ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение работ по модернизации систем защиты персональных данных и аттестации учреждений, подключенных к единой базе данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов, в соответствии с требованиями действующего законодательства РФ в сфере защиты информации и персональных данных в государственных информационных системах в 2013году.

1. Общие сведения

1.1. Полное наименование работы и ее условное обозначение

Полное наименование работы: выполнение работ по модернизации систем защиты персональных данных и аттестации учреждений, подключенных к единой базе данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов, в соответствии с требованиями действующего законодательства РФ в сфере защиты информации и персональных данных в государственных информационных системах в 2013году.

Условное обозначение работы: выполнение работ по модернизации систем защиты персональных данных и аттестации учреждений.

1.2. Основание для проведения работ

Выполнение работ по модернизации систем защиты персональных данных и аттестации учреждений осуществляется на основании следующих документов:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
- Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Постановление Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных

систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 3 февраля 2012 г. № 79 «Об утверждении положения о лицензировании деятельности по технической защите конфиденциальной информации»;
- Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом Гостехкомиссии России от 27 октября 1995 г. № 199);
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России, 15 февраля 2008 г.;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, ФСТЭК России 14 февраля 2008 г.;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены 8 Центром 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 обработке в информационных системах персональных данных (утверждены 8 Центром ФСБ России от 21 февраля 2008 г. №149/6/6-622);
- Положение по аттестации объектов информатизации по требованиям безопасности информации, Гостехкомиссия России, 1994 г.;

– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 г. № 282;
– РД «Защита от НСД к информации», ч. 1 «Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларируемых возможностей», Гостехкомиссия России, 1999 г.;
– РД «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации», Гостехкомиссия России, 1992 г.;
– РД «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1992 г.;
– РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», Гостехкомиссия России, 1992 г.;
– РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»,Гостехкомиссия России, 1997 г.;
– «Сборником временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам», Гостехкомиссия России, 2002 г.;
– РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;
– 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, комплексность и обозначение документов при создании автоматизированных систем»;
– ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

1.3. Срок выполнения работ

Начало: со дня заключения Договора.

Окончание: в течение 45 (Сорока пяти) дней со дня заключения Договора.

1.4. Порядок оформления и предъявления заказчику результатов работ

По завершении работ по каждому этапу Исполнитель предъявляет Заказчику отчетные документы в соответствии с разделом 5.9 настоящего Технического задания и акты сдачи-приемки выполненных работ.

Порядок оформления и предъявления Заказчику результатов работ приведен в разделе 6 настоящего Технического задания.

1.5. Принятые сокращения

АРМ	-	Автоматизированное рабочее место
АС	-	Автоматизированная система
ЕИБД	-	Единая информационная база донорства
ИТ	-	Информационные технологии
ИЦЦК	-	Информационный центр Центра крови
ИСПДн	-	Информационная система персональных данных
ЛВС	-	Локальная вычислительная сеть
ЛПУ	-	Лечебно-профилактическое учреждение
МЭ	-	Межсетевой экран
НСД	-	Несанкционированный доступ (несанкционированные действия)
ОС	-	Операционная система
ОСК	-	Объект Службы крови
ПАК	-	Программно-аппаратный комплекс
ПО	-	Программное обеспечение
СЗИ	-	Система защиты информации
СКЗИ	-	Средство криптографической защиты информации
ТЗ	-	Техническое задание
ТС	-	Технические средства
ФГБУЗ	-	Федеральное государственное бюджетное учреждение здравоохранения
ФМБА	-	Федеральное медико-биологическое агентство
ФСБ России	-	Федеральная служба безопасности Российской Федерации
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю Российской Федерации

1.6. Основные определения

Доступ к информации	-	возможность получения информации и ее использования
Единая информационная база донорства	-	распределенный программно-аппаратный комплекс единой базы данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов
Информационная система персональных данных	-	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

Информационный центр Центра крови	-	структурное подразделение ФГБУЗ Центр крови ФМБА России, осуществляющее техническую поддержку и обеспечивающее функционирование аппаратно-программных средств ЕИБД
Конфиденциальность информации	-	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Нарушитель безопасности информации	-	физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах
Несанкционированный доступ (несанкционированные действия)	-	доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам
Обработка персональных данных	-	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Объект Службы крови	-	учреждение (структурное подразделение), входящее в состав Службы крови, имеющее необходимые помещения, оборудование, персонал для осуществления деятельности в сфере обращения донорской крови и (или) ее компонентов
Персональные данные	-	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Служба крови	-	объединенные в единую систему на функциональной основе в целях обеспечения на территории Российской Федерации единства организационных основ деятельности в сфере обращения донорской крови и (или) ее компонентов: 1) федеральные органы исполнительной власти в сфере охраны здоровья, органы исполнительной власти субъектов Российской Федерации в сфере охраны здоровья, а также органы местного самоуправления, осуществляющие полномочия в сфере охраны здоровья; 2) медицинские организации, образовательные организации, научные организации, подведомственные соответственно федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской Федерации, государственным академиям наук и осуществляющие деятельность в сфере обращения донорской крови и (или) ее

		компонентов; 3) организации федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба; 4) медицинские организации, которые подведомственны уполномоченным органам местного самоуправления и соответствующие структурные подразделения которых (осуществляют заготовку, хранение, транспортировку донорской крови и (или) ее компонентов) созданы не позднее 1 января 2006 года.
Технические средства информационной системы	-	средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации
Угрозы безопасности информации	-	совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в информационной системе
Федеральное медико-биологическое агентство	-	федеральный орган исполнительной власти, находящийся в ведении Министерства здравоохранения Российской Федерации, осуществляющий функции по оказанию государственных услуг, в том числе организацию деятельности Службы крови, по контролю и надзору в сфере донорства крови и ее компонентов, в том числе ведение единой информационной базы по реализации мероприятий по развитию, организации и пропаганде донорства крови и ее компонентов
Федеральное государственное бюджетное учреждение здравоохранения «Центр крови Федерального медико-биологического агентства»	-	учреждение здравоохранения, предметом и целью деятельности которого является заготовка, переработка, хранение и обеспечение безопасности донорской крови и ее компонентов, ведение единой информационной базы по реализации мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов
Целостность информации	-	состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

2. Назначение и цели модернизации систем защиты информации объектов Службы крови

2.1. Назначение

Основным назначением модернизируемых систем защиты информации объектов Службы крови является:

- предотвращение неправомерного доступа, копирования, предоставления или распространения информации ограниченного доступа (обеспечение конфиденциальности информации);
- исключение неправомерного уничтожения или модифицирования информации ограниченного доступа (обеспечение целостности информации);
- исключение неправомерного блокирования информации ограниченного доступа (обеспечение доступности информации);
- обеспечение соответствия требованиям действующего законодательства РФ в сфере защиты информации и персональных данных в государственных информационных системах ОСК.

2.2. Цели модернизации

Основными целями при выполнении работ по модернизации систем защиты информации и аттестации объектов Службы крови является:

- проведение обследования объектов Службы крови на соответствие требованиям по защите информации ограниченного доступа в государственных информационных системах;
- разработка организационно-распорядительной, нормативно-методической и эксплуатационной документации в области обработки и защиты информации ограниченного доступа в государственных информационных системах на объектах Службы крови;
- разработка технических решений на модернизацию систем защиты информации объектов Службы крови;
- внедрение систем защиты информации на объектах Службы крови;
- исследование уязвимостей информационных систем и систем защиты информации объектов Службы крови с применением специальных средств анализа защищенности;
- разработка комплектов документов, необходимых для проведения аттестации объектов Службы крови на соответствие требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах;
- проведение аттестационных испытаний объектов Службы крови по требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах.

3. Характеристики объекта защиты

Объектом защиты в рамках настоящего Технического задания являются:

- информация ограниченного распространения (в том числе персональные данные), содержащаяся в информационных системах учреждений, подключенных к единой базе данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов;
- технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), на которых осуществляется обработка информация ограниченного доступа;
- общесистемное, прикладное, специальное программное обеспечение, информационные технологии;
- средства защиты информации, применяемые для защиты информации ограниченного доступа.

Работы в рамках настоящего Технического задания выполняются на объектах Заказчика, указанных в Приложении № 1 и Приложении № 2.

Защите подлежат АРМ пользователей и сервера на ОСК, а также АРМ пользователей в ЛПУ (по одному АРМ в каждом ЛПУ).

В соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» для информационных систем персональных данных ОСК был установлен класс К1.

Классификация информационных систем Заказчика в соответствии с требованиями Постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» должна быть проведена Исполнителем на этапе обследования (согласно разделу 5.2 настоящего ТЗ).

4. Требования к системе защиты информации

4.1. Общие требования к системе защиты информации

4.1.1. Требования к структуре и функциям системы защиты информации

Система защиты информации объектов Службы крови (далее - ОСК) должна состоять из следующих уровней:

- головной центр управления системами защиты информации (Информационный центр ФГБУЗ Центр крови ФМБА России);
- подчиненные центры управления системами защиты информации (системы защиты информации объектов Службы крови);
- системы защиты информации лечебно-профилактических учреждений.

В составе модернизируемой системы защиты информации должны быть реализованы следующие подсистемы защиты:

- подсистема управления доступом и учетными данными пользователей;
- подсистема регистрации событий безопасности;
- подсистема обеспечения целостности;
- подсистема межсетевого экранирования;
- подсистема защиты от утечек информации;
- подсистема обнаружения вторжений;
- подсистема антивирусной защиты;
- подсистема анализа защищённости;
- подсистема криптографической защиты.

Полный перечень функций, обеспечиваемых данными подсистемами, приведен в разделе 4.2 настоящего Технического задания.

4.1.2. Требования к режимам функционирования

Режимы функционирования должны:

- обеспечивать возможность круглосуточного функционирования СЗИ;
- обеспечивать независимость функционирования средств защиты информации от изменений в организационной структуре объекта внедрения при сохранении состава и содержания выполняемых функций;
- допускать настройку и изменение конфигурации средств защиты информации без перепрограммирования;
- обеспечивать возможность изменения настроек, политик и правил доступа пользователей к средствам защиты информации при изменении ИТ-инфраструктуры, вводе новых регламентов обеспечения информационной безопасности, изменения организационно-штатной структуры Заказчика;
- обеспечивать возможность выявления причин неисправности взаимодействия с другими узлами сети, используя функции журналирования и изменения режимов работы средств защиты информации.

4.1.3. Требования к показателям назначения

Архитектура СЗИ в совокупности с механизмом поддержки функциональных подсистем не должна накладывать каких-либо ограничений на информационные технологии, используемые на объектах информатизации.

Модернизация СЗИ должно осуществляться на основе действующего законодательства РФ в сфере защиты информации и персональных данных в государственных информационных системах.

Архитектура СЗИ объекта информатизации должна обеспечивать реализацию функций защиты информации на всех технологических этапах эксплуатации СЗИ, в том числе при проведении технического обслуживания и ремонта.

4.1.4. Требования к надежности

Аппаратно-программные компоненты СЗИ должны быть рассчитаны для функционирования в режиме круглосуточной работы и позволять осуществлять выполнение процедур резервирования и восстановления системы после сбоев.

4.1.5. Требования к безопасности

Размещение и монтаж используемых в СЗИ технических средств должны производиться в строгом соответствии с требованиями, установленными предприятиями-изготовителями этих технических средств.

Размещение оборудования на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

В нормальных условиях технические средства и отдельные блоки не должны терять физическую устойчивость в такой степени, чтобы подвергать опасности пользователей и обслуживающий персонал.

При необходимости предпринимать специальные меры предосторожности во избежание возникновения опасности при работе, установке, обслуживании, транспортировании и хранении технических средств, должны быть подготовлены необходимые инструкции (разделы эксплуатационных документов).

Конструкция технических средств должна ограничить опасность возникновения пожара или поражения электрическим током в результате электрических или механических перегрузок, отказов, ненормальной работы или ошибок в эксплуатации.

