядро, не менее 4 ядер
  - Оперативная память не менее 8Гб
  - Не менее 500Гб на жестком диске
- Для персональных компьютеров (пользовательской части ИС АИСТ)
  - Аппаратная платформа x86 или x86-64
  - Операционная система Microsoft Windows 7
  - Процессор не менее 2.0ГГц на ядро, не менее 2 ядер
  - Оперативная память не менее 4Гб
  - Не менее 200Гб на жестком диске
  - Видеокарта и экран с разрешением не менее 1280x1024 точек
  - Клавиатура, манипулятор «мышь»
  - Звуковая карта, устройства воспроизведения звука (динамики или колонки)

1.13. Требования к надежности

Создаваемая Поставщиком система должна обладать надежностью, обеспечивающей круглосуточную работу пользователей и оперативное восстановление работоспособности при любых сбоях.

Система в целом должна не терять работоспособность в случае возникновения сбоев, аварий и отказов, возникающих на рабочих станциях и печатающих устройствах.

ПО должно обеспечивать восстановление работоспособности при появлении сбоев, аварий и отказов, возникающих на серверах и сетевом аппаратном обеспечении.

В Системе должны быть реализованы функции резервного копирования и восстановления баз данных из резервных копий. Система должна позволять производить настройку параметров резервного копирования (периодичность, время, по запросу администратора).

Система должна в целом сохранять работоспособность при некорректных действиях конечных пользователей:

- ввод некорректных данных;
- неверный или аварийный выход из системы (завершение работы с системой) на рабочей станции.

Применение подсистемы защиты информации и выбор применяемых средств защиты информации не должны ухудшать надежность системы в целом.

1.14. Требования к поддержке эксплуатации

Программное обеспечение должно иметь развитые средства администрирования и поддержки эксплуатации, включающие средства проверки целостности данных и восстановления их при сбоях.

Для обеспечения целостности баз данных необходимо производить периодическое резервное копирование баз данных. Резервное копирование и восстановление должно производиться на сервере средствами программного обеспечения. Выполнение процедур восстановления данных должно выполняться администратором системы.

1.15. Требования по сохранности информации при авариях

В системе должны быть использованы средства и реализованы технические решения, обеспечивающие сохранность информации и восстановление функционирования системы без потери информации в аварийных ситуациях.

Сохранность информации на сервере системы должна обеспечиваться при следующих аварийных ситуациях:

- отказ комплекса программно-технических средств системы в результате сбоя или выхода из строя его технических средств;
- отказ комплекса программно-технических средств системы в результате сбоя его общесистемного программного обеспечения или программного обеспечения общего назначения;
- сбой или отказ комплекса программно-технических средств системы в результате ошибки в прикладном программном обеспечении системы;

В системе должна быть обеспечена сохранность (за счет хранения на энергонезависимых носителях) конфигурационной информации системы.

В системе должны быть предусмотрены Поставщиком два уровня резервного копирования всей централизованно сохраняемой и критической для функционирования системы информации. Резервное копирование на дисках, резервное копирование на съемные устройства хранения данных.

В течение 20 рабочих дней от даты заключения государственного контракта Поставщик предоставляет Заказчику проект эксплуатационной документации на систему с регламентом и процедурами резервного копирования, восстановления данных и программного обеспечения с учетом времени их актуальности.

1.16. Требования к патентной чистоте

ПО должно быть свободно от возможности предъявления любых прав и притязаний третьих лиц, основанных на промышленной, интеллектуальной или другой собственности.

Вопросы правообладания информацией (информационными ресурсами), формируемой в связи с использованием системы, находятся в полной компетенции Грузополучателей и регулируются действующими нормативными положениями действующего законодательства.

1.17. Требования к обеспечению безопасности персональных данных

Создаваемая на объектах Грузополучателей СЗПДн должна обеспечить безопасность персональных данных при их обработке в информационной системе персональных данных.

СЗПДн в ИСПДн должна обеспечить:

- конфиденциальность информации - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на нее право;
- целостность информации – избежание несанкционированной модификации информации;
- доступность информации – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Методы и способы защиты ПДн, применяемые в СЗПДн, должны соответствовать требованиям, предъявляемым к информационным системам персональных данных утвержденных приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» для многопользовательского режима обработки персональных данных, разных правах доступа, и подключаемых к сетям международного информационного обмена.

По окончании приемочных испытаний и до начала обработки подлежащей защите информации необходимо проведение аттестации ИСПДн с целью официального подтверждения ее соответствия требованиям стандартов, нормативно-правовых актов и нормативно-технических документов (в том числе по безопасности ПДн), утвержденных ФСТЭК.

Проектные решения должны обеспечивать соблюдение следующих нормативных правовых актов и нормативно-методических документов:

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Методический документ ФСТЭК от 11.02.2014 г. "Меры защиты информации в государственных информационных системах"
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства РФ № 687 от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
- Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/5-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;
- Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК, 2008г;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (РД ОК), Гостехкомиссия (ФСТЭК) России, 2002;
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к информации (РД АС). Гостехкомиссия (ФСТЭК) Россия, 1992;
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД СВТ). Гостехкомиссия (ФСТЭК) Россия, 1992;
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД МЭ). Гостехкомиссия (ФСТЭК) Россия, 1998;
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия (ФСТЭК) Россия, 1992.

Поставщик в течение 20 рабочих дней от даты заключения государственного контракта представляет Заказчику проекты документов для реализации подсистемы защиты информации.

2. Технические требования к закупаемому оборудованию и программному обеспечению

2.1.Требования к АРМ тип 1

АРМ типа 1 предназначены для эксплуатации в пределах ЛВС Грузополучателей. АРМ тип 1 включают в себя оборудование и программное обеспечение, перечисленные в разделе 2.1 настоящего Технического задания. Здесь и далее, если не указано иное, каждый компонент АРМ поставляется в количественном соотношении «1 АРМ = 1 единица компонента».

2.1.1. Требования к персональному компьютеру форм-фактора «все в одном»

Персональные компьютеры форм-фактора «все в одном» должны удовлетворять следующим условиям:

Таблица 1

Параметр	**Требование**
Экран	Диагональ не менее 22”, не более 25”, максимальное разрешение не ниже 1920*1080, яркость не ниже 300 кд/м^2
Процессор	Количество процессорных ядер – не менее двух, тактовая частота – не менее 2,50ГГц, кэш – не менее 6Mb
Оперативная память	Не менее 8Гб DDR3 1600МГц, работающих в двухканальном режиме, с возможностью расширения до 16ГБ.
Жесткий диск	Не менее SATA 500Гб 7200rpm
Оптический привод	Не менее DVD±RW
Графическая подсистема	Встроенная, с поддержкой HD
Звуковая подсистема	Не менее двух встроенных стереодинамиков
Сетевые подключения	Встроенный адаптер Ethernet 10/100/1000 Мбит/с
Слот расширения	Не менее одного порта miniPCIe
Порты подключения периферийных устройств	Не менее 8 портов USB
Устройство ввода	Полноразмерная клавиатура RUS/ENG с цифровым блоком, интерфейс подключения USB
Устройство позиционирования	Оптическая мышь, число кнопок не менее двух, интерфейс подключения USB
Вес	Не более 12кг
Питание	Блок питания мощностью не более 200Вт с сертификатом эффективности не хуже 80 PLUS Gold
Безопасность	Наличие слота для замка Kensington Lock

2.1.2. Требования к веб-камере

Веб-камеры должны удовлетворять следующим условиям:

Таблица 2

Параметр	**Требование**
Разрешение датчика	не менее 0,7 мегапиксель

Крепление	Портативное, к монитору
Тип интерфейса подключения к ПК	USB
Встроенный микрофон	Да
Длина шнура	не менее 1,4 м

2.1.3. Требования к сетевому фильтру

Сетевые фильтры должны удовлетворять следующим условиям:

Таблица 3

Параметр	**Требование**
Суммарная мощность нагрузки	Не менее 2кВт
Максимальный ток нагрузки	Не менее 10А
Фильтрация радиочастотных и электромагнитных помех	Да
Номинальное напряжение	220В
Тип вилки	5 шт. Schuko CEE7/4 с заземлением
Длина шнура	Не менее 3м

2.1.4. Требования к принтеру лазерному

Принтеры лазерные должны удовлетворять следующим условиям:

Таблица 4

Параметр	**Требование**
Тип печати	Лазерная, черно-белая
Максимальный формат печати	А4
Автоматическая двухсторонняя печать	Да
Скорость печати	Не менее 24 стр./мин
Интерфейсы подключения	Не хуже USB 2.0 Не хуже Ethernet 10/100
Разрешение печати (точек на дюйм)	Не менее 600х600
Стартовый комплект картриджа	Не менее 1000 стр.
Дополнительный комплект картриджа	Не менее 2000 стр.
Нагрузка	не менее 8000 стр. в месяц
Объем памяти	не менее 32Мб
Расходные материалы	картридж (фотобарабан и тонер – картридж в одном устройстве)

2.1.5. Требования к штрих-кодовому сканеру

Штрих-кодовые сканеры должны удовлетворять следующим условиям:

Таблица 5

Параметр	Требование
Тип сканера	Ручной
Максимальное разрешение сканера	Не более 0,102 мм
Максимальная скорость сканирования	Не менее 400 сканирований в секунду
Интерфейс подключения к ПК	USB
Устойчивость к падениям	Высота не менее 1,5м
Обязательное визуальное и звуковое подтверждение правильности чтения штрихового кода	

2.1.6. Требования к комплекту средств защиты информации

В качестве средств защиты информации для АРМ типа 1 должны использоваться:

- средства защиты информации от НСД;
- средства антивирусной защиты с бесплатным обновлением баз в течение двух лет;

Предлагаемое к использованию программное обеспечение должно быть лицензионно-чистым.

