Описание объекта закупки - Техническое задание
на оказание в области информационной безопасности в Министерстве образования и молодежной политики Свердловской области

1. Общие сведения

1.1. Объекты защиты

Информационные системы персональных данных (далее – ИСПДн), состоящие из 9 автоматизированных рабочих мест (далее – АРМ):

- ИСПДн «Стипендиаты Губернатора» (включает АРМ № 1);
- ИСПДн «Сведения о педагогических работниках для выплаты пособия» (включает АРМ № 1);
- ИСПДн «Аттестация педагогов» (включает АРМ № 2);
- ИСПДн «Обеспечение кадровой деятельности» (включает АРМ №№ 3-8);
- ИСПДн «Противодействие коррупции» (включает АРМ № 8);
- ИСПДн «Подросток» (включает АРМ № 9).

1.2. Состав услуг

Услуги включают:

- поставка средств защиты информации;
- установка и настройка средств защиты информации;
- **аттестация информационных систем персональных данных.**

Перечень необходимых средств защиты информации приведен в Приложении № 1.

Технические требования к поставляемым средствам защиты информации приведены в Приложении № 2.

1.2.1. Место оказания услуг: Министерство образования и молодежной политики Свердловской области (г. Екатеринбург, ул. Малышева, 33; г. Екатеринбург, ул. Малышева, 101).

1.3. Основание оказания услуг

Основаниями оказания настоящих услуг являются:

- наличие у учреждения: информационных систем, в которых осуществляется обработка информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в частности, персональных данных;
- требования законодательства Российской Федерации в области защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

2. Назначение и цели создания системы защиты объекта информатизации

2.1. Назначение системы защиты

Система защиты объектов информатизации предназначена для обеспечения выполнения требований Федерального закона РФ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»; Федерального закона РФ № 152-ФЗ от 27 июля 2006 г. «О персональных данных».

2.2. Цели создания системы защиты объекта информатизации

Основными целями создания системы защиты объектов информатизации являются:

- защита информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, обрабатываемой в информационных системах, от неправомерного или случайного доступа к ней, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения ее, а также от иных неправомерных действий в ее отношении за счёт комплексного использования организационных, программных, программно-аппаратных средств и мер защиты;
- выполнение требований законодательства по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.
-

2.3. Цели аттестации объекта информатизации

Целью аттестации объектов информатизации является оценка эффективности реализованных в рамках системы защиты мер по обеспечению безопасности информации в соответствии с национальными стандартами ограниченного распространения. Требования к системе защиты объекта информатизации

3. Требования законодательства в сфере защиты информации

Для объектов информатизации мероприятиями по защите информации, обрабатываемой на объекте информатизации, будут являться меры, соответствующие выполнению требований:

- Федерального закона РФ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;
- Федерального закона РФ № 152-ФЗ от 27.07.2006 г. «О персональных данных»;
- Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа Федерального агентства правительственной связи и информации при Президенте РФ от 13.06.2001 г. № 152 «Об утверждении инструкции по организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказа ФСБ РФ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказа 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»;
- Приказа ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

3.1. Требования к системе защиты объектов информатизации в целом

Для реализации мероприятий по обеспечению безопасности информации, обрабатываемой на объекте информатизации, Исполнитель должен создать систему защиты информации, обрабатываемой на объектах информатизации.

3.2. Требования к надёжности

Элементы системы защиты объектов информатизации должны удовлетворять условиям работы в круглосуточном режиме, а также иметь возможность восстановления в случаях сбоев.

Должна быть предусмотрена техническая поддержка средств защиты информации сроком на один год. Техническая поддержка должна включать в себя:

- консультации и ответы на вопросы по электронной почте.