Технические средства СЗИ должны соответствовать требованиям электробезопасности, установленными ГОСТ 21552-84 (п.п. 1.7, 1.8), ГОСТ Р МЭК 60950-2002 (п.п. 2.6, 2.7, 3.1, 3.2), ГОСТ 25861-83 (п.п. 2.1-2.7), ГОСТ Р 50571.22-2000 (раздел 707) и обеспечивать защиту пользователей и обслуживающий персонал от поражения электрическим током.

Значения вредных факторов производственной среды и трудового процесса при работе с техническими средствами (уровни электромагнитных полей, акустического шума, концентрация вредных веществ в воздухе, мягкое рентгеновское излучение), оказывающих неблагоприятное влияние на здоровье человека, не должны превышать действующих норм, установленных СанПиН 2.2.2./2.4.1340-03 от 03.06.2003 г.

4.1.6. Требования к патентной чистоте

При модернизации СЗИ объектов Службы крови должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.

При поставке программного обеспечения должны быть выполнены требования Гражданского Кодекса Российской Федерации в части передачи неисключительной лицензии. Выполнение требований по обеспечению лицензионной чистоты программного обеспечения, обеспечивается Исполнителем.

Программное обеспечение СЗИ объектов Службы крови, приобретаемое у сторонних организаций, должны сопровождаться документацией, подтверждающей правомочность этих организаций поставлять данную продукцию и сопровождаться лицензионным соглашением.

4.1.7. Требования по стандартизации и унификации

Решения по использованию технических средств и ПО в СЗИ объектов Службы крови должны по возможности состоять из однотипных компонент в целях обеспечения снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации.

4.1.8. Требования к эксплуатации

Условия, режим эксплуатации, виды и периодичность обслуживания технических средств определяются требованиями поставщиков технических средств и программного обеспечения.

4.2. Требования к функциям системы защиты информации

4.2.1. Требования к подсистеме управления доступом и учетными данными пользователей

В части управления учетными записями пользователей подсистема управления доступом и учетными данными пользователей должна обеспечивать:

- возможность формирования единого каталога учетных данных пользователей;
- синхронизацию содержимого единого каталога с данными в защищаемых информационных системах;
- администрирование жизненного цикла учетных записей в защищаемых информационных системах: автоматическое создание, обновление, блокировка, разблокировка и удаление учетных записей;
- управление блокировкой и разблокировкой учетных записей.

В части управления правами доступа пользователей подсистема должна обеспечивать:

- возможность автоматизации процедур запроса и согласования прав доступа к информационным ресурсам;
- автоматическое назначение полномочий пользователям в защищаемых информационных системах в соответствии с утвержденными запросами прав доступа;

– автоматическое назначение полномочий пользователям в защищаемых информационных системах в соответствии с ролевой моделью (заранее предопределенным набором минимальных прав доступа пользователя);
– предоставление интерфейса самообслуживания пользователей: запрос прав доступа, смена/сброс паролей;
– возможность аудита прав доступа и построения отчетности;

В части создания и поддержания в актуальном состоянии единого каталога информационных ресурсов подсистема должна обеспечивать:

– возможность хранения описаний информационных ресурсов, сведений об ответственных за информационный ресурс, и другой характеризующей ресурс информации;
– хранение актуальной информации об имеющихся информационных ресурсах и обеспечение возможности формирования запросов на доступ к требуемому ресурсу (в рамках должностных обязанностей);

В части управления ролями пользователей подсистема должна обеспечивать:

– возможность создания типовых наборов прав и полномочий пользователей для доступа к информационным ресурсам в соответствии с их должностными обязанностями;
– возможность создание хранилища актуальной информации о полномочиях пользователей в защищаемых информационных системах;
– контроль совместимости полномочий пользователей;
– возможность периодического аудита полномочий пользователей – проверка их неизбыточности.

В части управления аутентификацией и авторизацией пользователей подсистема должна обеспечивать:

– усиленную аутентификацию пользователей;
– поддержку персональных идентификаторов eToken PRO/R2, Rutoken;
– реализацию механизма однократной аутентификации пользователей (Single Sign-On) при доступе к информационным системам;
– централизованное регулирование доступа к защищаемым информационным системам путем настройки соответствующих политик;
– возможность применения требований к паролям пользователей путем настройки политик безопасности;
– возможность аудита действий пользователей при обращении к защищаемым информационным системам;
– возможность аудита действий администраторов при создании, изменении политик доступа в защищаемым информационным системам.

В части обеспечения целостности подсистема управления доступом и учетными данными пользователей должна обеспечивать:

- контроль целостности файлов, каталогов, элементов системного реестра;
- контроль буфера обмена ОС;
- функциональный контроль ключевых компонентов операционной системы;
- реакцию средства защиты информации при нарушении целостности:
    - регистрацию события в журнале;
    - блокировку компьютера;
    - восстановление повреждённой/модифицированной информации;
    - отклонение или принятие изменений;
    - функциональный самоконтроль подсистем.
- автоматическое затирание данных на диске при удалении файлов пользователем.

В части разграничения доступа к внешним устройствам, подключениям и контролю печати подсистема управления доступом и учетными данными пользователей должна обеспечивать:

- разграничение доступа к следующим устройствам:
    - последовательные и параллельные порты;
    - локальные устройства;
    - сменные, логические и оптические диски;
    - USB – устройства;
    - устройства PCMCI;
    - устройства IEEE1394;
    - устройства SecureDigital.
- управление подключениями (IrDA, Wi-Fi, FireWire, Ethernet, Bluetooth);
- контроль вывода информации на отчуждаемые носители;
- контроль вывода конфиденциальных данных на печать;
- управление грифами конфиденциальности при печати документов из приложений MS Word и MS Excel;
- возможность создания централизованных политик безопасности по использованию отчуждаемых USB-носителей информации.

В части мониторинга и регистрации событий безопасности подсистема управления доступом и учетными данными пользователей должна обеспечивать:

- централизованный сбор и хранение журналов безопасности, регистрацию событий безопасности;
- возможность автоматического оповещения по электронной почте о событиях несанкционированного доступа;
- возможность формирования отчетов по результатам аудита;
- возможность делегирования административных полномочий в рамках организационных подразделений;
- централизованный мониторинг и оперативное управление своими компонентами.

Средства защиты информации, применяемые в составе подсистемы управления доступом и учетными данными пользователей, должны быть сертифицированы на соответствие требованиям ФСТЭК России.

4.2.2. Требования к подсистеме регистрации событий безопасности

Подсистема регистрации событий безопасности может быть реализована как техническими, так и организационными мерами и должна обеспечивать:

- регистрацию входа (выхода) пользователя в систему (из системы) либо регистрацию загрузки и инициализации операционной системы и ее программного останова;
- запись в журналах регистрации следующих параметров: даты и времени входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результата попытки входа (успешная или неуспешная); идентификатора пользователя, предъявленного при попытке доступа;
- учет защищаемых носителей информации;
- защиту информации о событиях безопасности.

Средства защиты информации входящие в состав подсистемы регистрации событий безопасности должны быть сертифицированы ФСТЭК России.

4.2.3. Требования к подсистеме обеспечения целостности

Подсистема обеспечения целостности должна обеспечивать контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

В подсистеме обеспечения целостности должны быть реализованы следующие организационные мероприятия:

- определение круга лиц, которым разрешены действия по внесению изменений в конфигурацию информационных систем и систем защиты информации;
- документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты информации;
- анализ потенциального воздействия планируемых изменений в конфигурации информационных систем и систем защиты информации на обеспечение информационной безопасности;
- управление изменениями конфигурации информационных систем и систем защиты информации.

4.2.4. Требования к подсистеме межсетевого экранирования

Подсистема межсетевого экранирования предназначена для организации безопасного взаимодействия между компонентами системы в распределенной сетевой среде.

Подсистема межсетевого экранирования должна выполнять следующие функции в системе:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

– фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
– фильтрацию с учетом любых значимых полей сетевых пакетов;
– фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
– фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
– фильтрацию с учетом даты и времени;
– идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
– предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
– идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
– регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
– регистрацию и учет запросов на установление виртуальных соединений;
– локальную сигнализацию попыток нарушения правил фильтрации;
– регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратного отключения межсетевого экрана;
– возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;
– контроль целостности своей программной и информационной части;
– контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.

В целях обеспечения безопасного межсетевого взаимодействия средства подсистемы межсетевого экранирования могут иметь совместную реализацию с сетевыми средствами подсистемы криптографической защиты.

Средства подсистемы межсетевого экранирования должны быть сертифицированы ФСТЭК России на соответствие требованиям защищенности от НСД для межсетевых экранов не ниже 4 класса защищенности.

4.2.5. Требования к подсистеме защиты от утечек информации

Подсистема защиты от утечек информации предназначена для контроля утечек информации и основана на контентном анализе информации, проходящей через контролируемые участки.

Подсистема защиты от утечек информации должна быть реализована на базе специализированного программно-аппаратного средства предотвращения утечек информации ограниченного доступа.

Общие требования к подсистеме защиты от утечек информации:

- решение должно иметь единую схему анализа данных всеми детектирующими сенсорами (т.е. сетевыми сканерами и агентами на конечных компьютерах, и для пассивного мониторинга, и для блокировки, и для поиска);
- система должна иметь возможность масштабирования за счет балансировки нагрузки одного агента на несколько одновременно работающих анализаторов;
- функциональность анализатора отпечатков (файловых и табличных) должна поддерживаться автономно на каждом сервере и конечном компьютере за счет автоматической репликации хранилища;
- система должна выделять и инспектировать текстовое содержимое из файлов и вложений;
- система должна инспектировать метаданные хранимых файлов;
- система должна реализовывать алгоритм анализа передаваемых и хранимых файлов на основе цифровых отпечатков данных;
- система должна автоматически обнаруживать и сканировать файловые папки в локальной сети. Должна быть реализованы функции «обнаружить все общие папки в заданной подсети», «просканировать все административные папки»;
- система должна иметь средства для автоматического выявления серийных утечек данных любого типа от одного пользователя в течение заданного периода времени, с помощью задания порога и интервала;
- система должна рекурсивно проверять содержимое вложенных (ZIP, TAR, RAR) архивов путем анализа цифровых отпечатков каждого файла;
- система должна иметь информацию о методической доле ложных срабатываний, подтвержденную независимым исследованием.

Требования к определению политик безопасности в подсистеме:

- решение должно допускать использование нескольких методов определения информации ограниченного доступа;
- должна быть предусмотрена возможность одновременно и многократно использовать классификаторы информации в нескольких политиках;
- решение должно обладать возможностью задания единой системы политик в рамках всей подсистемы защиты;

– каждая политика должна иметь возможность одновременного применения к данным в движении (Data-in-Motion), используемым данным (Data-in-Use) и хранимым данным (Data-at-Rest), как на уровне сети, так и на конечных компьютерах;
– продукт должен иметь единую веб-консоль централизованного управления устройствами, конечными компьютерами, политиками и отчетами;
– решение не должно требовать для настройки утилит командной строки, редактирования текстовых файлов, интерфейсов программирования (API) а также языков сценариев (скриптов). Не допускается хранение паролей в открытом виде в файлах настроек. Исключения делаются только для использования командной строки при однократном вводе в эксплуатацию программно-аппаратных комплексов, а также для запуска сценариев автоматической реакции на инциденты;
– политики безопасности должны определяться на основе следующего: содержимое, отправитель и получатель, тип файла, коммуникационный протокол, категория веб-сайта;
– система должна иметь возможность определения одной политики на основе нескольких разнородных типов данных одновременно (например, словарь и отпечатки), используя произвольную булевскую логику (операции И, ИЛИ, НЕ, скобки);
– решение должно иметь возможность в рамках одной политики произвольно назначать уровень критичности инцидентам в зависимости от срабатывания правил;
– система должна обеспечивать ведение контроля и журнала автоматического аудита настроек и изменений политик;
– система должна предлагать настраиваемый механизм присвоения уровня критичности каждому инциденту в зависимости от содержимого;
– система должна предоставлять возможность выборочного включения и исключения правил на основе корпоративной службы каталогов, чтобы политики применялись в зависимости от отправителя и/или получателя/назначения информации;
– система должна предоставлять удобный графический интерфейс для настройки пользовательских политик на основе готовых политик и созданных классификаторов информации;
– система должна предоставлять простой способ активации готовой политики непосредственно в веб-консоли управления, не прибегая к редактированию файлов.