Решения по использованию средств защиты должны приниматься с учетом обеспечения поддержки его функционирования производителем или распространителем данного ПО.

В процессе эксплуатации СЗПДн права на использование (лицензии) применяемых средств защиты должны поддерживаться в актуальном состоянии.

Программные (программно-аппаратные) средства должны иметь соответствующие сертификаты ФСТЭК и/или ФСБ России, позволяющие их использование для защиты информации в информационных системах персональных данных.

2.1.7. Требования к программному обеспечению общего назначения

В качестве программного обеспечения общего назначения для АРМ типа 1 необходимо предложить лицензированные покупные программные средства:

- операционные системы, совместимые с системой АИСТ;
- пакет офисных приложений для АРМ, совместимый с форматами Microsoft Office (doc, xls, ppt), включая текстовый редактор, электронные таблицы, программу работы с презентациями. Проверка пунктуации русского языка в текстовом редакторе должна выполняться без помощи скачиваемых дополнений. Редактор электронных таблиц в составе офисного пакета должен обладать функциями: "вычислить формулу" (показать этапы вычисления);
- системы управления сохранением и восстановлением данных;
- системы мониторинга и инвентаризации;

2.2. Требования к АРМ тип 2

АРМ типа 2 предназначены для эксплуатации в пределах ЛВС Грузополучателей. АРМ тип 2 включают в себя оборудование и программное обеспечение, перечисленные в разделе 2.2 настоящего Технического задания.

2.2.1. Требования к персональному компьютеру форм-фактора «все в одном»

Персональные компьютеры форм-фактора «все в одном» должны удовлетворять следующим условиям:

Таблица 6

Параметр	**Требование**
Экран	Диагональ не менее 22”, не более 25”, максимальное разрешение не ниже 1920*1080, яркость не ниже 300 кд/м^2
Процессор	Количество процессорных ядер – не менее двух, тактовая частота – не менее 2,50ГГц, кэш – не менее 6Mb
Оперативная память	Не менее 8Гб DDR3 1600МГц, работающих в двухканальном режиме, с возможностью расширения до 16ГБ.
Жесткий диск	Не менее SATA 500Гб 7200rpm
Оптический привод	Не менее DVD±RW
Графическая подсистема	Встроенная, с поддержкой HD
Звуковая подсистема	Не менее двух встроенных стереодинамиков
Сетевые подключения	Встроенный адаптер Ethernet 10/100/1000 Мбит/с
Слот расширения	Не менее одного порта miniPCIe
Порты подключения периферийных устройств	Не менее 8 портов USB
Устройство ввода	Полноразмерная клавиатура RUS/ENG с цифровым блоком, интерфейс подключения USB
Устройство позиционирования	Оптическая мышь, число кнопок не менее двух, интерфейс подключения USB
Вес	Не более 12кг
Питание	Блок питания мощностью не более 200Вт с сертификатом эффективности не хуже 80 PLUS Gold
Безопасность	Наличие слота для замка Kensington Lock

2.2.2. Требования к сетевому фильтру

Сетевые фильтры должны удовлетворять следующим условиям:

Таблица 7

Параметр	**Требование**
Суммарная мощность нагрузки	Не менее 2кВт
Максимальный ток нагрузки	Не менее 10А
Фильтрация радиочастотных и электромагнитных помех	Да
Номинальное напряжение	220В
Тип вилки	5 шт. Schuko CEE7/4 с заземлением
Длина шнура	Не менее 3м

2.2.3. Требования к принтеру лазерному

Принтеры лазерные должны удовлетворять следующим условиям:

Таблица 8

Параметр	**Требование**
Тип печати	Лазерная, черно-белая
Максимальный формат печати	А4
Автоматическая двухсторонняя печать	Да
Скорость печати	Не менее 24 стр./мин
Интерфейсы подключения	Не хуже USB 2.0 Не хуже Ethernet 10/100
Разрешение печати (точек на дюйм)	Не менее 600х600
Стартовый комплект картриджа	Не менее 1000 стр.
Дополнительный комплект картриджа	Не менее 2000 стр.
Нагрузка	не менее 8000 стр. в месяц
Объем памяти	не менее 32Мб
Расходные материалы	картридж (фотобарабан и тонер – картридж в одном устройстве)

2.2.4. Требования к штрих-кодовому сканеру

Штрих-кодовые сканеры должны удовлетворять следующим условиям:

Таблица 9

Параметр	**Требование**
Тип сканера	Ручной
Максимальное разрешение сканера	Не более 0,102 мм
Максимальная скорость сканирования	Не менее 400 сканирований в секунду
Интерфейс подключения к ПК	USB
Устойчивость к падениям	Высота не менее 1,5м
Обязательное визуальное и звуковое подтверждение правильности чтения штрихового кода	

2.2.5. Требования к комплекту средств защиты информации

В качестве средств защиты информации для АРМ типа 2 должны использоваться:

- средства защиты информации от НСД;
- средства антивирусной защиты с бесплатным обновлением баз в течение двух лет;

Предлагаемое к использованию программное обеспечение должно быть лицензионно-чистым.

Решения по использованию средств защиты должны приниматься с учетом обеспечения поддержки его функционирования производителем или распространителем данного ПО.

В процессе эксплуатации СЗПДн права на использование (лицензии) применяемых средств защиты должны поддерживаться в актуальном состоянии.

Программные (программно-аппаратные) средства должны иметь соответствующие сертификаты ФСТЭК и/или ФСБ России, позволяющие их использование для защиты информации в информационных системах персональных данных.

2.2.6. Требования к программному обеспечению общего назначения

В качестве программного обеспечения общего назначения для АРМ типа 2 необходимо предложить лицензированные покупные программные средства:

- операционные системы, совместимые с системой АИСТ;
- пакет офисных приложений для АРМ, совместимый с форматами Microsoft Office (doc, xls, ppt), включая текстовый редактор, электронные таблицы, программу работы с презентациями. Проверка пунктуации русского языка должна выполняться без помощи скачиваемых дополнений. Редактор электронных таблиц в составе офисного пакета должен обладать функциями: "вычислить формулу" (показать этапы вычисления);
- системы управления сохранением и восстановлением данных;
- системы мониторинга и инвентаризации;

2.3.Требования к АРМ тип 3

АРМ типа 3 предназначены для эксплуатации в пределах ЛВС грузополучателей. АРМ тип 3 включают в себя оборудование и программное обеспечение, перечисленные в разделе 2.3 настоящего Технического задания.

2.3.1. Требования к персональному компьютеру форм-фактора «все в одном»

Персональные компьютеры форм-фактора «все в одном» должны удовлетворять следующим условиям:

Таблица 10

Параметр	**Требование**
Экран	Диагональ не менее 22”, не более 25”, максимальное разрешение не ниже 1920*1080, яркость не ниже 300 кд/м^2
Процессор	Количество процессорных ядер – не менее двух, тактовая частота – не менее 2,50ГГц, кэш – не менее 6Mb
Оперативная память	Не менее 8Гб DDR3 1600МГц, работающих в двухканальном режиме, с возможностью расширения до 16ГБ.
Жесткий диск	Не менее SATA 500Гб 7200rpm
Оптический привод	Не менее DVD±RW
Графическая подсистема	Встроенная, с поддержкой HD
Звуковая подсистема	Не менее двух встроенных стереодинамиков
Сетевые подключения	Встроенный адаптер Ethernet 10/100/1000 Мбит/с
Слот расширения	Не менее одного порта miniPCIe
Порты подключения периферийных устройств	Не менее 8 портов USB
Устройство ввода	Полноразмерная клавиатура RUS/ENG с цифровым блоком, интерфейс подключения USB
Устройство позиционирования	Оптическая мышь, число кнопок не менее двух, интерфейс подключения USB
Вес	Не более 12кг
Питание	Блок питания мощностью не более 200Вт с сертификатом эффективности не хуже 80 PLUS Gold
Безопасность	Наличие слота для замка Kensington Lock

2.3.2. Требования к сетевому фильтру

Сетевые фильтры должны удовлетворять следующим условиям:

Таблица 11

Параметр	**Требование**
Суммарная мощность нагрузки	Не менее 2кВт
Максимальный ток нагрузки	Не менее 10А
Фильтрация радиочастотных и электромагнитных помех	Да
Номинальное напряжение	220В
Тип вилки	5 шт. Schuko CEE7/4 с заземлением
Длина шнура	Не менее 3м

2.3.3. Требования к принтеру лазерному

Принтеры лазерные должны удовлетворять следующим условиям:

Таблица 12

Параметр	**Требование**
Тип печати	Лазерная, черно-белая
Максимальный формат печати	А4
Автоматическая двухсторонняя печать	Да
Скорость печати	Не менее 24 стр./мин
Интерфейсы подключения	Не хуже USB 2.0 Не хуже Ethernet 10/100
Разрешение печати (точек на дюйм)	Не менее 600x600
Стартовый комплект картриджа	Не менее 1000 стр.
Дополнительный комплект картриджа	Не менее 2000 стр.
Нагрузка	не менее 8000 стр. в месяц
Объем памяти	не менее 32Мб
Расходные материалы	картридж (фотобарабан и тонер – картридж в одном устройстве)

2.3.4. Требования к штрих-кодовому сканеру

Штрих-кодовые сканеры должны удовлетворять следующим условиям:

Таблица 13

Параметр	**Требование**
Тип сканера	Ручной

Параметр	Требование
Максимальное разрешение сканера	Не более 0,102 мм
Максимальная скорость сканирования	Не менее 400 сканирований в секунду
Интерфейс подключения к ПК	USB
Устойчивость к падениям	Высота не менее 1,5м
Обязательное визуальное и звуковое подтверждение правильности чтения штрихового кода	

2.3.5. Требования к термотрансферному принтеру

Термотрансферные принтеры используются для печати самоклеющихся этикеток, и должны удовлетворять следующим условиям:

Таблица 14

Параметр	Требование
Печать	Термотрансферный способ
Язык программирования	ZPL или ZPL 2
Разрешение печати	Не менее 8 точек на мм
Ширина области печати	Не менее 100 мм
Скорость печати	Этикетки годной продукции: не менее 50 мм/сек. Технологические этикетки: не менее 100 мм/сек.
Производительность	Этикетки годной продукции: не менее 70 п.м./день. Технологические этикетки: не менее 450 п.м./день.