3.3. Требования к организационному обеспечению

На момент проведения Аттестации у Заказчика должны быть подготовлены следующие документы (в случае их отсутствия Исполнитель разрабатывает документы; в случае их наличия Исполнитель проверяет их актуальность и полноту содержания):

- документ о назначении ответственного за организацию обработки персональных данных;
- документ о назначении администратора информационной безопасности;
- акт классификации ИСПДн «Обеспечение кадровой деятельности» по требованиям безопасности;
- акт оценки вреда субъектам персональных данных, чьи персональные данные обрабатываются в ИСПДн «Обеспечение кадровой деятельности»;

- документ о мероприятиях по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн «Обеспечение кадровой деятельности», включающий:
  - назначение ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн «Обеспечение кадровой деятельности»;
  - перечень персональных данных, обрабатываемых в ИСПДн «Обеспечение кадровой деятельности»;
  - перечень сотрудников, имеющих право доступа к персональным данным, обрабатываемым в ИСПДн «Обеспечение кадровой деятельности»;
  - границы контролируемой зоны ИСПДн «Обеспечение кадровой деятельности»;
  - перечень помещений, в которых осуществляется обработка персональных данных в ИСПДн «Обеспечение кадровой деятельности»;
  - перечень сотрудников, имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ИСПДн «Обеспечение кадровой деятельности»;
  - назначение ответственного пользователя средств криптографической защиты информации (далее — СКЗИ) ИСПДн «Обеспечение кадровой деятельности»;
  - перечень мест размещения СКЗИ и их пользователей;
  - матрицу доступа пользователей к защищаемым информационным ресурсам ИСПДн «Обеспечение кадровой деятельности»;
- акт классификации ИСПДн «Противодействие коррупции» по требованиям безопасности;
- акт оценки вреда субъектам персональных данных, чьи персональные данные обрабатываются в ИСПДн «Противодействие коррупции»;
- документ о мероприятиях по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн «Противодействие коррупции», включающий:
  - назначение ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн «Противодействие коррупции»;
  - перечень персональных данных, обрабатываемых в ИСПДн «Противодействие коррупции»;
  - перечень сотрудников, имеющих право доступа к персональным данным, обрабатываемым в ИСПДн «Противодействие коррупции»;
  - границы контролируемой зоны ИСПДн «Противодействие коррупции»;
  - перечень помещений, в которых осуществляется обработка персональных данных в ИСПДн «Противодействие коррупции»;
  - перечень сотрудников, имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ИСПДн «Противодействие коррупции»;
  - назначение ответственного пользователя СКЗИ ИСПДн «Противодействие коррупции»;
  - перечень мест размещения СКЗИ и их пользователей;
  - матрицу доступа пользователей к защищаемым информационным ресурсам ИСПДн «Противодействие коррупции»;
- акт классификации ИСПДн «Стипендиаты Губернатора» по требованиям безопасности;
- акт оценки вреда субъектам персональных данных, чьи персональные данные обрабатываются в ИСПДн «Стипендиаты Губернатора»;
- документ о мероприятиях по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн «Стипендиаты Губернатора», включающий:
  - назначение ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн «Стипендиаты Губернатора»;

- перечень персональных данных, обрабатываемых в ИСПДн «Стипендиаты Губернатора»;
- перечень сотрудников, имеющих право доступа к персональным данным, обрабатываемым в ИСПДн «Стипендиаты Губернатора»;
- границы контролируемой зоны ИСПДн «Стипендиаты Губернатора»;
- перечень помещений, в которых осуществляется обработка персональных данных в ИСПДн «Стипендиаты Губернатора»;
- перечень сотрудников, имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ИСПДн «Стипендиаты Губернатора»;
- назначение ответственного пользователя СКЗИ ИСПДн «Стипендиаты Губернатора»;
- перечень мест размещения СКЗИ и их пользователей;
- матрицу доступа пользователей к защищаемым информационным ресурсам ИСПДн «Стипендиаты Губернатора»;

– акт классификации ИСПДн «Сведения о педагогических работниках для выплаты пособия» по требованиям безопасности;

– акт оценки вреда субъектам персональных данных, чьи персональные данные обрабатываются в ИСПДн «Сведения о педагогических работниках для выплаты пособия»;