Требования к подсистеме в части анализа отпечатков структурированных данных:
– система должна иметь механизм анализа цифровых отпечатков для табличных данных, например, данных клиентов;
– решение должно иметь возможность централизованного применения цифровых отпечатков на всех анализаторах и площадках организации, путем односторонней репликации из центра управления;

- должна быть возможность задавать расписание, по которому синхронизируется база отпечатков между центральным офисом и подразделениями;
- система должна иметь возможность подключаться к источнику данных напрямую по протоколу ODBC;
- решение не должно требовать выгрузку/копирование данных в центральное хранилище для снятия отпечатков;
- решение должно давать возможность комбинировать содержимое полей и задавать индивидуальные пороги для каждого из сочетаний;
- должна быть возможность задействовать классификатор цифровых отпечатков многократно в нескольких политиках, выбирая нужные поля в каждом случае независимо (т.е. единый классификатор из 10 млн записей может быть задействован многократно в разных политиках с разным набором полей в каждом случае).

Требования к подсистеме в части анализа отпечатков неструктурированных данных:

- отпечатки данных должны сниматься с одного источника данных и автоматически применяться на всех анализаторах и площадках организации, путем односторонней репликации из центра;
- должна быть возможность задавать расписание, по которому синхронизируется база отпечатков между центральным офисом и подразделениями;
- система должна минимально использовать копирование/выгрузку информации в центральное хранилище для снятия отпечатков;
- системе должно быть достаточно прав только на чтение для снятия отпечатков;
- система должна быть устойчива к изменениям документов и обнаруживать фрагменты текста в форматах, отличных от исходных. Например, система должна быть способной обнаружить абзац текста из документа MS Word, вставленный в тело сообщения, либо напечатанный в формате PDF;
- система должна обнаруживать черновики и редакции документов, измененные или скопированные, требуя однократного снятия отпечатка с единственной версии документа;
- система должна иметь возможность игнорировать заданные фрагменты текста при анализе. Срабатывание должно происходить только на том содержимом, которое относится к информации ограниченного доступа.

Требования подсистеме в части идентификации и классификации информации:

- идентификация информации ограниченного доступа по ключевым словам, словарям, лексиконам и шаблонам регулярных выражений;
- в системе должна быть реализована функция вычисления контрольных разрядов для тех данных, которые имеют такое свойство;
- система должна опознавать данные по наличию языкового контекста.

– система должна распознавать не менее 400 форматов файлов распространенных приложений, в т. ч. офисных, архивов, исходного кода, зашифрованных контейнеров;
– система должна иметь готовые классификаторы информации ограниченного доступа, общее количество шаблонов – не менее 1000.

Требования подсистеме в части контроля сетевых каналов утечки информации:

– сетевой мониторинг и предотвращение (автоматическая блокировка) информационных утечек через сообщения электронной почты, передаваемые по протоколу SMTP;
– сетевой мониторинг и предотвращение (автоматическая блокировка) информационных утечек при работе с сетью через безопасный протокол HTTPS;
– сетевой мониторинг и предотвращение (автоматическая блокировка) информационных утечек по протоколу FTP, без передачи содержимого в открытом виде по протоколу ICAP;
– сетевой мониторинг и предотвращение (автоматическая блокировка) информационных утечек при отправке электронной почты по протоколу SMTP, с анализом данных непосредственно на почтовом шлюзе;
– возможность создание отказоустойчивой кластерной конфигурации веб-шлюза;
– возможность создание отказоустойчивой кластерной конфигурации почтового шлюза;
– предотвращение информационных утечек при выполнении заданий сетевой печати, с функциями оптического распознавания текста (OCR), без использования агентов на конечных компьютерах.

Требования подсистеме в части сканирования информации в сети:

– сканирование файлов с информацией ограниченного доступа на серверах и АРМ пользователей, без установки агентов на целевые системы, с возможностью запуска произвольного сценария немедленной автоматической реакции (перемещение, удаление, шифрование и т.д.);
– сканирование информации ограниченного доступа в таблицах СУБД по протоколу ODBC, без установки агентов на целевые системы;
– система должна иметь возможность масштабирования за счет балансировки нагрузки одного сканера на несколько одновременно работающих анализаторов.

Требования подсистеме в части управления и ведения отчетности:

– наличие единой веб-консоли, сочетающей функции управления инцидентами безопасности и контроля почтовых очередей;
– ведение системой транспортного журнала, фиксирующего получение каждого сообщения, с возможностью поиска по следующим полям:
    - уникальный идентификатор сообщения Message ID;
    - дата/время;
    - отправитель;

- получатель;
- результат сканирования со ссылкой на инцидент (при наличии блокировки);
- состояние сообщения (доставлено, в очереди, удалено).

– единая настройка политик для данных в движении (Data-in-Motion), используемых данных (Data-in-Use) и хранимых данных (Data-at-Rest);
– классификация информации ограниченного доступа по содержимому и местоположению;
– определение сотрудников, имеющих право на обработку и пересылку информации ограниченного доступа;
– учет действий системы и сотрудников, ответственных за обеспечение информационной безопасности по каждому инциденту, отображаемый в виде истории;
– ролевое разграничение прав доступа ответственных за обеспечение информационной безопасности по управлению инцидентами в зависимости от типа информации ограниченного доступа;
– система учета инцидентов полного цикла, отслеживающая состояние каждого инцидента и ответственных исполнителей;
– наличие подсистемы определения имен пользователей для инцидентов, сгенерированных сетевыми сканерами веб-каналов;
– автоматическое прикрепление ко всем инцидентам справочных данных о нарушителе, подразделении, телефоне на основе данных из службы каталога; отображение информации в системе учета инцидентов;
– автоматическое прикрепление к инцидентам необходимых фактов в виде копий сообщений со всеми вложениями;
– выбор реакции при нарушении политики безопасности, включающий варианты: Аудит, Блокирование, Уведомление руководителю сотрудника, Уведомление отправителю, Уведомление администратору безопасности, Перенаправление электронной почты на шлюз шифрования, Запуск произвольного сценария, удаление файлового вложения.

Требования к возможностям интеграции подсистемы с ИТ-инфраструктурой:

– возможность установки удаленного анализатора на канал каждой площадки;
– децентрализованный анализ данных с единой системой управления;
– бесперебойная работа анализаторов утечек данных при потере связности с центральным сервером управления;
– сохранение полного набора всех имеющихся аналитических средств (включая цифровые отпечатки) при потере связности анализатора на удаленной площадке с сервером управления;
– пассивный мониторинг утечек информации по каналам SMTP, HTTP, FTP, IM с подключением через SPAN- (MIRROR-) порт коммутатора Ethernet;

– инспектирование веб-трафика HTTP/HTTPS исключительно средствами собственного веб-шлюза без использования протокола ICAP;
– интеграция со службами каталогов по протоколу LDAP с поддержкой Microsoft Active Directory, Microsoft Active Directory Application Mode, IBM Lotus Domino.

4.2.6. Требования к подсистеме обнаружения вторжений

Подсистема обнаружения вторжений предназначена для обнаружения атак на основе анализа сетевого трафика на сетевом и транспортном уровнях стандартной модели взаимодействия открытых систем.

Подсистема обнаружения вторжений должна выполнять следующие функции в системе:

– работу системы обнаружения вторжений на сетевом уровне;
– использование сигнатурного метода анализа;
– обнаружения в режиме реального времени несанкционированной сетевой активности;
– протоколирование всех событий, возникающих при срабатывании правил обнаружения;
– возможность аудита протоколированных событий.

Средства подсистемы обнаружения вторжений должны быть сертифицированы ФСТЭК России.

4.2.7. Требования к подсистеме антивирусной защиты

Подсистема антивирусной защиты предназначена для противодействия угрозам программно-математического воздействия.

Программный интерфейс средств антивирусной защиты, включая средства управления, должен быть на русском языке.

Средства антивирусной защиты, включая средства управления, должны обладать контекстной справочной системой на русском языке.

Средства антивирусной защиты должны включать:

– программные средства антивирусной защиты рабочих станций и серверов;
– программные средства централизованного управления, мониторинга и обновления;
– обновляемые базы данных сигнатур вредоносных программ и атак;
– эксплуатационную документацию на русском языке.

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

– регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток;
– множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
– проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Средства антивирусной защиты должны быть совместимы с уже существующими на объектах Службы крови средствами управления подсистемой антивирусной защиты.

Средства подсистемы антивирусной защиты должны быть сертифицированы ФСТЭК России.

4.2.8. Требования к подсистеме анализа защищённости

Подсистема анализа защищенности должна быть реализована на базе специализированных программных средств (сканеров безопасности).

Архитектура подсистемы анализа защищенности должна предусматривать размещение всех функциональных компонентов подсистемы в рамках локальной вычислительной сети Заказчика.

Подсистема анализа защищенности должна обеспечивать:

- выявление и анализ уязвимостей, связанных с ошибками в конфигурации системного и прикладного программного обеспечения, которые могут быть использованы нарушителем для реализации атаки на систему;
- контроль установки обновлений программного обеспечения;
- контроль состава технических средств, программного обеспечения и средств защиты информации;
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- анализ функционирования подсистемы межсетевого экранирования на основе имитации внешних атак;

Средства подсистемы анализа защищенности должны быть сертифицированы ФСТЭК России.

4.2.9. Требования к подсистеме криптографической защиты

Подсистема криптографической защиты информации предназначена для защиты информации ограниченного доступа, при ее передаче по каналам связи, в том числе в информационных системах общего пользования, путем использования криптографических преобразований.

Подсистема должна обеспечивать шифрование произвольного объема IP-трафика как между рабочими станциями, так и между серверами и рабочими станциями. Средства криптографической защиты, применяемые в составе подсистемы, должны иметь как программно-аппаратную, так и программную реализацию, для установки на рабочие станции.

Программно-аппаратные комплексы средств криптографической защиты должны обеспечивать поддержание не менее 10 одновременных защищенных соединений с возможностью их дальнейшего увеличения без модернизации защищенной виртуальной сети.

В подсистеме криптографической защиты должны быть реализованы следующие функции:

- выработка ключей, соответствующих ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р34.10-2001;
- создание узлов защищенной сети (криптографические шлюзы и клиенты), удаление узлов защищенной сети, определение политик связей защищённых узлов между

собой, определение политики безопасности и формирование списков прикладных задач для узлов защищенной сети;

- автоматическая рассылка справочной и ключевой информации;
- проведение автоматического обновления программного обеспечения криптошлюзов и криптографических клиентов;
- формирование симметричных ключей связи узлов (криптошлюзы и криптографические клиенты) между собой;
- формирование сертификатов электронно-цифровой подписи формата X.509 v.3;
- ведение списков отозванных сертификатов электронно-цифровой подписи;
- наличие модуля гарантированной доставки обновления справочно-ключевой информации на криптошлюзы и криптографические клиенты;

Специальное программное средство криптографической защиты, предназначенное для установки на рабочие станции пользователей, должно соответствовать следующим требованиям:

- поддерживать ОС MS Windows (XP, Vista, 7 (32/64bit), 2008 (32/64bit)) или эквивалентные;
- обеспечивать защиту (конфиденциальность, подлинность и целостность) IP- трафика (приложений, систем управления и служебного трафика ОС), передаваемого между защищаемыми рабочими станциями пользователей посредством шифрования;
- поддерживать прозрачную работу через устройства статической и динамической NAT/PAT маршрутизации;
- обеспечивать возможность зашифрованного взаимодействия между защищаемыми узлами по протоколу TCP/IP на основе заданной политики безопасности и связям;
- передавать файлы между участниками защищенного взаимодействия с подтверждением доставки, без установки дополнительного ПО;
- обеспечивать возможность предоставления дополнительных сервисных функций для оперативного защищенного обмена циркулярными сообщениями, проведения текстовых конференций;
- программное обеспечение должно шифровать каждый IP-пакет на симметричном ключе связи с другим клиентом, выработанном в ПО, реализующем функции управления защищённой сетью;
- обеспечивать возможность удаленного централизованного обновления адресной и ключевой информации комплекса с контролем прохождения обновления;
- взаимодействие с другими рабочими станциями с установленным СПО с использованием технологии «клиент-клиент».