Каждый термотрансферный принтер должен быть укомплектован стартовым комплектом расходных материалов. Один комплект расходных материалов должен включать в себя:

1) Самоклеющиеся этикетки размерами не менее 25*50мм в количестве не менее 50 000 штук
2) Самоклеющиеся этикетки размерами не менее 100*100мм в количестве не менее 10 000 штук
3) Термотрансферная лента размерами не менее 60мм*450м в количестве не менее 3 штук
4) Термотрансферная лента размерами не менее 100мм*450м в количестве не менее 3 штук

Самоклеющиеся этикетки должны удовлетворять следующим условиям:

Таблица 15

Параметр	Требование
Материал этикетки	Бумага полуглянцевая
Плотность бумаги, не ниже	80 гр/м2
Толщина бумаги, не менее	0,069 мм
Клей	На резиновой основе
Температурный диапазон использования клея	-40 - +70 0С
Скорость прилипания клея, не более	650 N/m
Температура этикетирования, не ниже	-50 С
Подложка должна быть из суперкаландрированной бумаги с глазированной поверхностью с плотностью	

Параметр	Требование
60 г/м2, толщиной 0,055 мм и прозрачностью 45%.	

Требования к термотрансферной ленте в рулонах (должно соответствовать требованиям выбранного оборудования):

- размеры (диаметр и ширина втулки, внешний диаметр рулона, сторона намотки) должны соответствовать выбранному типу принтера;
- термотрансферная лента должна быть предназначена для печати по бумаге;
- термотрансферная лента должна обеспечивать качественную печать при скоростях печати до 150 мм/сек.

2.3.6. Требования к комплекту средств защиты информации

В качестве средств защиты информации для АРМ типа 3 должны использоваться:

- средства защиты информации от НСД;
- средства антивирусной защиты с бесплатным обновлением баз в течение двух лет;

Предлагаемое к использованию программное обеспечение должно быть лицензионно-чистым.

Решения по использованию средств защиты должны приниматься с учетом обеспечения поддержки его функционирования производителем или распространителем данного ПО.

В процессе эксплуатации СЗПДн права на использование (лицензии) применяемых средств защиты должны поддерживаться в актуальном состоянии.

Программные (программно-аппаратные) средства должны иметь соответствующие сертификаты ФСТЭК и/или ФСБ России, позволяющие их использование для защиты информации в информационных системах персональных данных.

2.3.7. Требования к программному обеспечению общего назначения

В качестве программного обеспечения общего назначения для АРМ типа 3 необходимо предложить лицензированные покупные программные средства:

- операционные системы, совместимые с системой АИСТ;
- пакет офисных приложений для АРМ, совместимый с форматами Microsoft Office (doc, xls, ppt), включая текстовый редактор, электронные таблицы, программу работы с презентациями. Проверка пунктуации русского языка должна выполняться без помощи скачиваемых дополнений. Редактор электронных таблиц в составе офисного пакета должен обладать функциями: "вычислить формулу" (показать этапы вычисления);
- системы управления сохранением и восстановлением данных;
- системы мониторинга и инвентаризации;

2.4.Требования к серверному оборудованию

Комплект должен соответствовать следующим требованиям:

- Функционирование в режиме 24x7;
- Соответствие индустриальным отраслевым стандартам.

Серверное оборудование и АРМ медицинского персонала должны быть объединены в ЛВС.

Защита от сбоев электропитания должна быть реализована с помощью источников бесперебойного питания. ИБП должен обеспечивать мощность нагрузки не менее суммарного значения максимальных потребляемых мощностей защищаемого оборудования.

2.4.1. Требования к серверу

Комплект серверного оборудования должен включать один сервер, удовлетворяющий следующим условиям:

Таблица 16

Параметр	Требования
Форм-фактор	Корпус для напольного размещения
Процессоры	Один процессор с тактовой частотой не ниже 3ГГц на ядро, не менее 4 ядер, кэш третьего уровня не менее 8Мб
Оперативная память	Объем установленной памяти – не менее 8Гб, не менее 4 разъемов для установки памяти типа UDIMM ECC 1600MT/s общим объемом до 32Гб.
Слоты расширения	Не менее 3 слотов PCIe из них: не менее двух x16 электрически и физически, не менее одного x1. Один слот PCI.
Привод для оптических дисков	наличие слота для установки привода оптических дисков
Дисковая система	Возможность установки не менее 6 жестких дисков из них не менее 4 типа LFF. Интерфейс подключения жестких дисков – не хуже SATA I. Должно быть установлено не менее 2 жестких дисков объемом 1Тб и частотой вращения шпинделя 7200 об/мин
Контроллер RAID	Поддержка RAID 0, 1, 5, 10.
Сетевой интерфейс	Встроенный сетевой контроллер 10/100/1000Base-T
Блок питания	Минимальная мощность блока питания – 290Вт.
Модуль управления	Должен иметь совмещенный интерфейс, предоставлять возможность удаленного управления питанием сервера, а также возможность удаленного KVM.

2.4.2. Требования к программному обеспечению общего назначения

В качестве программного обеспечения общего назначения используются лицензированные покупные программные средства:

- Операционная система Microsoft Windows Server 2008R2. В целях обеспечения взаимодействия с системой АИСТ и общесистемными компонентами единой донорской базы не допускается использование эквивалентных операционных систем. Операционная система должна обеспечивать доступ к серверу всем пользователям ЛВС грузополучателей, оснащаемым закупаемыми по данному Техническому заданию персональными компьютерами;
- Программное обеспечение сохранения и восстановления данных для использования на физических и виртуальных серверах под управлением операционных систем Microsoft Windows Server, которые поставляет Поставщик;
- Программное обеспечение мониторинга и инвентаризации для сервера, поставляемого Поставщиком.

Количество и тип поставляемых лицензий на программные средства для сервера Поставщик определяет самостоятельно, в зависимости от предлагаемого им технического решения по размещению виртуальных серверов таким образом, чтобы выполнялись основные информационные серверные роли (служба каталога, подсистема сохранения и восстановления данных, подсистема мониторинга и инвентаризации, сервер приложения АИСТ) и обеспечивалось их непрерывное функционирование в рамках объектов Грузополучателей.

2.4.3. Требования к средствам защиты информации

В качестве средств защиты информации должны использоваться:

- средства защиты информации от НСД;
- программные (программно-аппаратные) средства аутентификации пользователей;
- средства межсетевого экранирования;
- средства антивирусной защиты;

Предлагаемое к использованию программное обеспечение должно быть лицензионно-чистым.

Решения по использованию средств защиты должны приниматься с учетом обеспечения поддержки его функционирования производителем или дистрибутором данного ПО.

В процессе эксплуатации СЗПДн права на использование (лицензии) применяемых средств защиты должны поддерживаться в актуальном состоянии.

Программные (программно-аппаратные) средства должны иметь соответствующие сертификаты ФСТЭК и/или ФСБ России, позволяющие их использование для защиты информации в информационных системах персональных данных.

2.4.4. Архитектура единого информационно-технологического пространства

2.4.4.1. Требования к службе каталога

В ходе выполнения работ Поставщик должен создать на объектах Грузополучателей службы каталога, включив в нее все закупаемые на объекты Грузополучателей по настоящему Техническому заданию АРМ и сервера.

Поставщик должен обеспечить преемственность результата работ по созданию единой службы каталогов Грузополучателей, выполняемых по настоящему Техническому заданию, с существующей единой службой каталогов Службы Крови, обладающей следующими характеристиками:

- Хранение до 100.000 (ста тысяч) объектов.
- Обслуживание до 10.000 (десяти тысяч) пользователей с ежегодным приростом количества пользователей приблизительно в 20% (двадцать процентов).
- Обеспечение распределённого хранилища каталога.
- Распределение объектов по отдельным контейнерам с целью их упорядочивания или разграничения полномочий.
- Обеспечение независимости от изменений в организационной структуре Службы Крови.
- Сохранение работоспособности при выходе из строя одного или нескольких из поддерживающих его работу серверов.
- Обеспечение сервиса глобального каталога.
- Обеспечение навигации и поиска по каталогу.
- Обеспечение бесперебойной работы в среде с межсетевыми экранами.
- Обеспечение возможности изменения набора атрибутов объектов каталога.
- Обеспечение возможности надёжной аутентификации пользователей и динамического и целостного управления правами доступа к объектам.
- Обеспечение защиты от несанкционированного доступа к данным каталога.
- Обеспечение сервиса разрешения доменных имён (DNS).
- Обеспечение сервиса автоматического управления и назначения адресов (DHCP).
- Обеспечение сервиса сетевого времени (NTP).

По результату выполнения работ Поставщик должен предоставить Заказчику документ «Пояснительная Записка по Службе Каталога» с описанием полученной в ходе выполнения работ архитектуры единой службы каталогов, включающие в себя следующие разделы:

- Описание сервиса разрешения имен (DNS).
- Описание сервиса автоматической конфигурации IP адресов (DHCP).
- Описание сервиса сетевого времени (NTP).
- Логические схемы организации Службы Каталога Active Directory Грузополучателей.