– документ о мероприятиях по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн «Сведения о педагогических работниках для выплаты пособия», включающий:

- назначение ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- перечень персональных данных, обрабатываемых в ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- перечень сотрудников, имеющих право доступа к персональным данным, обрабатываемым в ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- границы контролируемой зоны ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- перечень помещений, в которых осуществляется обработка персональных данных в ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- перечень сотрудников, имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- матрицу доступа пользователей к защищаемым информационным ресурсам ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- назначение ответственного пользователя СКЗИ ИСПДн «Сведения о педагогических работниках для выплаты пособия»;
- перечень мест размещения СКЗИ и их пользователей.

– акт классификации ИСПДн «Аттестация педагогов» по требованиям безопасности;

– акт оценки вреда субъектам персональных данных, чьи персональные данные обрабатываются в ИСПДн «Аттестация педагогов»;

– документ о мероприятиях по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн «Аттестация педагогов», включающий:

- назначение ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн «Аттестация педагогов»;
- перечень персональных данных, обрабатываемых в ИСПДн «Аттестация педагогов»;
- перечень сотрудников, имеющих право доступа к персональным данным, обрабатываемым в ИСПДн «Аттестация педагогов»;

- границы контролируемой зоны ИСПДн «Аттестация педагогов»;
- перечень помещений, в которых осуществляется обработка персональных данных в ИСПДн «Аттестация педагогов»;
- перечень сотрудников, имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ИСПДн «Аттестация педагогов»;
- матрицу доступа пользователей к защищаемым информационным ресурсам ИСПДн «Аттестация педагогов»;
- назначение ответственного пользователя СКЗИ ИСПДн «Аттестация педагогов»;
- перечень мест размещения СКЗИ и их пользователей;

– акт классификации ИСПДн «Подросток» по требованиям безопасности;

– акт оценки вреда субъектам персональных данных, чьи персональные данные обрабатываются в ИСПДн «Подросток»;

– документ о мероприятиях по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн «Подросток», включающий:

- назначение ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн «Подросток»;
- перечень персональных данных, обрабатываемых в ИСПДн «Подросток»;
- перечень сотрудников, имеющих право доступа к персональным данным, обрабатываемым в ИСПДн «Подросток»;
- границы контролируемой зоны ИСПДн «Подросток»;
- перечень помещений, в которых осуществляется обработка персональных данных в ИСПДн «Подросток»;
- перечень сотрудников, имеющих право доступа в помещения, в которых осуществляется обработка персональных данных в ИСПДн «Подросток»;
- назначение ответственного пользователя СКЗИ ИСПДн «Подросток»;
- перечень мест размещения СКЗИ и их пользователей;
- матрицу доступа пользователей к защищаемым информационным ресурсам ИСПДн «Подросток».

Исполнитель разрабатывает следующие документы:

– Модель угроз ИСПДн;

– Требования по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– Описание технологического процесса обработки персональных данных в ИСПДн;

– Описание системы защиты ИСПДн;

– Технический паспорт ИСПДн.

4. Услуги по установке и настройке средств защиты информации.

Исполнителем оказываются услуги по установке и настройке поставляемых средств защиты информации.

Средства защиты информации настраиваются таким образом, чтобы обеспечивать выполнение всех необходимых требований федеральных законов, нормативных документов РФ, ФСТЭК России и ФСБ России к защите персональных данных при их обработке в ИСПДн.

5. Аттестация

Аттестация объекта информатизации включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации требованиям по защите информации.

Аттестации подлежат объекты информатизации, указанные в п. 1.1 настоящего Технического задания.

В качестве исходных данных, необходимых для аттестации, используются: модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, проектная и эксплуатационная документация на систему защиты, организационно-распорядительные документы по защите информации, результаты анализа угроз безопасности информации информационной системы. Аттестация проводится в соответствии с программой и методиками аттестационных испытаний.