Криптографические средства должны реализовываться в виде специального программного обеспечения или программно-аппаратных комплексов, сертифицированных ФСБ России на соответствие требованиям к стойкости СКЗИ по классу защиты не ниже КС2.

4.3. Требования к видам обеспечения

4.3.1. Требования к программному обеспечению

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

ПО базовых средств защиты информации, входящих в состав СЗИ, должно соответствовать требованиям руководящих документов ФСТЭК России и/или ФСБ России.

4.3.2. Требования к техническому обеспечению

СЗИ должна функционировать на всех технических средствах, входящих в состав объектов информатизации. Точное количество и состав технических средств определяется на этапе обследования. При необходимости Исполнитель осуществляет приведение в соответствие набора технических средств, использующихся в работе СЗИ, требованиям действующего законодательства РФ в сфере защиты информации и персональных данных в государственных информационных системах. При этом технические средства должны соответствовать единому архитектурному решению.

Решения по использованию технических средств должны приниматься с учетом обеспечения поддержки его функционирования производителем или поставщиком данных технических средств.

4.3.3. Требования к организационному обеспечению

Создаваемая система не должна затрагивать организационную структуру подразделений и должна минимально влиять на конфигурацию существующей ИТ-инфраструктуры Заказчика.

5. Требования к составу и содержанию работ по модернизации систем защиты информации и аттестации объектов Службы крови

5.1. Требования к порядку (последовательности, этапам) выполнения работ

Работы по модернизации систем защиты информации и аттестации объектов Службы крови должны в себя включать следующие этапы:

- обследование объектов Службы крови на соответствие требованиям по защите информации ограниченного доступа в государственных информационных системах;
- разработка организационно-распорядительной, нормативно-методической и эксплуатационной документации в области обработки и защиты информации ограниченного доступа в государственных информационных системах на объектах Службы крови;
- разработка технических решений на модернизацию систем защиты информации объектов Службы крови;
- внедрение систем защиты информации на объектах Службы крови;
- исследование уязвимостей информационных систем и систем защиты информации объектов Службы крови с применением специальных средств анализа защищенности;
- разработка комплектов документов, необходимых для проведения аттестации объектов Службы крови на соответствие требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах;
- проведение аттестационных испытаний объектов Службы крови по требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах.

Работы должны быть организованы таким образом, чтобы не нарушать технологический процесс в сфере заготовки, переработки, хранения и транспортировки крови и ее компонентов.

5.2. Требования к выполнению работ по обследованию объектов Службы крови на соответствие требованиям по защите информации ограниченного доступа в государственных информационных системах

Целью проведения работ по обследованию объектов Службы крови на соответствие требованиям по защите информации ограниченного доступа в государственных информационных системах является:

- сбор информации о процессах обработки информации ограниченного доступа и существующей ИТ-инфраструктуре объектов Службы крови;
- сбор и анализ информации о текущем состоянии мер по обеспечению информационной безопасности объектов Службы крови;
- оценка соответствия процессов обработки и защиты информации ограниченного доступа требованиям действующего законодательства;

Работы по обследованию проводятся на объектах Заказчика, указанных в Приложении № 1 и Приложении № 2 к настоящему ТЗ.

В ходе выполнения работ по обследованию Исполнитель должен разработать и согласовать с заказчиком документ: «Методика проведения обследования», содержащий подход Исполнителя к проведению обследования и график выезда на объекты Заказчика.

Работы по обследованию объектов Службы крови должны включать:

- сбор исходных данных о категориях обрабатываемой информации, технологиях и режимах обработки информации;
- сбор исходных данных о квалификации персонала, обслуживающего средства защиты информации;
- сбор исходных данных о реализованных организационных и технических мерах по обеспечению информационной безопасности;
- разработку рекомендаций по подготовке объекта к внедрению средств защиты информации;
- разработку отчетов по результатам обследования;
- определение актуальных угроз и актуальных нарушителей безопасности информации;
- проведение классификации информационных систем ОСК;
- разработку требований на модернизацию систем защиты информации для ОСК.

Отчет об обследовании объекта Службы крови должен содержать:

- результаты анализа внутренних документов, регламентирующих порядок обработки и защиты информации ограниченного доступа;
- результаты анализа состава и структуры информационных систем;
- перечень реализованных технических и организационных мер защиты информации, оценку их достаточности и соответствия требованиям нормативных документов РФ;
- результаты степени участия персонала в обработке информации ограниченного доступа и характера взаимодействия персонала между собой;
- описание и анализ информационных потоков информации ограниченного доступа, с учетом всего ее жизненного цикла: от сбора до уничтожения;
- схемы ЛВС объекта;
- схемы размещения рабочих мест
- вывод по результатам обследования.

По результатам выполнения работ по каждому объекту Службы крови должен быть разработан следующий комплект документов:

- Отчет об обследовании объекта Службы крови.
- Модель угроз и модель нарушителя безопасности информации.
- Акт классификации.
- Техническое задание на модернизацию системы защиты информации.

5.3. Требования к разработке организационно-распорядительной, нормативно-методической и эксплуатационной документации в области обработки и защиты информации ограниченного доступа в государственных информационных системах на объектах Службы крови

Целью разработки организационно-распорядительной, нормативно-методической и эксплуатационной документации является формирование комплекта документов для объектов Службы крови в соответствие с требованиями действующего законодательства РФ в сфере защиты информации и персональных данных в государственных информационных системах.

По результатам работ по разработке организационно-распорядительных, нормативно-методических и эксплуатационных документов для каждого объекта Службы крови должен быть разработан следующий комплект документов:

- Приказ об определении подразделений и лиц, ответственных за эксплуатацию средств защиты информации.
- Приказ о назначении ответственного за обеспечение безопасности информации ограниченного доступа.
- Приказ о создании комиссии по классификации информационных систем.
- Приказ о вводе системы защиты информации в эксплуатацию.
- Политика в отношении обработки персональных данных.
- Положение о порядке хранения и уничтожения носителей информации.
- Положение о порядке организации и проведения работ по защите информации ограниченного доступа.
- Порядок резервного копирования информации.
- Инструкция администратора информационной безопасности.
- Инструкция пользователя системы защиты информации.
- Инструкция по антивирусной защите.
- Инструкция по парольной защите.
- Инструкция о порядке обращения с носителями информации ограниченного доступа.
- Журналы учета машинных носителей информации.
- Перечень пользователей, допущенных к обработке информации ограниченного доступа и лиц, допущенных в помещение.
- Перечень обрабатываемой информации ограниченного доступа.

5.4. Требования к разработке технических решений на модернизацию систем защиты информации объектов Службы крови

Целью разработки технических решений на модернизацию систем защиты информации является формирование проектной документации на реализацию СЗИ объектов Службы крови в соответствии с требованиями Технических заданий, разработанных по результатам обследования и действующего законодательства.

В рамках разработки технических решений для каждого объекта Службы крови должны быть разработаны следующие проектные документы на модернизацию СЗИ:

– Ведомость технического проекта.
– Пояснительная записка к техническому проекту.
– Описание комплекса технических средств.
– Схема организационной структуры.
– Схема структурная комплекса технических средств.
– Ведомость покупных изделий.

В рамках разработки технических решений должна быть разработана эксплуатационная документация в следующем составе:

– Ведомость эксплуатационных документов.
– Описание технологического процесса обработки данных.
– Инструкция по эксплуатации комплекса технических средств
– Инструкция о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав системы защиты информации.

5.4.1. Разработка программы и методики приемо-сдаточных испытаний

В рамках разработки технических решений для каждого из видов приемо-сдаточных испытаний должны быть разработаны программы и методики испытаний:

– Программа и методика предварительных испытаний;
– Программа и методика опытной эксплуатации;
– Программа и методика приемочных испытаний.

Программа и методика предварительных испытаний должна содержать:

– перечень объектов испытаний;
– состав предъявляемой документации;
– описание проверяемых взаимосвязей между объектами испытаний;
– очередность испытаний частей СЗИ;
– порядок и методы испытаний, в том числе состав программных средств и оборудования, необходимых для проведения испытаний.

Программа и методика опытной эксплуатации должна содержать:

– условия и порядок функционирования СЗИ;
– сроки опытной эксплуатации;
– порядок устранения недостатков, выявленных в процессе опытной эксплуатации.

Программа и методика приемочных испытаний должна содержать:

– критерии приемки СЗИ;
– условия и сроки проведения испытаний;
– средства для проведения испытаний;
– перечень лиц, ответственных за проведение испытаний;
– методику испытаний и обработки их результатов;
– перечень оформляемой документации.

5.5. Требования к внедрению систем защиты информации на объектах Службы крови

Работы по внедрению систем защиты информации объектов Службы крови должны быть выполнены в рамках адаптированного и согласованного проектного решения. Система защиты информации должна включать головной центр управления системы защиты информации, подчиненные центры управления СЗИ, а также местные системы защиты информации.

Работы по реализации системы защиты информации на каждом объекте Службы крови включать:

- поставку исполнителем средств защиты информации;
- пусконаладочные работы по модернизации системы защиты информации;
- предварительные испытания системы защиты информации;
- опытную эксплуатацию системы защиты информации;
- приемочные испытания системы защиты информации.

Исполнитель поставляет средства защиты информации (программное обеспечение и оборудование) в соответствии со спецификациями, приведенными в Приложении №3 и Приложении №4 к настоящему Техническому заданию.

Требования к поставляемым средствам защиты информации приведены в разделе 4.2 настоящего Технического задания.

Испытания и приемка системы защиты информации представляют собой процесс проверки функционирования системы, определения и проверки соответствия характеристик системы требованиям настоящего Технического задания, а также выявления и устранения недостатков в работе системы и в разработанной документации.

5.5.1. Предварительные испытания

Предварительные испытания СЗИ проводятся Исполнителем в присутствии представителей Заказчика для определения её работоспособности и решения вопроса о возможности приемки СЗИ в опытную эксплуатацию. Предварительные испытания следует выполнять после проведения Исполнителем отладки и тестирования поставляемых программных и технических средств СЗИ, и предоставления им соответствующих документов о готовности СЗИ к испытаниям, а также после ознакомления персонала СЗИ с эксплуатационной документацией.

Предварительные испытания проводятся в соответствии с документом «Программа и методика предварительных испытаний».

Предварительные испытания СЗИ проводятся путем выполнения автономных тестов в каждой из подсистем защиты:

- в подсистеме управления доступом и учетными данными пользователей;
- в подсистеме регистрации событий безопасности;
- в подсистеме обеспечения целостности;
- в подсистеме межсетевого экранирования;
- в подсистеме защиты от утечек информации;
- в подсистеме обнаружения вторжений;
- в подсистеме антивирусной защиты;

– в подсистеме анализа защищённости;
– в подсистеме криптографической защиты.

По результатам предварительных испытаний формируется протокол, который должен содержать заключение о возможности (невозможности) приемки СЗИ в опытную эксплуатацию, а также перечень необходимых доработок и рекомендуемые сроки их выполнения.

Предварительные испытания завершаются оформлением акта приемки СЗИ в опытную эксплуатацию.

5.5.2. Опытная Эксплуатация

Опытная эксплуатация СЗИ проводится с целью определения характеристик СЗИ и готовности персонала Заказчика к работе в реальных условиях функционирования СЗИ , а также определения фактической эффективности СЗИ и, при необходимости, корректировки документации.

Опытная эксплуатация проводится в соответствии с документом «Программа и методика опытной эксплуатации».

По результатам опытной эксплуатации СЗИ принимается решение о возможности (невозможности) предъявления системы на приемочные испытания.

Опытная эксплуатация завершается оформлением акта о завершении опытной эксплуатации.

5.5.3. Приемочные испытания

Приемочные испытания СЗИ проводятся для определения соответствия СЗИ требованиям Технического задания, оценки качества опытной эксплуатации и решения вопроса о возможности приемки СЗИ в промышленную эксплуатацию.

Приемочные испытания проводятся в соответствии с документом «Программа и методика приемочных испытаний».