- Дополнения соглашения по именованию объектов в Службе Каталога.
- Описание физических объектов Службы Каталогов.
- Описание ролевой модели и модели делегирования полномочий в Службе Каталога.
- Описание необходимых Групповых Политик Безопасности в Службе Каталога.
- Описание интеграции, и шаблонов безопасности для серверов баз данных и серверов приложений в Службе Каталога.
- Описание метода, обеспечивающего надежность организации единого информационно-технологического пространства.

2.4.4.2. Требования к подсистеме сохранения и восстановления данных

Поставщик должен создать подсистему сохранения и восстановления данных на АРМ и серверах, поставляемых на объекты Грузополучателей, в соответствии со следующими требованиями:

- Полное восстановление "образа" сервера или АРМ.
- Интегрированная защита данных.
- Поддержка виртуальных сред VMware vSphere/ESX/ESXi, Microsoft Hyper-V™, Citrix XenServer, Red Hat® Enterprise Virtualization и Parallels Server 4.
- Возможность каталогизации резервных копий с функциями поиска.
- Поддержка дисковых, ленточных и облачных хранилищ.
- Поддержка до пяти мест хранения резервных копий. Дополнительная защита данных за счет хранения резервных копий в нескольких местах.
- Зона безопасности. Специальный защищенный раздел на жестком диске для хранения резервных копий.
- Резервное копирование по расписанию и по событию с поддержкой условий.

По результату выполнения работ Поставщик должен предоставить Грузополучателю документ «Пояснительная Записка по подсистеме сохранения и восстановления данных (подсистеме резервного копирования)».

2.4.4.3. Требования к подсистеме мониторинга и инвентаризации

В целях обеспечения сервисной поддержки информационной системы Грузополучателю из Единого информационного центра Службы Крови, Поставщик должен развернуть на АРМ и серверах Грузополучателей подсистему мониторинга и инвентаризации, которая должна обладать следующими функциональными возможностями:

- Интеграция между всеми компонентами подсистемы
- Интеграция со Службой Каталога Active Directory
- Инвентаризация аппаратного и программного обеспечения
- Автоматизированное развертывание Программного Обеспечения
- Управление обновлениями Программного Обеспечения
- Мониторинг использования Программного Обеспечения
- Мониторинг конфигураций
- Развертывание операционных систем Microsoft Windows
- Удаленное управление
- Система должна управлять стационарными АРМ в предзагрузочной среде
- Управление виртуализированным программным обеспечением
- Мониторинг состояния оборудования
- Мониторинг состояния здоровья серверов и приложений
- Мониторинг Базовых Информационных Сервисов
- Возможность изменения, создания собственных «Пакетов Управления и Мониторинга»

- Встроенная «База Знаний» с рекомендацией разработчиков по устранению проблем в инфраструктуре
- Возможность автоматического наполнения конфигурационной базы данных, используя учетную информацию из Службы Каталога
- Подсистема подготовки отчетов по состоянию работоспособности, доступности инфраструктуры

По результату выполнения работ Поставщик согласовывает и передает Грузополучателю документ «Пояснительная Записка по подсистеме мониторинга и инвентаризации» с описанием архитектуры системы.

2.5. Требования к источникам бесперебойного питания (ИБП)

2.5.1. Требования к ИБП для АРМ тип 1, 2, 3

Источники бесперебойного питания для персональных компьютеров тип 1, 2, 3 должны удовлетворять следующим условиям:

Таблица 17

Параметр	**Требования**
Топология	Линейно-интерактивная («Line-interactive»)
Максимальная выходная мощность	Не менее 1100 ВА / 660 Вт
«Холодный старт»	Поддерживается (возможность запуска ИБП для питания нагрузки при отсутствии входного напряжения)
Диапазон входного напряжения при работе от сети	Нижняя граница – 180В или меньше, верхняя граница – 240В или больше
Выходные соединения	Не менее 4 (четырех) разъемов IEC 320 C13 с функцией батарейной поддержки и защиты от перенапряжения
Время автономной работы при полной нагрузке	Не менее 2,5 мин
Время автономной работы при половинной нагрузке	Не менее 10 мин
Время перезарядки батарей	Не более 24 часов
Входная частота	47 - 63 Гц

2.5.2. Требования к ИБП для серверного оборудования

Поставщик должен выполнить поставку источника бесперебойного питания, удовлетворяющего следующим условиям:

Таблица 18

Параметр	**Требования**
Форм-фактор	Корпус для напольного размещения
Топология	Линейно-интерактивная («Line-interactive»)
Максимальная выходная мощность	Не менее 1000 Вт
«Холодный старт»	Поддерживается (возможность запуска ИБП для питания нагрузки при отсутствии входного напряжения)

Параметр	Требования
Форм-фактор	Корпус для напольного размещения
Диапазон входного напряжения при работе от сети	Нижняя граница – 200В или меньше, верхняя граница – 240В или больше
Выходные соединения	8 (восемь) разъемов IEC 320 C13 с функцией батарейной поддержки и защиты от перенапряжения
Время автономной работы при полной нагрузке	Не менее 5 мин
Время автономной работы при половинной нагрузке	Не менее 14 мин
Время перезарядки батарей	Не более 24 часов

2.5.3. Требования к ИБП для настенного шкафа

Источник бесперебойного питания для настенного шкафа используется в настенном телекоммуникационном шкафу, и предназначен для обеспечения бесперебойного электропитания сетевого коммутатора и маршрутизатора.

ИБП для настенного шкафа должен удовлетворять следующим условиям:

Таблица 19

Параметр	Требования
Топология	Линейно-интерактивная («Line-interactive»)
Максимальная выходная мощность	Не менее 1100 ВА / 660 Вт
«Холодный старт»	Поддерживается (возможность запуска ИБП для питания нагрузки при отсутствии входного напряжения)
Диапазон входного напряжения при работе от сети	Нижняя граница – 180В или меньше, верхняя граница – 240В или больше
Выходные соединения	Не менее 4 (четырех) разъемов IEC 320 C13 с функцией батарейной поддержки и защиты от перенапряжения
Время автономной работы при полной нагрузке	Не менее 2,5 мин
Время автономной работы при половинной нагрузке	Не менее 10 мин
Время перезарядки батарей	Не более 24 часов
Входная частота	47 - 63 Гц

2.6. Заземление

Грузополучатели обеспечивают наличие на объекте действующего аттестованного контура заземления с сопротивлением токам растекания не более 4 Ом, соответствующего следующим нормативным документам ANSI/TIA/EIA-607 и требованиям ГОСТ 12.1.030-81 ССБТ, ГОСТ 464-79, ГОСТ Р 50571.10-96 (МЭК 364-5-54-80), ГОСТ Р 50571.21-2000 (МЭК 60364-5-548-96), ГОСТ Р 50571.22-2000 (МЭК 60364-7-707-84), ГОСТ Р 50571.2-94 в части обязательного исполнения требований, установленных действующим законодательством.

2.7. Требования к комплекту оборудования для создания инфраструктуры

Для создания инфраструктуры локальной вычислительной сети на объектах Грузополучателей Поставщик поставляет и выполняет пуско-наладку сетевого оборудования, климатического оборудования серверной, а также поставляет комплект расходных материалов и создает СКС, в соответствии с требованиями, перечисленными ниже.

2.7.1. Активное сетевое оборудование

2.7.1.1. Требования к маршрутизатору

Маршрутизатор должен удовлетворять следующим условиям:

Таблица 20

Параметр	Требования
Архитектура	Модульная
Порты Ethernet	Не менее двух 10/100/1000Мбит/с
Маршрутизация	Поддержка статической, RIPv1 и RIPv2 маршрутизации, OSPF, а также маршрутизации multicast-трафика (PIM, DVMRP, IGMP snooping)
Безопасность	Поддержка протокола 802.1x, списки доступа для трафика, коммутируемого на втором уровне (VLAN ACL), на третьем и четвертом уровнях (Router ACL), а также Port-based ACLs (PACL) и Time-based ACL. Для обеспечения безопасности при администрировании необходима поддержка протоколов SSH и SNMPv3, а также централизованная аутентификация на TACACS+ и RADIUS серверах
Поддержка протоколов FHRP	Требуется
Поддержка технологии VPN	Да, возможностью резервирования VPN туннелей
Модули расширения	Не менее двух
Служебные USB-порты	Не менее одного
Оперативная память	Не менее 480Мб
Монтаж	На стену или в стандартную стойку 19”
Прочее	Расширение возможностей ПО маршрутизатора должно производиться без перерыва в работе

2.7.1.2. Требования к сетевому коммутатору

Сетевой коммутатор локальной сети должен удовлетворять следующим условиям:

Таблица 21

Параметр	Требования
Порты Ethernet	Не менее двадцати четырех 10/100/1000Мбит/с
Порты SFP	Не менее четырех
Поддержка протоколов	IEEE 802.1q, IEEE 802.1p, IEEE 802.1d, IEEE 802.1X; SSH и SNMP v3
Маршрутизация	Поддержка статической маршрутизации
Поддержка списков контроля доступа (ACL)	Требуется

Параметр	Требования
Матрица коммутации	не менее 88 Гбит/с
Количество поддерживаемых MAC-адресов	Не менее 8 000
Поддержка качества обслуживания	Классификация трафика по полям DSCP или 802.1p (CoS), стандартные и расширенные списки доступа для выделения заданного типа трафика, WRED, очередность Strict Priority, Shaped Round Robin. Возможность определения максимальной полосы для определенного вида трафика, а также выделения гарантированной полосы CIR
Возможность объединения в стек (опционально)	Требуется
Монтаж	В стандартную стойку 19”

2.7.2. Требования к комплекту климатического оборудования

Каждый комплект климатического оборудования, поставляемый Поставщиком Грузополучателям, должен включать в себя:

- Внутренний блок кондиционера 2 шт.
- Внешний блок кондиционера 2 шт.
- Согласователь работы кондиционеров 1 шт.
- Устройство электрообогрева дренажа 4 шт.
- Помпа дренажная 2 шт.
- Комплект материалов для монтажа кондиционеров 1 шт.

Климатические агрегаты должны удовлетворять следующим условиям:

Таблица 22

Параметр	Требования
Тип климатического агрегата	Сплит-система
Мощность охлаждения	Не менее 2,5кВт
Электропитание	1 фазный, 220/230/240В 50Гц
Максимальная длина трубопровода / перепад высот между блоками	25 / 15 м
Хладагент	R 410 A
Рабочий диапазон наружных температур при охлаждении	Нижняя граница диапазона -30°C или ниже, верхняя граница диапазона +30°C или выше
Воздушный фильтр	Фотокаталитический моющийся дезодорирующий

2.7.3. Требования к комплекту материалов СКС

Для построения СКС на объектах Грузополучателей Поставщик должен поставить комплект материалов СКС, в количестве и по номенклатуре Приложения 1. Поставляемый Поставщиком комплект материалов должен быть достаточным для построения локальной сети объектов Грузополучателей без увеличения номенклатуры или количества материалов, и быть достаточным для подключения в локальную сеть всего поставляемого по настоящему Техническому заданию на объекты Грузополучателей компьютерного и сетевого оборудования с лицензионным программным обеспечением.

2.7.3.1. Требования к настенному шкафу

Настенный шкаф используется для размещения сетевого оборудования, и должен удовлетворять следующим требованиям:

Таблица 23

Параметр	**Требования**
Ширина-Глубина-Высота, мм	Не менее 650х650х550 (9U)
Степень защиты	Не менее IP20
Допустимая статичная нагрузка	Не менее 60 кг
Поставка	В разобранном виде, в заводской упаковке
Передняя дверь	Стеклянная дверь
Задняя дверь	нет
Прочие	Глухие боковые панели, кабельные вводы в крыше и/или днище шкафа, комплект для заземления шкафа, не менее 2 вентиляторов, не менее 1 кабельный организатор 19” 1U с металлическими кольцами, не менее 1 патч-панель 19” не менее 24 порта RJ45 кат.5е

2.7.4. Общие требования к структурированной кабельной системе

Кабельная система, которую создает Поставщик на объектах Грузополучателей из поставляемого по настоящему Техническому заданию комплекта расходных материалов для подключения поставляемого по настоящему Техническому заданию компьютерного и сетевого оборудования с лицензионным программным обеспечением, должна соответствовать требованиям стандартов ISO 11801 Edition 2 for Category 5e/Class 5D, ANSI/TIA 568-C.2 на основе неэкранированной витой пары категории 5е. Тракт СКС должен обеспечивать работоспособность на частоте вплоть до 100МГц.

Согласно ГОСТ 53315—2009 дополнительно должен быть обеспечен класс пожаробезопасности оболочек кабелей, проводов и шнуров не ниже П.1.8.1.2.1, что соответствует типу оболочек не ниже LSZH.

СКС должна быть построена по принципу «иерархическая звезда», с соблюдением ограничений стандартов на длины кабелей и способов их прокладки.

В зоне рабочих мест кабели СКС прокладывать в многосекционных ПВХ кабельных каналах (коробах) сечением не менее 110х50 мм. Коэффициент использования площади поперечного сечения короба не должен превышать 50%. Розетки монтировать внутрь короба. Короба устанавливать на высоте 800 мм от пола (за исключением специальных случаев, например, обхода капитальных конструкций здания, монтажа внутри мебели). Расположение, конструкция и монтаж горизонтальных трасс должны соответствовать нормам ОСТН-600-93 и ANSI/TIA/EIA-569. Конструкция лотков должна предусматривать меры против скопления влаги (уклон, перфорация и т.п.).

Тестирование линий СКС выполнять тестерами на соответствие корректности физической разводки (Wire Map). Тестирование кабельных линий выполнять на соответствие стандарту ANSI/TIA-568B.

Маркировка элементов кабельной системы должна выполняться в соответствии с требованием стандарта ANSI/TIA/EIA 606 и быть устойчивой к внешним воздействиям. Идентификаторы и записи применяются по отношению к следующим элементам кабельной инфраструктуры: кабелям; коммутационному оборудованию; коннекторам коммутационного оборудования; трассам; помещениям. Окончательную систему маркировки согласовать с Грузополучателем на этапе выполнения строительно-монтажных работ.

3. Технические требования к СЗПДн

Создаваемая система защиты персональных данных должна соответствовать требованиям Приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Архитектура СЗПДн в совокупности с механизмом поддержки функциональных подсистем не должна накладывать каких-либо существенных ограничений на информационные технологии, используемые в ИС.

Архитектура СЗПДн должна обеспечивать реализацию функций безопасности на всех технологических этапах эксплуатации ИС, в том числе при проведении технического обслуживания и ремонта.

Эффективность СЗПДн должна достигаться комплексным применением различных средств и методов.

СЗПДн в комплексе с организационно-техническими мероприятиями по защите ПДн от утечки по техническим каналам должны обеспечить безопасность персональных данных при их обработке в ИСПДн.

Требования по организации физической защиты ПДн в данном документе не предъявляются.

3.1. Серверная часть

1) Средства защиты информации от несанкционированного доступа к информации, сертифицированные ФСТЭК России по классу не ниже 5-го класса средств вычислительной техники в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к информации (РД АС). Гостехкомиссия (ФСТЭК) Россия, 1992, которые могут использоваться для защиты информации в информационных системах персональных данных и выполняющие следующие функции:

- идентификация и аутентификация пользователя при входе в операционную систему;
- возможность применения механизмов дискреционного принципа доступа;
- блокировка системы при заданном количестве неудачных попыток ввода идентификатора и пароля при входе в систему;
- блокирование доступа к СВТ при превышении установленного интервала времени неактивности данного СВТ;
- идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- контроль доступа пользователей к периферийным устройствам;
- динамическая и статическая блокировка доступа к внешним устройствам.
- регистрацию входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова;
- регистрацию выдачи печатных (графических) документов на бумажный носитель;
- регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;
- регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрацию попыток доступа программных средств к дополнительным защищаемым объектам доступа;
- очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей;
- периодическое тестирование целостности компонент (системных файлов) – при входе пользователя и/или загрузке системы и далее периодически в процессе функционирования системы;
- возможность экспорта/импорта настроек для быстрого восстановления системы в случае сбоев или отказов системы.

2) Средство антивирусной защиты, сертифицированное ФСТЭК России не ниже 4-го класса антивирусных средств в соответствии требованиями к средствам антивирусной защиты по профилю защиты типа Б, которое может использоваться для защиты информации в информационных системах персональных данных.

3) Программное средство, реализующее функции резервного копирования и надежного восстановления информации, которое может использоваться для защиты информации в информационных системах персональных данных.

3.2. Клиентская часть (персональные компьютеры)

1) Средства защиты информации от несанкционированного доступа к информации, сертифицированные ФСТЭК России по классу не ниже 5-го класса средств вычислительной техники в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к информации (РД АС). Гостехкомиссия (ФСТЭК) Россия, 1992 , которые могут использоваться для защиты информации в информационных системах персональных данных и выполняющие следующие функции:

- идентификация и аутентификация пользователя при входе в операционную систему;
- возможность применения механизмов дискреционного принципа доступа;
- блокировка системы при заданном количестве неудачных попыток ввода идентификатора и пароля при входе в систему;
- блокирование доступа к СВТ при превышении установленного интервала времени неактивности данного СВТ;
- идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- контроль доступа пользователей к периферийным устройствам;
- динамическая и статическая блокировка доступа к внешним устройствам.
- регистрацию входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова;
- регистрацию выдачи печатных (графических) документов на бумажный носитель;
- регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;
- регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрацию попыток доступа программных средств к дополнительным защищаемым объектам доступа;
- очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей;
- периодическое тестирование целостности компонент (системных файлов) – при входе пользователя и/или загрузке системы и далее периодически в процессе функционирования системы;
- возможность экспорта/импорта настроек для быстрого восстановления системы в случае сбоев или отказов системы;

2) Средство антивирусной защиты, сертифицированное ФСТЭК России не ниже 4-го класса антивирусных средств в соответствии требованиями к средствам антивирусной защиты по профилю защиты типа В и Г, которое может использоваться для защиты информации в информационных системах персональных данных.

3.3. Для использования на объекте Грузополучателей

Программное (программно-аппаратное) средство защиты информации Vipnet, сертифицированное ФСТЭК России и ФСБ России, которое может использоваться для защиты информации в информационных системах персональных данных, обеспечивающее:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- защиту информации при ее передаче по каналам связи.

В целях обеспечения взаимодействия с используемыми в едином информационном пространством Службы крови Российской Федерации средствами защиты информации не допускается использование эквивалентных средств защиты информации.

4. Требования к содержанию и выполнению работ

4.1. Перечень работ по вводу в эксплуатацию

На объекте Грузополучателей Поставщик должен выполнить следующие комплексы работ:

- Внедрение и пуско-наладка компьютерного и сетевого оборудования с лицензионным программным обеспечением;
- Внедрение и пуско-наладка технологического программного обеспечения (АИСТ).