Приемочные испытания СЗИ проводятся Исполнителем в присутствии представителей Заказчика путем выполнения комплексных тестов.

Комплексный тест должен соответствовать указанным требованиям:
– быть логически увязанным;
– обеспечивать проверку выполнения функций подсистем и частей СЗИ во всех режимах функционирования, в том числе связей между ними;
– обеспечивать проверку реакции системы на некорректную информацию и аварийные ситуации.

По результатам приемочных испытаний формируется протокол, который должен содержать следующие разделы:
– назначение испытаний СЗИ;
– состав технических и программных средств, используемых при испытании;
– указание методик, в соответствии с которыми проводились испытания, обработка и оценка результатов;
– условия проведения испытаний и характеристики исходных данных;

– обобщенные результаты испытаний;
– выводы о результатах испытаний и соответствии модернизированной системы требованиям Технического задания.

5.6. Требования к работам по исследованию уязвимостей информационных систем и систем защиты информации объектов Службы крови с применением специальных средств анализа защищенности

Работы по исследованию уязвимостей информационных систем и систем защиты информации объектов Службы крови с применением специальных средств анализа защищенности должны включать:

– анализ и оценку уровня эффективности подсистем защиты;
– инструментальный анализ защищенности информационных систем и систем защиты информации.

До начала работ по исследованию уязвимостей Исполнитель должен разработать и согласовать с Заказчиком документ «Методика проведения исследования уязвимостей», содержащий подход Исполнителя к проведению исследования уязвимостей и график исследования объектов Заказчика.

В рамках работ по анализ и оценке уровня эффективности подсистем защиты выполняется оценка реализованных защитных мер в части:

– защиты периметра сети;
– сегментирования сети;
– контроля доступа к оборудованию;
– межсетевого экранирования;
– обнаружения вторжений;
– криптографической защиты;
– контроля целостности;
– предотвращения атак;
– защиты от утечек;
– анализа защищенности;
– идентификации и аутентификации пользователей систем;
– управления доступом к конфиденциальной информации;
– контроля доступа к портам и устройствам;
– регистрации и учета;
– антивирусной защиты;
– мониторинга и аудита;
– резервирования и восстановления данных;
– настроек параметров безопасности систем, обрабатывающих информацию конфиденциального характера;
– управления изменениями;
– управления обновлениями безопасности программного обеспечения;

– управления носителями конфиденциальной информации и ключевой информации;

– централизованного управления системой защиты информации.

Инструментальный анализ защищенности информационных систем и систем защиты информации, с целью выявления уязвимостей и определения уровня защищенности информационных систем, состоящий из:

– внешней части теста на проникновение, при проведении которого осуществляется:

  ▪ сбор и анализ общедоступной информации, информации о информационных системах с помощью поисковых систем, через регистрационные базы данных (DNS, Whois и т. п.) и другие публичные источники информации;

  ▪ проведение инвентаризационного сканирования открытых портов и активных сервисов на внешнем сетевом периметре;

  ▪ сбора информации и формирование списка целей для атак;

  ▪ выявление уязвимостей систем и ресурсов внешнего сетевого периметра (включая веб-приложения), эксплуатация которых может привести к компрометации ресурса и/или к получению неавторизованного доступа к критичной информации;

  ▪ разработка векторов и реализация методов проникновения в информационные системы Заказчика;

  ▪ выполнение попытки получения доступа к внутренним информационным системам и ресурсам объекта информатизации и местам хранения/обработки информации ограниченного доступа.

– из работ внутри объектов заказчика, при проведении которых осуществляется:

  ▪ идентификация доступных в пределах размещения объекта информатизации точек беспроводного доступа и анализ возможности проникновения через них в информационные системы Заказчика;

  ▪ сбор информации о сетевых сервисах, операционных системах и приложениях, доступных из сегмента пользователей локальной сети и определение мест обработки (хранения) информации ограниченного доступа;

  ▪ реализация попытки получения учетных записей и другой критичной информации путём перехвата сетевого трафика;

  ▪ выявление уязвимостей ресурсов, способных привести к возможности осуществления несанкционированных воздействий на них;

  ▪ разработка векторов и реализация методов получения несанкционированного доступа к ключевым ресурсам информационных систем с учетом анализа полученных данных;

  ▪ выполнение попытки получения несанкционированного доступа к серверам, базам данных и рабочим станциям пользователей с использованием уязвимостей программного обеспечения, сетевого оборудования, некорректных настроек и найденных учетных записей.

– из работ по инструментальному анализу защищенности АРМ, серверов, коммутационного оборудования, операционных систем и других узлов сети объектов Службы крови в целях обнаружения уязвимостей установленного сетевого программного и аппаратного обеспечения, необходимо выполнить:
  - определение доступности узлов проверяемой сети;
  - определение открытых TCP и UDP портов на узлах проверяемой сети;
  - верификацию типа операционной системы, установленной на проверяемом узле сети;
  - верификацию сетевых сервисов;
  - определение NetBios-имени проверяемого узла сети;
  - определение DNS-имени проверяемого узла сети;
  - проверку учетных записей для узлов сети, функционирующих под управлением операционных систем;
  - определение наличия и доступности общих сетевых ресурсов на проверяемых узлах сети;
  - сопоставление служб и сервисов, запущенных на узлах сети, назначенным по умолчанию портам;
  - проверку известных уязвимостей операционных систем;
  - проверку известных уязвимостей сервиса FTP;
  - проверку известных уязвимостей сервиса RPC;
  - проверку узлов сети на наличие DOS-уязвимости (отказ в обслуживании);
  - проверку наличия удаленного доступа к приложениям;
  - проверку возможности получения прав удаленного администратора;
  - проверку наличия паролей по умолчанию;
  - подбор паролей через SMB;
  - проверку других известных уязвимостей информационных систем.

По результатам выполнения работ по исследованию уязвимостей информационных систем и систем защиты информации объектов Службы крови с применением специальных средств анализа защищенности необходимо разработать Отчет об обнаруженных уязвимостях по результатам инструментального анализа защищенности для каждого объекта Службы крови.

5.7. Требования к разработке комплектов документов, необходимых для проведения аттестации объектов Службы крови на соответствие требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах

Для каждого объекта Службы крови должен быть разработан комплект документов, необходимый для прохождения аттестационных испытаний, в следующем составе:

– Перечень защищаемых информационных систем (ресурсов).

– Матрица доступа к разделяемым информационным ресурсам.

– Технический паспорт на систему защиты информации (включает перечень технических средств обработки информации, перечень средств защиты информации и схему размещения компонентов системы защиты информации).
– Программа и методика аттестационных испытаний.

5.8. Требования к проведению аттестационных испытаний объектов Службы крови по требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах

При проведении аттестационных испытаний объектов Службы крови аттестационная комиссия должна руководствоваться требованиями следующих законодательных актов и нормативно-методических документов:

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
– Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
– Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
– Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282.
– Положение по аттестации объекта информатизации по требованиям безопасности информации, Гостехкомиссия России, 1994 г.

При проведении аттестационных испытаний объектов Службы крови должны использоваться следующие методы проверок и испытаний:

– Экспертно-документальный метод. Экспертно-документальный метод предусматривает проверку соответствия объекта информатизации требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации требованиям по выбору, размещению, монтажу и эксплуатации технических средств объекта.
– Проверка функций (комплекса функций) защиты информации от несанкционированного доступа с использованием тестирующих средств. Проверка и испытания функций или комплекса функций защиты информации от НСД с помощью тестирующих средств выполняется с применением специальных

сертифицированных программных тестирующих средств, методом пробного пуска средств защиты или путем применения попыток «взлома» систем защиты информации.

При проведении аттестационных испытаний на каждом из объектов Службы крови проверяются следующие подсистемы защиты:

- подсистема управления доступом и учетными данными пользователей;
- подсистема регистрации событий безопасности;
- подсистема обеспечения целостности;
- подсистема межсетевого экранирования;
- подсистема защиты от утечек информации;
- подсистема обнаружения вторжений;
- подсистема антивирусной защиты;
- подсистема анализа защищённости;
- подсистема криптографической защиты.

Аттестационные испытания проводятся в соответствии с разработанным Исполнителем и согласованным Заказчиком документом «Программа и методика аттестационных испытаний».

По результатам прохождения аттестационных испытаний для каждого ОСК должен быть выдан комплект документов в следующем составе:

- Протокол проведения аттестационных испытаний.
- Заключение по результатам аттестационных испытаний.
- Аттестат соответствия требованиям безопасности информации.

5.9. Сроки выполнения работ и перечень документов, предъявляемых по результатам выполнения этапов работ

По результатам выполнения этапов работ Исполнитель разрабатывает и передает Заказчику документы, указанные в таблице 1.

Таблица 1. Документы, предъявляемые по результатам выполнения работ

№ этапа	Наименование этапа	Документы, предъявляемые по результатам работ
1.	Обследование объектов Службы крови на соответствие требованиям по защите информации ограниченного доступа в государственных информационных системах	Методика проведения обследования. **Для каждого ОСК:** – Отчет об обследовании объекта Службы крови. – Модель угроз и модель нарушителя безопасности информации. – Акт классификации. – Техническое задание на модернизацию системы защиты информации.
2.	Разработка организационно-распорядительной, нормативно-методической	**Для каждого ОСК:** – Приказ об определении подразделений и лиц, ответственных за эксплуатацию средств защиты информации.

	и эксплуатационной документации в области обработки и защиты информации ограниченного доступа в государственных информационных системах на объектах Службы крови	– Приказ о назначении ответственного за обеспечение безопасности информации ограниченного доступа. – Приказ о создании комиссии по классификации информационных систем. – Приказ о вводе системы защиты информации в эксплуатацию. – Политика в отношении обработки персональных данных. – Положение о порядке хранения и уничтожения носителей информации. – Положение о порядке организации и проведения работ по защите информации ограниченного доступа. – Инструкция администратора информационной безопасности. – Инструкция пользователя системы защиты информации. – Порядок резервного копирования информации. – Инструкция по антивирусной защите. – Инструкция по парольной защите. – Инструкция о порядке обращения с носителями информации ограниченного доступа. – Журналы учета машинных носителей информации. – Перечень пользователей, допущенных к обработке информации ограниченного доступа и лиц, допущенных в помещение. – Перечень обрабатываемой информации ограниченного доступа.
3.	Разработка технических решений на модернизацию систем защиты информации объектов Службы крови	**Для каждого ОСК:** – Ведомость технического проекта. – Пояснительная записка к техническому проекту. – Описание комплекса технических средств. – Схема организационной структуры. – Схема структурная комплекса технических средств. – Ведомость покупных изделий. – Ведомость эксплуатационных документов. – Описание технологического процесса обработки данных. – Инструкция по эксплуатации комплекса технических средств – Инструкция о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав системы защиты информации. – Программа и методика предварительных испытаний; – Программа и методика опытной эксплуатации; – Программа и методика приемочных испытаний.
4.	Внедрение систем защиты информации на объектах	**Для каждого ОСК:** – Протокол предварительных испытаний.

	Службы крови	– Акт приемки СЗИ в опытную эксплуатацию. – Акт о завершении опытной эксплуатации СЗИ. – Протокол приемочных испытаний. – Акт о вводе СЗИ в промышленную эксплуатацию.
5.	Исследование уязвимостей информационных систем и систем защиты информации объектов Службы крови с применением специальных средств анализа защищенности	Методика проведения исследования уязвимостей. **Для каждого ОСК:** – Отчет об обнаруженных уязвимостях по результатам инструментального анализа защищенности.
6.	Разработка комплектов документов, необходимых для проведения аттестации объектов Службы крови на соответствие требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах	**Для каждого ОСК:** – Перечень защищаемых информационных систем (ресурсов). – Матрица доступа к разделяемым информационным ресурсам. – Технический паспорт на систему защиты информации. – Программа и методика аттестационных испытаний.
7.	Проведение аттестационных испытаний объектов Службы крови по требованиям действующего законодательства РФ в сфере защиты информации ограниченного доступа в государственных информационных системах	**Для каждого ОСК:** – Протокол проведения аттестационных испытаний. – Заключение по результатам аттестационных испытаний. – Аттестат соответствия требованиям безопасности информации.