4.2. Требования к работам по внедрению и пуско-наладке компьютерного и сетевого оборудования с лицензионным программным обеспечением

В состав работ внедрению и пуско-наладке компьютерного и сетевого оборудования с лицензионным программным обеспечением входит:

1) Доставка компьютерного и сетевого оборудования с лицензионным программным обеспечением до места эксплуатации по адресу Грузополучателей;
2) Проведение разгрузочных работ при доставке компьютерного и сетевого оборудования с лицензионным программным обеспечением на объекте Грузополучателей;
3) Складирование компьютерного и сетевого оборудования с лицензионным программным обеспечением на объекте в согласованном с уполномоченным лицом Грузополучателей помещении, соответствующем требованиям по сохранности и защищенности хранимого компьютерного и сетевого оборудования с лицензионным программным обеспечением;
4) Оформление бухгалтерских документов на поставленное компьютерное и сетевое оборудование с лицензионным программным обеспечением (перечень документов определяется Государственным контрактом);
5) Извлечение компьютерного и сетевого оборудования с лицензионным программным обеспечением из упаковочной транспортной тары;
6) Перемещение использованной упаковки от компьютерного и сетевого оборудования с лицензионным программным обеспечением из помещений объекта Грузополучателей в мусорные контейнеры;
7) Размещение компьютерного и сетевого оборудования с лицензионным программным обеспечением на согласованных с уполномоченным лицом Грузополучателей местах в помещениях объекта информатизации. При этом Поставщик не несет ответственности и финансовых расходов за хранение доставленного на склад Грузополучателей оборудования и программного обеспечения. Грузополучатель обеспечивает хранение оборудования и программного обеспечения до начала установки таким образом, чтобы предотвратить любые возможности краж или порчи;
8) Проведение монтажных работ по созданию на объектах Грузополучателей структурированной кабельной системы, включая согласование с уполномоченным лицом Грузополучателей мест размещения сетевых узлов локальной вычислительной сети (настенных шкафов)
9) Монтаж компьютерного и сетевого оборудования с лицензионным программным обеспечением, поставляемого по настоящему Техническому заданию на объект информатизации;
10) Пусконаладка компьютерного и сетевого оборудования с лицензионным программным обеспечением, поставляемого по настоящему Техническому заданию на объект Грузополучателей;
11) Настройка компьютерного и сетевого оборудования с лицензионным программным обеспечением, поставляемого по настоящему Техническому заданию на объект Грузополучателей;
12) Настройка телекоммуникационного оборудования и каналов связи в объеме, необходимом для организации возможности осуществления передачи данных из ИС АИСТ Грузополучателей в ЕИЦ, а также удаленного администрирования АРМов и серверного оборудования из Единого информационного центра ФГБУЗ «Центр крови» ФМБА России. Настройка производится в отношении поставляемого Поставщиком по настоящему Техническому заданию активного сетевого оборудования и программного (программно-аппаратного) средства защиты информации Vipnet, используемого для межсетевого экранирования и защиты информации при ее передаче по каналам связи. Работы включают в себя подключение к оборудованию провайдера связи, размещенном в «точке присутствия» на объекте Грузополучателей, и обеспечение возможности передачи данных до истечения срока поддержки эксплуатации;
13) Создание информационных сервисов на объекте Грузополучателей в соответствии с требованиями, описанными в разделе 2 настоящего Технического задания;

14) Установка и настройка средств защиты информации, поставляемых по настоящему Техническому заданию;
15) Обеспечение информационного взаимодействия между информационной системой Грузополучателей и ЕИЦ с соблюдением требований Указа Президента РФ от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";
16) Подготовка организационно-распорядительной документации и аттестация объекта Грузополучателей на соответствие требованиям безопасности информации, во взаимодействии с уполномоченными лицами Грузополучателей;
17) Оформление актов выполненных работ.

4.3. Требования к внедрению и пуско-наладке технологического программного обеспечения (АИСТ)

Поставщик осуществляет работы во взаимодействии с уполномоченным лицом Грузополучателей (главный врач, заведующий СПК или иное должностное лицо, обладающее соответствующими полномочиями).

Поставщик проводит установку и настройку системы АИСТ на персональных компьютерах пользователей и сервере приложений, поставляемых им по настоящему Техническому заданию, а также:

- оказывает консультационные услуги по подготовке и вводу данных для обеспечения функционирования системы АИСТ на объектах эксплуатации и в едином информационном центре;
- оказывает консультационные услуги по подготовке и вводу данных при инструктаже и консультировании Пользователей, в том числе удаленно из ЕИЦ.
- осуществляет перенос данных (при необходимости и при условии их предоставления Поставщику Грузополучателем (объектом информатизации) с описанием структуры данных в течение не более чем 30 календарных дней с даты заключения Контракта) АИС, используемой на объекте информатизации, в систему АИСТ, внедряемую в рамках выполняемых по настоящему Техническому заданию работ. Оказание консультационной поддержки по внедрению специалистам Поставщика будет осуществляться представителем Грузополучателей посредством телефонной связи и/или электронной почты. Корректность результатов переноса данных оценивается рабочей группой, состоящей из представителей Поставщика и представителей объекта информатизации, и закрепляется отметкой в акте выполненных работ;
- Обеспечивает настройку справочников системы для локализации технологического процесса.

Поставщик проводит настройку передачи данных между каждым объектов Грузополучателей СПК (ОПК) и РИЦ соответствующего СПК (ОПК). Грузополучатель должен обеспечить физический доступ представителей поставщика на объект.

4.4. Требования по обеспечению передачи данных из АИСТ Грузополучателя в Единую информационную базу данных.

Поставщик должен обеспечить передачу данных из ПО АИСТ Грузополучателей в Единую информационную базу данных, используя информационное взаимодействие объектов Службы крови России.

4.5. Требования к составу передаваемых данных в ЕИБД.

Поставщик должен обеспечить передачу следующей информации из ПО АИСТ Грузополучателей в Единую Информационную Базу Данных (ЕИБД):

- информация о доноре:
  - ФИО;
  - пол;
  - дата рождения;
  - паспортные данные;

- адрес регистрации;
- адрес фактического проживания;
- место работы;
- группа крови;
- резус;
- kell;
- фенотип;
- титры антител;
- примечания;

- информация об отводах:
  - тип отвода;
  - дата, когда отвод был выставлен;
  - код учреждения, которым был поставлен отвод;
  - дата, когда отвод был снят;
  - название учреждения, которым был снят отвод;
- информация о врачебных осмотрах:
  - информация о доноре;
  - дата осмотра;
  - результаты осмотра;
- информация о донациях:
  - уникальный код донации ;
  - дата донации;
  - тип донации;
  - данные о реципиенте (если известен);
  - объем компонента (в мл. дозах), объем крови для анализов;
  - осложнения (если есть);
  - информация об оплате.
- информация об анализах:
  - вид анализов (гематологический/серологический/биохимический);
  - уникальный код пробы;
  - дата проведения анализа;
  - тип анализа;
  - значения анализа;
  - место проведения анализа;
  - информация о запасах на карантине:
  - дата снятия остатков;
  - тип компонента;
  - группа крови;
  - резус;
  - общий объем компонента;
  - общее количество контейнеров с компонентом;
  - объем карантинизированных компонентов;
  - количество карантинизированных контейнеров с компонентом.
- информация об остатках в экспедиции:
  - дата снятия остатков;
  - тип компонента и препарата;
  - группа крови;

- резус;
- общий объем компонента ;
- общее количество контейнеров компонентов продукции;

- информация о выдаче из экспедиции:
  - дата выдачи;
  - уникальный код контейнера
  - тип компонента ;
  - получатель.
  - данные о подборе компонента.

Для соблюдения формата передачи данных Поставщик должен использовать в качестве средства передачи данных специализированный модуль ПО АИСТ (АРМ «Сервер ОПК»).

4.6. Требования к частоте передачи данных в ЕИБД.

Поставщик должен обеспечить передачу данных из ПО АИСТ Грузополучателей в Единую информационную базу данных информации с частотой 1 (одна) передача данных в 15 минут или чаще.

4.7. Требования к мониторингу передачи данных в ЕИБД

Поставщик должен осуществлять мониторинг передачи данных для всех объектов Грузополучателей.

Поставщик круглосуточно должен предоставлять Грузополучателю возможность получения информации о состоянии передачи данных и информации, поступающей из АИС Грузополучателя в ЕИБД.

4.8. Консультационные услуги по подготовке и вводу данных для обеспечения функционирования системы АИСТ на объектах эксплуатации и в едином информационном центре.

Поставщик должен обеспечивать поддержку эксплуатации системы АИСТ на объектах, в том числе:

- осуществлять мониторинг функционирования системы АИСТ на следующих рабочих местах пользователей, включая взаимодействие с удаленными источниками информации:

1. Регистратура (регистрации и использование данных о донорах и донорских отводах).
2. Предварительное обследование донора (ввод результатов предварительных исследований).
3. Врач (ведение электронных карт доноров, запись в них результатов осмотра доноров и назначений).
4. Отдел заготовки крови и ее компонентов (регистрация эксфузий, регистрация пробирок и контейнеров с плазмой, тромбоцитами).
5. Переработка (регистрация компонентов крови).
6. Выездная бригада (проверка по базе отведенных от донорства доноров, регистрация доноров, регистрация донаций на выезде).
7. Касса, справки (формирование и печать справок о сдаче крови/плазмы, индивидуальных и суточных ведомостей о выплатах).
8. Склад неапробированной продукции, Выбраковка, Этикетировка.
9. Карантинизация плазмы.
10. Криобанк (долговременное хранение эритроцитов с редкими группами крови).
11. Иммунологические исследования (ввод результатов исследования крови донора на маркеры гемотрансмиссивных инфекций).
12. Биохимические исследования (ввод результатов биохимических исследований крови донора).
13. Иммуногематологические исследования (исследование крови реципиента и индивидуальный подбор доноров).
14. Гематологические исследования (антигенные характеристики эритроцитов крови).
15. Экспедиция (прием и учет продукции, заявок от ЛПУ, выдача компонентов крови в ЛПУ).
16. Единый донорский центр (организация обмена данными между учреждениями, прием и обработка данных о лицах с абсолютными противопоказаниями к донорству, ведение баз данных о деятельности других ОПК, СПК в регионе).
17. Почетный донор России (подготовка списков доноров для передачи в вышестоящие органы для награждения, ежегодная сверка списков).
18. Производство криопреципитата, отмытых эритроцитов и вирусинактивация компонентов.

19. Врач-эпидемиолог.
20. Аутодонор.
21. Главный врач.
22. Печать технологических штрих-кодовых этикеток.
23. Регистратура и ведение карты больного во внешнем источнике данных для ЕДЦ (с локализацией по профилю). Для организаций, выявляющих лиц, которые по состоянию здоровья не могут быть донорами (КВД, центр СПИД, туберкулезный диспансер, наркологический диспансер, психоневрологический диспансер, учреждения Роспотребнадзора).

- в случае выявления нарушений или неисправностей в работе АИСТ принимать меры по устранению данных нарушений и неисправностей;
- осуществлять резервное копирование и индексирование баз данных в соответствии с согласованным регламентом;
- выполнять работы по восстановлению функционирования системы АИСТ после аварийных ситуаций, обеспечивать восстановление баз данных АИСТ из резервной копии; выверку и восстановление ссылочной целостности данных;
- выполнять работы по локализации неисправностей технических средств;
- осуществлять контроль работы телекоммуникационных систем системы обмена данными для информационного взаимодействия с единым информационным центром;
- участвовать в разборе нестандартных ситуаций, возникающих при отражении в системе движения объектов по технологическому циклу (либо при его нарушениях) и готовить предложения по доработке программного обеспечения;
- консультационные услуги по подготовке и вводу данных при инструктаже и консультировании Пользователей, в том числе удаленно из ЕИЦ.

4.9. Консультационные услуги из единого информационного центра по информационному обеспечению удаленного мониторинга и администрирования программного обеспечения на местах.

Проведение мониторинга работоспособности всей инфраструктуры и удаленное администрирование должны выполняться в режиме односменной работы и включать в себя:

- восстановление работоспособности общесистемного программного обеспечения и системы АИСТ;
- поддержку актуальности общесистемного программного обеспечения и системы АИСТ;
- проверку правильности эксплуатации системы АИСТ и поддержку ее эффективного использования на объекте Грузополучателей;
- обеспечение консультаций и поддержки пользователей системы АИСТ на АРМ информационной системы Грузополучателей;
- участие в разборе нестандартных ситуаций возникающих на объектах Грузополучателей;
- оперативную корректировку неверных данных и генерации отчетов.

4.10. Консультационные услуги по подготовке и вводу данных при инструктаже и консультировании Пользователей, в том числе удаленно из ЕИЦ.

Инструктаж Пользователей производится Поставщиком во всех необходимых случаях: обновление персонала, внутренние переводы персонала, изменение должностных обязанностей и др. по указанию Пользователя.

Инструктаж Пользователей на рабочих местах (в технологической цепи) проводится Поставщиком в объеме достаточном для последующей самостоятельной работы персонала Пользователя.

Консультирование персонала Пользователя должно выполняться как силами обслуживающего персонала Поставщика на месте эксплуатации, так и удаленно, силами дежурного персонала Поставщика.

4.11. Обеспечение функционирования программного обеспечения общего назначения для АРМ

Необходимо осуществлять техническую поддержку следующего программного обеспечения общего назначения (лицензированных программных средств) и служб:

- операционных систем;

- систем управления сохранением и восстановлением данных;
- средств защиты информации от несанкционированного доступа;
- пакетов офисных приложений для АРМ;
- систем мониторинга и инвентаризации;
- антивирусного программного обеспечения;
- службы единого каталога.

4.12. Техническая поддержка системы защиты информации

4.12.1. Серверная часть

В целях поддержки программно-аппаратных средств в состоянии, наиболее точно соответствующем предъявляемым к СЗПДн требованиям, преодоления нештатных ситуаций, ликвидации последствий в оговоренные сроки с заданным уровнем качества необходимо осуществлять техническую поддержку следующих средств СЗПДн на сервере:

1) Средств защиты информации от несанкционированного доступа к информации.
2) Средств антивирусной защиты.
3) Программных средств, реализующих функции резервного копирования и надежного восстановления информации.

Режим оказания технической поддержки - 5 x 8 x NBD:

- 5 дней в неделю, 8 часов в день (исключая праздничные и выходные дни);
- время реакции — не позже следующего рабочего дня;
- график работы — 08:00–18:00 с понедельника по пятницу, исключая праздничные и выходные дни (часовой пояс поставщика ПО).

Способ оказания технической поддержки:

- по телефону разработчика или дистрибутора ПО;
- по e-mail разработчика или дистрибутора ПО;
- на объекте защиты ПДн Грузополучателей (по предварительной договоренности).

4.12.2. Клиентская часть и отдельные АРМ

В целях поддержки программно-аппаратных средств в состоянии, наиболее точно соответствующем предъявляемым к СЗПДн требованиям, преодоления нештатных ситуаций, ликвидации последствий в оговоренные сроки с заданным уровнем качества необходимо осуществлять техническую поддержку следующих средств СЗПДн на АРМ:

1. Средств защиты информации от несанкционированного доступа к информации.
2. Средств антивирусной защиты.
3. Программных средств, реализующих функции резервного копирования и надежного восстановления информации.

Режим оказания технической поддержки - 5 x 8 x NBD:

- 5 дней в неделю, 8 часов в день (исключая праздничные и выходные дни);
- время реакции — не позже следующего рабочего дня;
- график работы — 08:00–18:00 с понедельника по пятницу, исключая праздничные и выходные дни (часовой пояс поставщика ПО).

Способ оказания технической поддержки:

- по телефону разработчика или дистрибутора ПО;
- по e-mail разработчика или дистрибутора ПО;
- на объекте защиты ПДн Грузополучателей (по предварительной договоренности).

4.12.3. Техническая поддержка прочих программных средств

В целях поддержки программно-аппаратных средств в состоянии, наиболее точно соответствующем предъявляемым к СЗПДн требованиям, преодоления нештатных ситуаций, ликвидации последствий в оговоренные сроки с заданным уровнем качества необходимо осуществлять техническую поддержку следующих средств СЗПДн:

1) Программных (программно-аппаратных) средств обеспечивающих:

- межсетевое экранирование;
- защиту информации при ее передаче по каналам связи.

Режим оказания технической поддержки - 5 x 8 x NBD:

- 5 дней в неделю, 8 часов в день (исключая праздничные и выходные дни);
- время реакции — не позже следующего рабочего дня;
- график работы — 08:00–18:00 с понедельника по пятницу, исключая праздничные и выходные дни (часовой пояс поставщика ПО).

Способ оказания технической поддержки:

- по телефону разработчика или дистрибутора ПО;
- по e-mail разработчика или дистрибутора ПО;
- на объекте защиты ПДн Грузополучателей (по предварительной договоренности).

4.13. Задачи Поставщика

Поставщик должен организовать выполнение комплекса монтажных и пусконаладочных работ в оперативном контакте с Грузополучателей, в том числе:

- осуществлять оперативное руководство работами;
- осуществлять самостоятельно минимально необходимое администрирование системы (DHCP, FTP, DNS, внесение имен компьютеров, создание каталогов на сервере, внесение доменных имен пользователей и компьютеров, настройка сетевого клиента на АРМах, установка логина и пароля на АРМы пользователей, активация операционных систем, офисных и антивирусных программ)
- произвести обучение персонала в два этапа:

  1) Ознакомление ответственных лиц объектов грузополучателей с системой на территории Головного учреждения Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови»;

  2) произвести общий инструктаж (обучение) персонала на рабочих местах, осуществлять мониторинг и коррекцию действий персонала на этапе ввода в строй;
- произвести настройку под используемый техпроцесс (внести специфику в системные справочники, выявить отличия от типового технологического процесса, организовать согласование локальных решений с пользователями информационной системы Грузополучателей;
- произвести проверку (при необходимости настройку) средств работы с удаленными пользователями;
- при необходимости принять участие в отладке информационного взаимодействия с РИЦ и Единым информационным центром службы крови России;
- обеспечивать ежедневное присутствие своего представителя на объекте.

Поставщик должен обеспечивать в течение срока гарантийной поддержки эксплуатации сопровождение технических средств, в том числе:

- восстановление работы системы после аварийных ситуаций, обеспечивать восстановление баз данных;
- профилактические мероприятия на вычислительных и технических средствах, входящих в систему, в том числе резервное копирование и индексирование баз данных;
- наладку периферийного оборудования;
- локализацию неисправностей и передачу оборудования представителю производителя оборудования в гарантийный ремонт,
- проводить контроль работы телекоммуникационных систем (удаленные пользователи, информационное взаимодействие с РИЦ и Единым Информационным Центром службы крови России);

В целях организации исполнения каждого этапа исполнения государственного контракта, Поставщик в течение 10 рабочих дней после даты заключения государственного контракта представляет Грузополучателю календарный план-график работ.

5. Список нормативно-технических документов и правовых актов

5.1. Нормативно-технические документы

- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем»;
- ГОСТ 34.603-92. «Информационная технология. Виды испытаний автоматизированных систем»;
- РД 50-682-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения»;
- РД 50-680-88 «Методические указания. Автоматизированные системы. Основные положения»;
- РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;
- Р 50-34.126-92 «Информационная технология. Правила проведения работ при создании автоматизированных систем».
- Комплекс стандартов ЕСПД.
- ГОСТ РВ 15.201-2003 и др. (Системы разработки и постановки продукции на производство).
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (РД ОК), Гостехкомиссия (ФСТЭК) России, 2002;
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к информации (РД АС). Гостехкомиссия (ФСТЭК) Россия, 1992;
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД СВТ). Гостехкомиссия (ФСТЭК) Россия, 1992;
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД МЭ). Гостехкомиссия (ФСТЭК) Россия, 1998;
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия (ФСТЭК) Россия, 1992;
- «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждены приказом Гостехкомиссии России от 20 августа 2002 г. № 282;
- Нормативные документы ФСТЭК России по защите персональных данных;
- ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»;
- ГОСТ 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»;
- ГОСТ 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении».