6. Порядок контроля и приемки

6.1. Виды, состав, объем и методы испытаний системы защиты информации

Виды, состав, объем, и методы испытаний СЗИ определены в разделах 5.5 и 5.8 настоящего Технического задания.

В состав испытаний СЗИ объекта информатизации, должны быть включены проверки соответствия системы требованиям ТЗ и условиям Договора:

- полноты и качества реализации функций, указанных в ТЗ;
- комплектности СЗИ объекта информатизации;
- комплектности и качества документации;
- степени выполнения требований функционального назначения разработанных подсистем СЗИ объекта информатизации.

Должны быть предусмотрены следующие виды испытаний:

- предварительные испытания;
- опытная эксплуатация;
- приёмочные испытания.

Испытания СЗИ должны быть организованы и проведены в соответствии с ГОСТ 34.603-89 «Информационная технология. Виды испытаний автоматизированных систем».

6.2. Согласование отчетных материалов

По результатам работ по каждому этапу Исполнитель предоставляет Заказчику отчетные материалы в соответствии с таблицей 1 настоящего Технического задания.

Содержание отчетных материалов согласуется на уровне специалистов Заказчика и Исполнителя исходя из требований к содержанию работ, указанных в разделе 5. Отчетные документы, разработанные для объектов Службы крови, согласовываются и утверждаются уполномоченным сотрудником соответствующего ОСК.

Срок согласования отчетных материалов Заказчиком составляет 5 дней с момента предоставления материалов Исполнителем.

6.3. Общие требования к приемке работ

Контроль и приемка работ осуществляются на основании настоящего Технического задания и Договора.

Приёмка результатов выполнения работ по этапам оформляется Актом сдачи-приемки работ. Основанием для составления и подписания Акта сдачи-приемки работ является предоставление Исполнителем согласованного с Заказчиком комплекта отчетных документов, либо (при проведении испытаний), утвержденных сторонами Актов приемки.

Документация и другие результаты работ передаются Заказчику на основании Акта приема-передачи отчетной документации.

Предусмотренные испытания СЗИ объектов Службы крови проводятся приемочной комиссией.

7. Требования к документированию

Виды, комплектность и содержание документов в части, определенной настоящим ТЗ, должны учитывать требования ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплексность и обозначение документов при создании автоматизированных систем» и РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов».

Вся разрабатываемая документация, а также штатная документация по поставляемому оборудованию и программному обеспечению должна быть выполнена на русском языке.

Документация, разрабатываемая (изменяемая) Исполнителем в рамках выполнения работ по настоящему Техническому заданию, передается Заказчику в 2-х экземплярах в бумажном (сброшюрованном) виде и, дополнительно, в электронном виде на оптическом носителе.

8. Требования к технической поддержке и гарантиям качества по выполненным работам

8.1. Требования к гарантиям качества

Гарантия должна распространяться на все виды выполненных работ, поставляемое оборудование и программное обеспечение.

Гарантийный срок, в течение которого выявленные Заказчиком дефекты устраняются за счет Исполнителя – не менее 12 месяцев со дня подписания сторонами акта сдачи-приемки выполненных работ по заключительному этапу Плана-графика выполненных работ, а также актов приема-передачи прав и оборудования.

Гарантийные обязательства по СЗИ объектов Службы крови включают:

- предоставления пояснений (консультаций) по вопросам Заказчика, связанным с функционированием СЗИ или их аттестационными испытаниями;
- выезда на объекты Заказчика в случае проведения на указанных объектах проверок уполномоченными органами (ФСБ России, ФСТЭК России, Роскомнадзор);
- внесения изменений в настройки средств защиты информации или эксплуатационную документацию при поступлении соответствующих запросов со стороны Заказчика;
- устранение любых выявленных в процессе приемки и эксплуатации скрытых ошибок, возникших по вине Исполнителя, за счет Исполнителя.

8.2. Требования к технической поддержке

На период выполнения работ в соответствии с разделами 5.2 - 5.8 настоящего ТЗ Исполнитель обеспечивает присутствие на каждом объекте Заказчика своих представителей в рабочее время (для объектов работающих круглосуточно – в круглосуточном режиме), имеющих достаточную квалификацию для работы с внедряемыми системами защиты информации, а также с системой АИСТ, как основной производственной системой Заказчика для обработки персональных данных. При этом Исполнитель должен представить список своих представителей и их контактные данные.

В течение 12 месяцев со дня подписания сторонами акта сдачи-приемки выполненных работ Исполнитель обеспечивает круглосуточную техническую поддержку систем защиты информации Заказчика, реализованных в рамках выполнения работ по настоящему ТЗ. Исполнитель обязан обеспечить время реагирования на запросы Заказчика не более 8 часов.

Приложение №1. Перечень объектов Службы крови

№ п/п	Наименование объекта	Адрес объекта	Кол-во АРМ	Кол-во серверов
1.	ФГБУ «ГНЦ» Минздравсоцразвития России	г. Москва Новозыковский пр. 4а	30	3
2.	ГБУЗ "Калужская областная станция переливания крови"	г. Калуга,ул.М.Горького,71	62	5
3.	ГБУ Ростовской области "Станция переливания крови"	г. Ростов-на-Дону, ул. Ченцова, д. 71	62	5
4.	ГБУЗ "Станция переливания крови" ДЗ КК	г. Краснодар, ул. Димитрова,166	62	5
5.	Государственное бюджетное учреждение здравоохранения Пензенская областная станция переливания крови	г. Пенза, ул. Клары Цеткин, 41а	62	2
6.	Государственное бюджетное учреждения здравоохранения Астраханской области "Областной центр крови"	г. Астрахань, ул. Кубанская, д. 1Б	62	5
7.	Государственное бюджетное учреждение Республики Марий Эл "Республиканская станция переливания крови"	г. Йошкар-Ола, ул. Пролетарская, д. 66	62	5
8.	Бюджетное учреждение Чувашской Республики «Республиканская станция переливания крови» Министерства здравоохранения и социального развития Чувашской Республики	г. Чебоксары, ул. Пирогова, д. 9	62	5
9.	Государственное бюджетное учреждение Республики Дагестан "Республиканская станция переливания крови"	г. Махачкала, ул. Атаева, 3	62	5
10.	Государственное бюджетное учреждение здравоохранения Республики Карелия "Республиканская станция переливания крови"	г. Петрозаводск, ул. Пирогова, д. 4-а.	57	2
11.	Федеральное государственное бюджетное учреждение здравоохранения "Станция переливания крови Федерального медико-биологического агентства в г. Екатеринбурге"	г. Екатеринбург, ул. Соликамская, д.6	30	5
12.	Областное государственное бюджетное учреждение здравоохранения «Костромская областная станция переливания крови»	г. Кострома, пр. Мира, д. 106	62	5
13.	Бюджетное учреждение здравоохранения Воронежской области "Воронежская областная станция переливания крови"	г. Воронеж, ул. Транспортная, д. 56	62	5

14.	Государственное бюджетное учреждение здравоохранения "Иркутская областная станция переливания крови"	г. Иркутск, ул. Байкальская, д. 122	62	2
15.	Государственное бюджетное учреждение здравоохранения "Бурятская республиканская станция переливания крови МЗ РБ"	г. Улан-Удэ, ул. Пирогова, д. 7-а	62	5
16.	Государственное казенное учреждение здравоохранения "Краевая станция переливания крови"	г. Чита, ул. Балябина, д.5	62	5
17.	ФГБУЗ СПК ФМБА России в г. Челябинске	г. Челябинск, ул. Воровского, 51	30	3
18.	ФГБУ Российский НИИ гематологии и трансфузиологии ФМБА России	г. Санкт-Петербург, ул. 2-я Советская, д.16	30	3
19.	Федеральное государственное бюджетное учреждение “Научный центр сердечно-сосудистой хирургии им. А.Н. Бакулева" РАМН	г. Москва, Рублевское шоссе, д. 135	27	3
20.	Краевое государственное бюджетное учреждение здравоохранения "Алтайский краевой центр крови"	г. Барнаул , пр-т Ленина, д. 197	43	2
21.	Государственное бюджетное учреждение здравоохранения "Краевая станция переливания крови"	г. Владивосток, ул. Октябрьская, 6	41	5
22.	Краевое государственное казённое учреждение здравоохранения "Красноярский краевой центр крови №1"	г. Красноярск, ул. П. Железняка, 3-М	41	5
23.	Государственное бюджетное учреждение здравоохранения Новосибирской области "Новосибирский центр крови"	г. Новосибирск, ул. Серафимовича, 2/1	37	2
24.	Государственное бюджетное учреждение здравоохранения "Пермская краевая станция переливания крови"	г. Пермь, ул. Лебедева, 54	41	5
25.	Краевое государственное бюджетное учреждение здравоохранения "Станция переливания крови" министерства здравоохранения Хабаровского края	г. Хабаровск, ул. Волочаевская, д.46	41	2
26.	Областное государственное бюджетное учреждение здравоохранения "Смоленский центр крови"	г. Смоленск, ул. Ковтюха, д.6 г. Смоленск, ул. Чернышевского, д.9	41	5
27.	Бюджетное учреждение здравоохранения Удмуртской Республики "Республиканская станция переливания крови Министерства здравоохранения Удмуртской Республики"	Удмуртская Республика, г. Ижевск, ул. Воткинское шоссе, д.79	41	5

28.	Государственное бюджетное учреждение здравоохранения Республики Мордовия "Мордовская республиканская станция переливания крови"	Республика Мордовия, г. Саранск, ул. Дальняя, д. 3А	41	5
29.	Государственное бюджетное учреждение здравоохранения Архангельской области "Архангельская станция переливания крови"	г. Архангельск, пр-т Ломоносова, 311	41	5
30.	Бюджетное учреждение здравоохранения Орловской области "Орловская станция переливания крови"	г. Орел, Наугорское шоссе, 2	41	2
31.	Государственное казенное учреждение здравоохранения "Рязанская областная станция переливания крови"	г. Рязань, ул. Спортивная, 7	41	5
32.	Государственное бюджетное учреждение Республики Саха (Якутия) "Станция переливания крови"	г. Якутск, Республика Саха (Якутия), ул. Петра Алексеева, 87	43	5
33.	Государственное бюджетное учреждение здравоохранения Республиканская станция переливания крови Министерства здравоохранения республики Башкортостан	г. Уфа, Республика Башкирия, ул. Батырская, д.41/1	43	5
34.	Государственное бюджетное учреждение здравоохранения "Камчатская краевая станция переливания крови"	г. Петропавловск-Камчатский, ул. Курчатова, 17	41	5
35.	Государственное автономное учреждение здравоохранения " Республиканская станция переливания крови Министерства здравоохранения Республики Татарстан"	г. Казань, ул. Ново-Азинсксая д.33 г. Казань, ул. Сибирский тракт д.33	41	5
36.	Кировское областное государственное казенное учреждение здравоохранения "Кировский центр крови"	г. Киров, ул. Красноармейская, 74	41	5
37.	Государственное казенное учреждение здравоохранения Кемеровской области "Кемеровский областной центр крови"	г. Кемерово, пр. Октябрьский, 22	41	5
38.	Государственное бюджетное учреждение здравоохранения МОСПК.	г. Магадан, ул. Потапова, д. 2	41	5
39.	Государственное бюджетное учреждение здравоохранения "Оренбургская областная станция переливания крови"	г. Оренбург, ул. Аксакова, 32	41	5
40.	Государственное бюджетное учреждение здравоохранения Свердловской области "Свердловская областная станция переливания крови"	г. Первоуральск, ул. Медиков, д.10	41	5