- ГОСТ Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения"
- ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"
- ГОСТ Р ИСО/МЭК ТО 13335-3-2007 "Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий"
- ГОСТ Р МЭК 60950-1-2005 "Оборудование информационных технологий. Требования безопасности. Часть 1. Общие требования"
- ГОСТ Р 52633-2006 "Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации"
- ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения"
- ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий"
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 "Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер"
- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети"
- ГОСТ Р ИСО/МЭК 19794-4-2006 "Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца"

5.2. Нормативные правовые акты

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства РФ № 687 от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Методический документ ФСТЭК от 11.02.2014 г. "Меры защиты информации в государственных информационных системах"
- Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/5-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;

- Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК, 2008г;
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (РД ОК), Гостехкомиссия (ФСТЭК) России, 2002;
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к информации (РД АС). Гостехкомиссия (ФСТЭК) Россия, 1992;
- Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД СВТ). Гостехкомиссия (ФСТЭК) Россия, 1992;
- Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД МЭ). Гостехкомиссия (ФСТЭК) Россия, 1998;
- Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия (ФСТЭК) Россия, 1992.

Приложение 1. Потребность в оборудовании, программном обеспечении, материалах

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Ивановский-1 филиал

Таблица 24

№ п/п	Наименование	Ед.изм.	Требуемое кол-во
1	АРМ информационной системы		
1.1.	АРМ тип 1	комплект	2
1.2.	АРМ тип 2	комплект	3
1.5.	АРМ тип 3	комплект	3
2	Серверное оборудование		
2.1.	Серверное оборудование	комплект	1
3	Источники бесперебойного питания		
3.1.	ИБП для АРМ тип 1, 2, 3	шт.	8
3.2.	ИБП для серверного оборудования	шт.	1
3.3.	ИБП для настенного шкафа	шт.	1
4	Комплект оборудования для создания инфраструктуры		
4.1.	Комплект активного сетевого оборудования, в составе		
4.1.1.	Маршрутизатор	шт.	1
4.1.2.	Коммутатор	шт.	1
4.2.	Комплект климатического оборудования	комплект	1
4.3.	Комплект материалов СКС, в составе:		
4.3.1.	Кабель UTP кат.5е, 305м	коробка	3
4.3.2.	Шкаф настенный 19”	шт.	1
4.3.4.	Короб 110*50, 2м	шт.	40
4.3.5.	Розетки для короба информационные RJ45	шт.	16

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Ивановский-2 филиал

Таблица 25

№ п/п	Наименование	Ед.изм.	Требуемое кол-во
1	АРМ информационной системы		
1.1.	АРМ тип 1	комплект	1
1.2.	АРМ тип 2	комплект	3
1.5.	АРМ тип 3	комплект	2
2	Серверное оборудование		
2.1.	Серверное оборудование	комплект	1
3	Источники бесперебойного питания		
3.1.	ИБП для АРМ тип 1, 2, 3	шт.	6
3.2.1.	ИБП для серверного оборудования	шт.	1
3.2.5.	ИБП для настенного шкафа	шт.	1
4	Комплект оборудования для создания инфраструктуры		
4.1.	Комплект активного сетевого оборудования, в составе		
4.1.1.	Маршрутизатор	шт.	1
4.1.2.	Коммутатор	шт.	1
4.2.	Комплект климатического оборудования	комплект	1
4.3.	Комплект материалов СКС, в составе:		
4.3.1.	Кабель UTP кат.5е, 305м	коробка	2
4.3.2.	Шкаф настенный 19”	шт.	1
4.3.4.	Короб 110*50, 2м	шт.	30
4.3.5.	Розетки для короба информационные RJ45	шт.	12

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Шуйский филиал

Таблица 26

№ п/п	Наименование	Ед.изм.	Требуемое кол-во
1	АРМ информационной системы		
1.1.	АРМ тип 1	комплект	2
1.2.	АРМ тип 2	комплект	4
1.5.	АРМ тип 3	комплект	2
2	Серверное оборудование		
2.1.	Серверное оборудование	комплект	1
3	Источники бесперебойного питания		
3.1.	ИБП для АРМ тип 1, 2, 3	шт.	8
3.2.1.	ИБП для серверного оборудования	шт.	1
3.2.5.	ИБП для настенного шкафа	шт.	1
4	Комплект оборудования для создания инфраструктуры		
4.1.	Комплект активного сетевого оборудования, в составе		
4.1.1.	Маршрутизатор	шт.	1
4.1.2.	Коммутатор	шт.	1
4.2.	Комплект климатического оборудования	комплект	1
4.3.	Комплект материалов СКС, в составе:		
4.3.1.	Кабель UTP кат.5е, 305м	коробка	3
4.3.2.	Шкаф настенный 19”	шт.	1
4.3.4.	Короб 110*50, 2м	шт.	40
4.3.5.	Розетки для короба информационные RJ45	шт.	16

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Кинишемский филиал

Таблица 27

№ п/п	Наименование	Ед.изм.	Требуемое кол-во
1	АРМ информационной системы		
1.1.	АРМ тип 1	комплект	2
1.2.	АРМ тип 2	комплект	4
1.5.	АРМ тип 3	комплект	2
2	Серверное оборудование		
2.1.	Серверное оборудование	комплект	1
3	Источники бесперебойного питания		
3.1.	ИБП для АРМ тип 1, 2, 3	шт.	8
3.2.1.	ИБП для серверного оборудования	шт.	1
3.2.5.	ИБП для настенного шкафа	шт.	1
4	Комплект оборудования для создания инфраструктуры		
4.1.	Комплект активного сетевого оборудования, в составе		
4.1.1.	Маршрутизатор	шт.	1
4.1.2.	Коммутатор	шт.	1
4.3.	Комплект материалов СКС, в составе:		
4.3.1.	Кабель UTP кат.5е, 305м	коробка	3
4.3.2.	Шкаф настенный 19”	шт.	1
4.3.4.	Короб 110*50, 2м	шт.	40
4.3.5.	Розетки для короба информационные RJ45	шт.	16

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Вичугский филиал

Таблица 28

№ п/п	Наименование	Ед.изм.	Требуемое кол-во
1	АРМ информационной системы		
1.1.	АРМ тип 1	комплект	2
1.2.	АРМ тип 2	комплект	3
1.5.	АРМ тип 3	комплект	2
2	Серверное оборудование		
2.1.	Серверное оборудование	комплект	1
3	Источники бесперебойного питания		
3.1.	ИБП для АРМ тип 1, 2, 3	шт.	7
3.2.1.	ИБП для серверного оборудования	шт.	1
3.2.5.	ИБП для настенного шкафа	шт.	1
4	Комплект оборудования для создания инфраструктуры		
4.1.	Комплект активного сетевого оборудования, в составе		
4.1.1.	Маршрутизатор	шт.	1
4.1.2.	Коммутатор	шт.	1
4.2.	Комплект климатического оборудования	комплект	1
4.3.	Комплект материалов СКС, в составе:		
4.3.1.	Кабель UTP кат.5е, 305м	коробка	3
4.3.2.	Шкаф настенный 19”	шт.	1
4.3.4.	Короб 110*50, 2м	шт.	35
4.3.5.	Розетки для короба информационные RJ45	шт.	14

Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Фурмановский филиал

Таблица 29

№ п/п	Наименование	Ед.изм.	Требуемое кол-во
1	АРМ информационной системы		
1.1.	АРМ тип 1	комплект	1
1.2.	АРМ тип 2	комплект	4
1.5.	АРМ тип 3	комплект	2
2	Серверное оборудование		
2.1.	Серверное оборудование	комплект	1
3	Источники бесперебойного питания		
3.1.	ИБП для АРМ тип 1, 2, 3	шт.	7
3.2.1.	ИБП для серверного оборудования	шт.	1
3.2.5.	ИБП для настенного шкафа	шт.	1
4	Комплект оборудования для создания инфраструктуры		
4.1.	Комплект активного сетевого оборудования, в составе		
4.1.1.	Маршрутизатор	шт.	1
4.1.2.	Коммутатор	шт.	1
4.3.	Комплект материалов СКС, в составе:		
4.3.1.	Кабель UTP кат.5е, 305м	коробка	3
4.3.2.	Шкаф настенный 19”	шт.	1
4.3.4.	Короб 110*50, 2м	шт.	35
4.3.5.	Розетки для короба информационные RJ45	шт.	14

Приложение 2. Перечень грузополучателей

Таблица 30

№ п/п	Наименование Грузополучателя	Адрес фактический
1.	Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Ивановский-1 филиал	153000 Ивановская область, г.Иваново, ул.Любимова д.1
2.	Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Ивановский-2 филиал	153000 Ивановская область, г.Иваново, ул.Любимова, д.5
3.	Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Шуйский филиал	155900 Ивановская область, г.Шуя, ул.1-я Металлистов, д.1в
4.	Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Кинишемский филиал	155800 Ивановская область, г.Кинешма, ул.Гагарина, д.2а
5.	Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Вичугский филиал	155330 Ивановская область, г.Вичуга, ул.Ульяновская, д.12
6.	Областное бюджетное учреждение здравоохранения «Ивановская областная станция переливания крови» Фурмановский филиал	155520 Ивановская область, г.Фурманов, ул.Тимирязева, д.1