41.	Государственное бюджетное учреждение здравоохранения Псковской области "Станция переливания крови Псковской области"	г. Псков, Интернациональный переулок, 4	41	2
42.	Государственное бюджетное учреждение здравоохранения " Областная станция переливания крови"	г. Южно-Сахалинск, пр-т Мира, д.430	41	5
43.	Государственное областное бюджетное учреждение здравоохранения "Мурманская областная станция переливания крови"	г. Мурманск, ул. Павлова, дом 6, корп.10	41	5
44.	Федеральное государственное бюджетное учреждение науки "Кировский НИИ Гематологии и переливания крови ФМБА России"	г. Киров, ул. Красноармейская, 72	27	3
45.	Государственное учреждение "Республиканская станция переливания крови"	Республика Коми, г. Сыктывкар, Октябрьский проспект, 59	41	5
46.	Федеральное государственное бюджетное учреждение здравоохранения Клиническая больница № 172 ФМБА России	Ульяновская обл., г. Димитровград, ул. Тоси Потаповой д.171.	30	5
47.	ГУЗ «Республиканская станция переливания крови» МЗ РСО-Алания»	г. Владикавказ, ул. Барбашова, д. 37	43	2
Итого:			**2137**	**198**

Приложение №2. Перечень лечебно-профилактических учреждений

№ п/п	Наименование ЛПУ	Кол-во АРМ
	г. Астрахань	
1.	Областной наркологический диспансер	1
2.	Республиканский противотуберкулезный диспансер	1
3.	Областной кожно-венерологический диспансер	1
4.	Областной центр по профилактике и борьбе со СПИД и инфекционными заболеваниями	1
5.	Областная клиническая психиатрическая больница	1
6.	Управление Роспотребнадзора по Астраханской области	1
	г. Улан – Удэ	
7.	ЛПУ РКВД	1
8.	ЛПУ РЦПСиИЗ	1
9.	ЛПУ ЦГиЭвРБ	1
10.	Республиканский наркологический диспансер	1
11.	ЛПУ РПНД	1
12.	ЛПУ РКПТД	1
	г. Воронеж	
13.	Воронежский клинико-диагностический психоневрологический диспансер	1
14.	Воронежский областной клинический кожно-венерологический диспансер	1
15.	Воронежский областной центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
16.	Воронежский областной наркологический диспансер	1
17.	Воронежский областной клинический противотуберкулезный диспансер	1
	г. Махачкала	
18.	Республиканский кожно-венерологический диспансер	1
19.	Республиканский центр по профилактике и борьбе со СПИДом	1
20.	Республиканский наркологический диспансер	1
21.	Республиканский противотуберкулезный диспансер	1
22.	Республиканский психоневрологический диспансер	1
23.	Республиканский центр инфекционных болезней	1
	г. Иркутск	
24.	Иркутский областной центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
25.	Иркутский областной психоневрологический диспансер	1
26.	Центр гигиены и эпидемиологии в Иркутской области	1
27.	Иркутский областной противотуберкулезный диспансер	1
28.	Областной кожно-венерологический диспансер	1

	г. Калуга	
29.	Центр гигиены и эпидемиологии	1
30.	Областная туберкулезная больница	1
31.	Республиканский наркологический диспансер	1
32.	Калужский областной центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
33.	Республиканский кожно-венерологический диспансер	1
	г. Петрозаводск	
34.	Республиканский кожно-венерологический диспансер	1
35.	Республиканский центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
36.	Республиканский противотуберкулезный диспансер	1
	г. Кострома	
37.	Костромской областной противотуберкулезный диспансер	1
38.	Костромской областной наркологический диспансер	1
39.	Костромская областная психиатрическая больница	1
40.	Областной кожно-венерологический диспансер г. Костромы	1
	г. Краснодар	
41.	Центр гигиены и эпидемиологии в Краснодарском крае	1
42.	Клинический кожно-венерологический диспансер	1
43.	Клинический центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
44.	Наркологический диспансер	1
45.	Клинический противотуберкулезный диспансер	1
	г. Йошкар – Ола	
46.	Центр гигиены и эпидемиологии в Республике Марий-Эл	1
47.	Республиканский психоневрологический диспансер	1
48.	Республиканский противотуберкулезный диспансер	1
49.	Республиканский наркологический диспансер	1
50.	Республиканский центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
51.	Республиканский кожно-венерологический диспансер	1
	г. Пенза	
52.	Областная психиатрическая больница	1
53.	Областной противотуберкулезный диспансер	1
54.	Пензенский областной центр специализированных видов медицинской помощи	1
55.	Центр гигиены и эпидемиологии в Пензенской области	1
56.	Областная наркологическая больница	1
57.	Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1

	г. Ростов-на-Дону	
58.	Кожно-венерологический диспансер	1
59.	Противотуберкулезный клинический диспансер	1
60.	Психоневрологический диспансер	1
61.	Центр по борьбе со СПИДом и инфекционными заболеваниями	1
62.	Центр гигиены и эпидемиологии в Ростовской области	1
	г. Чита	
63.	Краевой кожно-венерологический диспансер	1
64.	Управление Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Забайкальскому краю	1
65.	Краевой наркологический диспансер	1
66.	Краевой центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
67.	Краевой противотуберкулезный диспансер Забайкальского края	1
	г. Чебоксары	
68.	Республиканская психиатрическая больница	1
69.	Республиканский противотуберкулезный диспансер	1
70.	Республиканский кожно-венерологический диспансер	1
71.	Республиканский наркологический диспансер	1
72.	Республиканский центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями	1
73.	Центр гигиены и эпидемиологии	1
	г. Уфа	
74.	ГУЗ «Республиканский наркологический диспансер №1 Минздрава Республики Башкортостан»	1
75.	ГУЗ «Республиканский противотуберкулезный диспансер Минздрава Республики Башкортостан»	1
76.	ГУЗ «Республиканский кожно-венерологический диспансер Минздрава Республики Башкортостан»	1
77.	ГУЗ «Республиканская психиатрическая больница№1 Минздрава Республики Башкортостан»	1
78.	ГУЗ «Республиканский центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями Минздрава Республики Башкортостан»	1
	г. Первоуральск	
79.	ФГУЗ «Федеральный Центр гигиены и эпидемиологии» г. Екатеринбург	1
80.	ОГУЗ «Свердловский областной кожно-венерологический диспансер» г. Екатеринбург	1
81.	ГУЗ «Свердловская областная клиническая психиатрическая больница» г. Екатеринбург	1
82.	ОГУЗ «Противотуберкулезный диспансер» г. Екатеринбург	1
83.	ГУЗ «Свердловская областная клиническая психиатрическая больница №3» г. Екатеринбург	1

	г. Южно – Сахалинск	
84.	ФГУЗ «Центр гигиены и эпидемиологии в Сахалинской области»	1
85.	ГУЗ «Сахалинский областной противотуберкулезный диспансер»	1
86.	«Сахалинский областной центр по профилактике и борьбе со СПИДом»	1
87.	ГУЗ «Сахалинская областная психиатрическая больница»	1
88.	ГУЗ «Сахалинский областной наркологический диспансер»	1
89.	ГУЗ «Сахалинский областной кожно-венерологический диспансер»	1
	г. Владивосток	
90.	ФГУЗ «Центр гигиены и эпидемиологии в Приморском крае»	1
91.	ГУЗ «Краевой противотуберкулезный диспансер»	1
92.	ГУЗ «Краевой клинический центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
93.	ГУЗ «Краевая клиническая психиатрическая больница»	1
94.	ГУЗ «Краевой наркологический диспансер»	1
95.	ГУЗ «Краевой клинический кожно-венерологический диспансер»	1
	г. Архангельск	
96.	ГУЗ «Архангельский областной клинический кожно-венерологический диспансер»	1
97.	ГУЗ «Архангельский областной психоневрологический диспансер»	1
98.	ГУЗ «Архангельский областной клинический центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
99.	ГУЗ «Областной клинический противотуберкулезный диспансер»	1
100.	ФГУЗ «Центра гигиены и эпидемиологии в Архангельской области»	1
	г. Мурманск	
101.	ГУЗ «Мурманский областной Центр специализированных видов медицинской помощи»	1
102.	ГУЗ «Мурманский областной наркологический диспансер»	1
103.	ГУЗ «Мурманский областной психоневрологический диспансер»	1
104.	ГУЗ «Мурманский областной центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
105.	ГУЗ «Мурманский областной противотуберкулезный диспансер»	1
106.	ФГУЗ «Центр гигиены и эпидемиологии в Мурманской области»	1
	г. Кемерово	
107.	ГУЗ «Кемеровский областной кожно-венерологический диспансер»	1
108.	ГУЗ «Кемеровский Областной Противотуберкулезный Диспансер»	1
109.	ГУЗ «Кемеровская Областная Клиническая Психиатрическая больница»	1
110.	ГУЗ «Областной Центр – СПИДа»	1
111.	ГУЗ «Кемеровский Областной Наркологический Диспансер»	1
112.	ФГУЗ «Центр гигиены и эпидемиологии в Кемеровской области»	1
	г. Ижевск	

113.	ГУЗ «Республиканский кожно-венерологический диспансер»	1
114.	ГУЗ «Республиканский наркологический диспансер»	1
115.	ГУЗ «Республиканская клиническая психиатрическая больница»	1
116.	ГУЗ «Удмуртский республиканский центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
117.	ГУЗ «Республиканская клиническая туберкулезная больница»	1
118.	ФГУЗ «Центр гигиены и эпидемиологии Удмуртской Республике»	1
	г. Пермь	
119.	ГУЗ «Пермская краевая психиатрическая больница»	1
120.	ГУЗ «Краевой наркологический диспансер № 1»	1
121.	ГУЗ «Пермский краевой центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
122.	ГУЗ «Краевой противотуберкулезный диспансер № 1 «Фтизиопульмонология»	1
123.	ФГУЗ «Центр гигиены и эпидемиологии в Пермском крае»	1
124.	ГУЗ «Краевой кожно-венерологический диспансер № 1»	1
	г. Новосибирск	
125.	ГБУЗ НСО «Новосибирский областной наркологический диспансер»	1
126.	«ГБУЗ НСО Государственная Новосибирская клиническая психиатрическая больница № 3»	1
127.	«ГБУЗ НСО ЦЕНТР СПИД»	1
128.	ГБУЗ НСО «Новосибирский областной противотуберкулезный диспансер»	1
129.	ФГУЗ «Центр гигиены и эпидемиологии в Новосибирской области»	1
130.	ГБУЗ НСО «Новосибирский областной кожно-венерологический диспансер»	1
	г. Барнаул	
131.	ГУЗ «Краевой кожно-венерологический диспансер»	1
132.	ГУЗ «Алтайский краевой наркологический диспансер»	1
133.	КГУЗ «Алтайский краевой противотуберкулезный диспансер»	1
134.	ГУЗ «Пермский краевой центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
	г. Казань	
135.	ГБУЗ «Республиканский наркологический диспансер МЗ РТ»	1
136.	ГУЗ «РКПД»	1
137.	ГУЗ «Республиканская клиническая психиатрическая больница им. акад. В.М. Бехтерева»	1
138.	ГУЗ «РЦПБ СПИД и ИЗ МЗ РТ»	1
139.	ФГУЗ «Центр гигиены и эпидемиологии в Республике Татарстан (Татарстан)»	1
	г. Хабаровск	
140.	ГУЗ «Краевой кожно-венерологический диспансер» МЗ ХК»	1
141.	ГУЗ «Краевая психиатрическая больница» МЗ Хабаровского края – наркологический диспансер»	1

142.	ГУЗ «Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями» министерства Хабаровского края»	1
143.	ГУЗ «Противотуберкулезный диспансер» МЗ Хабаровского края»	1
144.	ФГУЗ «Центр Гигиены и Эпидемиологии в Хабаровском крае»	1
145.	ГУЗ «Краевая психиатрическая больница» психиатрического диспансера № 2	1
	г. Якутск	
146.	ГУ «Якутский республиканский кожно-венерологический диспансер»	1
147.	ГУ «Якутский республиканский наркологический диспансер»	1
148.	ГУ «Якутский республиканский центр по профилактике и борьбе со СПИДом»	1
149.	ГУ НПЦ «Фтизиатрия»	1
150.	ФГУЗ «Центр гигиены и эпидемиологии в Республике Саха (Якутия)»	1
	г. Красноярск	
151.	КГБУЗ «Красноярский краевой психоневрологический диспансер №1»	1
	г. Смоленск	1
152.	ОГУЗ «Смоленский кожно-венерологический диспансер»	1
153.	ОГУЗ «Смоленский областной наркологический диспансер»	1
154.	ОГУЗ «Смоленский областной психоневрологический клинический диспансер»	1
155.	ОГУЗ «Смоленский центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
156.	ОГУЗ «Смоленский противотуберкулёзный клинический диспансер»	1
157.	ФГУЗ «Центр гигиены и эпидемиологии в Смоленской области»	1
	г. Орел	
158.	ОГУЗ «Орловского противотуберкулёзного диспансера»	1
159.	ОГУЗ «Орловского наркологического диспансера»	1
160.	ОГУЗ «Орловского областного центра по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
161.	ОГУЗ «Орловского областного кожно-венерологического диспансера»	1
	г. Псков	
162.	ГУЗ «Кожно-венерологического диспансера Псковской области»	1
163.	ГУЗ «Наркологического диспансера Псковской области»	1
164.	ГУЗ «Центра по профилактике и борьбе со СПИДом и инфекционными заболеваниями Псковской области»	1
165.	ГУЗ «Противотуберкулёзного диспансера Псковской области»	1
	г. Саранск	
166.	ГУЗ «Мордовского республиканского кожно-венерологического диспансера»	1
167.	ГУЗ «Республиканского наркологического диспансера»	1
168.	ГУЗ «Республиканского психоневрологического диспансера»	1
169.	ГУЗ «Республиканского центра по профилактике и борьбе со СПИДом инфекционным заболеваниям»	1
170.	ГУЗ «Республиканского противотуберкулёзного диспансера»	1

171.	ФГУЗ «Центра гигиены и эпидемиологии в Республике Мордовия»	1
	г. Рязань	
172.	ГУ «Рязанского областного кожно-венерологического диспансера»	1
173.	ГУЗ «Рязанского областного клинического наркологического диспансера»	1
174.	ГУЗ «Рязанского областного клинического психоневрологического диспансера»	1
175.	ГУЗ «Рязанского областного клинического кожно-венерологического диспансера (Центра СПИД)»	1
176.	ГУЗ «Рязанского областного клинического противотуберкулёзного диспансера»	1
177.	ФГУЗ «Центра гигиены и эпидемиологии в Рязанской области»	1
	г. Магадан	
178.	ГУЗ «Магаданского областного кожно-венерологического диспансера»	1
179.	ГУЗ «Магаданского областного наркологического диспансера»	1
180.	ГУЗ «Магаданского областного психоневрологического диспансера»	1
181.	ГУЗ «Магаданского областного центра по профилактике и борьбе со СПИДом инфекционным заболеваниям»	1
182.	ГУЗ «Магаданского областного противотуберкулёзного диспансера»	1
183.	ФГУЗ «Центра гигиены и эпидемиологии в Магаданской области»	1
	г. Петропавловск - Камчатский	
184.	ГУЗ «Камчатского краевого кожно-венерологического диспансера»	1
185.	ГУЗ «Камчатского краевого наркологического диспансера»	1
186.	ГУЗ «Камчатского краевого психоневрологического диспансера»	1
187.	ФГУЗ «Центра гигиены и эпидемиологии в Камчатском крае»	1
188.	ГУЗ «Камчатского краевого центра по профилактике и борьбе со СПИДом инфекционным заболеваниям»	1
189.	ГУЗ «Камчатского краевого противотуберкулёзного диспансера»	1
	г. Оренбург	
190.	ГУЗ «Оренбургской областной клинический наркологический диспансер»	1
191.	ГУЗ «Оренбургской областной центр по профилактике и борьбе со СПИДом инфекционным заболеваниям»	1
192.	ГУЗ «Оренбургской областной кожно-венерологический диспансер»	1
193.	ГУЗ «Оренбургская областная клиническая психиатрическая больница №1»	1
	г. Киров	
194.	ГЛПУ «Кировский областной клинический кожно-венерологический диспансер»	1
	г. Сыктывкар	
195.	ФГУЗ «Центр гигиены и эпидемиологии в Республике Коми»	1
196.	ГУ РК «Республиканский противотуберкулёзный диспансер»	1
197.	ГУ РК «Республиканский центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»	1
198.	ГУ «Коми психиатрическая больница»	1
199.	ГУ «Коми Республиканский наркологический диспансер»	1

200.	ГУ РК «Республиканский кожно-венерологический диспансер»	1
	г. Владикавказ	
201.	ГУЗ «Республиканский кожно-венерологический диспансер» МЗ РСО-Алания»	1
202.	ГУЗ «Республиканский наркологический диспансер»» МЗ РСО-Алания»	1
203.	ГУЗ «Республиканский Центр по профилактике и борьбе со СПИД и инфекционным заболеваниям» МЗ РСО-Алания»	1
204.	ГУЗ «Республиканский противотуберкулёзный диспансер»» МЗ РСО-Алания»	1
205.	ФГУЗ «Центр гигиены и эпидемиологии в РСО-Алания»	1
	Итого:	**205**

Приложение №3 Перечень поставляемого ПО

№	Серийный (заводской) номер, марка, модель и т.п.	Производитель	Наименование (описание) Лицензии	Единица измерения	Количество в единицах измерения
1	SC-29-KC2	VipNet	Передача права на использование ПО ViPNet Client 3.x (КС2)	шт.	205
2		Центр специальной системотехники	Приобретение базы данных сигнатур компьютерных атак для Аппаратно-программного комплекса обнаружения компьютерных атак "Аргус" (АПК Аргус) версии 1.5, право на использование на одном АПК Аргус в течение одного года.	шт.	47
3		Центр специальной системотехники	Приобретение лицензий на программное обеспечение "Аргус" версии 1.5.	шт.	47
4	(XS7.8-IP128)	Positive Technologies	Предоставление прав на использование XSpider 7.8, лицензия на 128 хоста, гарантийные обязательства в течение 1 года	шт.	12
5	(XS7.8-IP64)	Positive Technologies	Предоставление прав на использование XSpider 7.8, лицензия на 64 хоста, гарантийные обязательства в течение 1 года	шт.	33
6	(XS7.8-IP32)	Positive Technologies	Предоставление прав на использование XSpider 7.8, лицензия на 32 хоста, гарантийные обязательства в течение 1 года	шт.	2
7	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	51
8	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования	шт.	73

			(50-99 endpoint)		
9	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
10	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	50
11	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	72
12	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
13	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	73
14	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	69
15	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	51
16	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	72
17	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
18	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования	шт.	71

			(50-99 endpoint)		
19	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	72
20	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
21	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	73
22	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
23	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	50
24	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	70
25	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	51
26	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
27	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	62
28	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования	шт.	52

			(50-99 endpoint)		
29	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	72
30	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
31	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
32	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
33	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	52
34	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	73
35	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	53
36	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	73
37	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	72
38	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования	шт.	52

			(50-99 endpoint)		
39	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (50-99 endpoint)	шт.	53
40	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	49
41	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	35
42	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	35
43	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	47
44	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	30
45	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	47
46	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	33
47	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	30
48	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования	шт.	45

			(25-49 endpoint)		
49	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	47
50	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	47
51	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	33
52	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	49
53	KL4863RA*DS	Kaspersky lab	Kaspersky Endpoint Security для бизнеса – Стандартный. Лицензия на право использования (25-49 endpoint)	шт.	33
54		Oracle	Identity and Access Management Suite Plus	шт.	2540
55		Oracle	Identity Manager Connector	шт.	1
56		Oracle	Oracle Database SE	шт.	1
57	P73-05762	Microsoft	Microsoft® Windows® Server Standard 2012 Sngl OPEN 1 License No Level 2 PROC	шт.	2
58	R18-04281	Microsoft	Microsoft® Windows® Server CAL 2012 Sngl OPEN 1 License No Level User CAL User CAL	шт.	2541
59	7NQ-00213	Microsoft	SQLSvrStdCore 2012 RUS OLP 2Lic NL CoreLic Qlfd	шт.	8

Приложение №4 Перечень поставляемого оборудования

№ п/п	Индекс (и/или серийный, заводской номер, марка, модель оборудования и т.п.)	Производитель	Наименование Оборудования	Ед. изм.	Количество, в единицах измерения
1.	SC-119-1000	VipNet	ViPNet Coordinator HW1000	шт.	49
2	TCS-119-1000	VipNet	Техническое сопровождение ПАК ViPNet Coordinator HW1000	шт.	49
3	TSC-29-KC2	VipNet	Техническое сопровождение ПО ViPNet Client 3.x (КС2)	шт.	205
4.		Центр специальной системотехники	Документация, база данных сигнатур компьютерных атак текущей версии, дополнительное программное обеспечение на CD	шт.	47
5.		Центр специальной системотехники	Носитель информации для изготовления лицензионного DOM-модуля с программным обеспечением "Аргус" версии 1.5	шт.	47
6.		Центр специальной системотехники	Сертификат на техническую поддержку Аппаратно-программного комплекса обнаружения компьютерных атак "Аргус" (АПК Аргус) версии 1.5 в течение одного года для одного АПК Аргус.	шт.	47
	KL8067RMZZZ	Kaspersky lab	Kaspersky Certified Media Pack Customized	шт.	47
		Oracle	Стандартная техническая поддержка лицензионного програмного обеспечение Oracle Database Standard Edition	шт.	1
7.		Oracle	Стандартная техническая поддержка лицензионного програмного обеспечение Oracle Identity Manager	шт.	2540
8.		Oracle	Стандартная техническая поддержка лицензионного програмного обеспечение Oracle Identity Manager Connector	шт.	1
9.	654081-B21	HP	Сервер HP DL360p Gen8 8-SFF CTO Server	шт.	2
10.	654770-L21	HP	Процессор HP DL360p Gen8 E5-2640 FIO Kit	шт.	2
11.	669320-B21	HP	Модуль оперативной памяти HP 2GB 1Rx8 PC3-12800E-11 Kit	шт.	16

12.	652605-B21	HP	Жесткий диск HP 146GB 6G SAS 15K 2.5in SC ENT HDD	шт.	16
13.	652238-B21	HP	Оптический привод HP 9.5mm SATA DVD ROM Jb Kit	шт.	2
14.	684208-B21	HP	Сетевой адаптер HP Ethernet 1GbE 4P 331FLR FIO Adptr	шт.	2
15.	663201-B21	HP	Монтажный комплект HP 1U SFF BB Gen8 Rail Kit	шт.	2
16.	503296-B21	HP	Блок электропитания HP 460W CS Gold Ht Plg Pwr Supply Kit	шт.	2
17.	H1K92A3 7G2	HP	Техническая поддержка на 3 года HP Proliant DL36x(p) HW Support	шт.	2
18.	668812-421	HP	HP DL360e Gen8 E5-2403 4LFF Entry EU	шт.	2
19.	647893-B21	HP	HP 4GB 1Rx4 PC3L-10600R-9 Kit	шт.	6
20.	658071-B21	HP	HP 500GB 6G SATA 7.2k 3.5in SC MDL HDD	шт.	4
21.	503296-B21	HP	HP 460W CS Gold Ht Plg Pwr Supply Kit	шт.	2
22.	661530-B21	HP	HP DL360eGen8 Redundant Fan Kit	шт.	2
23.	U6D55E	HP	HP 3y Nbd DL360e ProCare Service	шт.	2
24.	C6N36AAE	HP	HP Insight Control ML/DL/BL Bundle E-LTU	шт.	2
25.	654081-B21 B19	HP	Многоязычная локализация Europe - Multilingual Localization	шт.	2
26.	669320-B21 0D1	HP	Заводская сборка Factory integrated	шт.	2
27.	652605-B21 0D1	HP	Заводская сборка Factory integrated	шт.	2
28.	652238-B21 0D1	HP	Заводская сборка Factory integrated	шт.	2
29.	663201-B21 0D1	HP	Заводская сборка Factory integrated	шт.	2
30.	503296-B21 0D1	HP	Заводская сборка Factory integrated	шт.	2
31.	H1K92A3	HP	Техническая поддержка на 3 года HP 3Y 4 hr 24x7 Proactive Care SVC	шт.	2
32.	WDSS-C-CP12-N	Websense	Код активации подписки Websense Data Security Suit	шт.	2540
33.	PRT-Y-CP12-N	Websense	Код активации подписки Premium Support - Triton	шт.	1