Для проведения аттестации применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В результате оказания услуг по аттестации Исполнителем разрабатываются следующие документы:

- программа и методики аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации;
- протокол аттестационных испытаний на соответствие требованиям по защите информации от несанкционированного доступа ИСПДн;
- заключение по результатам аттестационных испытаний на соответствие требованиям безопасности информации ИСПДн.

В случае положительного заключения по результатам аттестационных испытаний объекта информатизации выдается аттестат соответствия по требованиям безопасности информации ИСПДн.

6. Обязательные требования к Исполнителю

Исполнитель должен иметь следующие лицензии:

1) Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации на следующие виды работ:
   - контроль защищенности конфиденциальной информации от утечки по техническим каналам;
   - контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
   - проектирование в защищенном исполнении: средств и систем информатизации;
   - аттестационные испытания и аттестация на соответствие требованиям по защите информации;
   - установка, монтаж, наладка, испытания, ремонт средств защиты информации.
2) Лицензия ФСБ России на осуществление 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 на следующие виды работ:
   - передача шифровальных (криптографических) средств;
   - монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;
   - работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства.

7. Приложения к Техническому заданию:

- Приложение № 1 «Количество поставляемых средств защиты информации»;
- Приложения № 2 «Технические требования к поставляемым средствам защиты информации»;

Приложение № 1
к техническому заданию

Количество поставляемых средств защиты информации

№ п/п	Наименование	Объем поставки	
		Единица измерения	Кол-во
1	Право на использование модуля защиты от НСД и контроля устройств Средства защиты информации Secret Net Studio 8 (или эквивалент)	лицензия	8
2	Право на использование модуля обнаружения и предотвращения вторжений Средства защиты информации Secret Net Studio 8 на 1 год (или эквивалент)	лицензия	8
3	Право на использование модуля персонального межсетевого экрана Средства защиты информации Secret Net Studio 8 (или эквивалент)	лицензия	2
4	Сертификат активации сервиса технической поддержки СЗИ Secret Net Studio 8 (или эквивалент)	шт.	8
5	Kaspersky Стандартный Certified Media Pack (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	шт.	1
6	Передача неисключительных прав на использование ПО ViPNet Client 4.x (КС2)* (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	лицензия	3
7	Сертификат активации сервиса совместной технической поддержки ПО ViPNet Client на 1 год* (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	шт.	3
8	Передача права на использование ПО ViPNet Client 4.x (КС2)** (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	лицензия	1
9	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client на 1 год** (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	шт.	1
10	Компакт-диск с дистрибутивом ПО ViPNet** (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	шт.	1
11	Передача неисключительных прав на использование ПО ViPNet Client 4.x (КС1)*** (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	лицензия	1
12	Компакт-диск с дистрибутивом ПО ViPNet*** (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	шт.	1
13	Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client 4.x (КС1) на 1 год*** (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	шт.	1

* Сеть ViPNet № 2057.

** Сеть ViPNet № 1274.

*** Сеть ViPNet № 3395

Приложение № 2
к техническому заданию

Технические требования к поставляемым средствам защиты информации:

Наименование	Технические требования
Право на использование модуля защиты от НСД и контроля устройств Средства защиты информации Secret Net Studio 8 Производитель ООО «Код безопасности» Страна происхождения – Россия (или эквивалент)	***Должно осуществлять:*** • защиту серверов и рабочих станций от НСД; • контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; • разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации; • разграничение доступа пользователей к информации; • контроль утечек информации; • регистрацию событий безопасности и аудит. ***Требования к сертификации и применению в информационных системах:*** СЗИ должно соответствовать требованиям документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности, «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) не ниже 4 класса защиты, «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.П3 (ФСТЭК России, 2014). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля. СЗИ должно допускать использование в следующих информационных системах: • автоматизированные системы - до класса 1Г (включительно); • государственные информационные системы – до 1 класса защищенности (включительно); • информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно); • автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно). СЗИ должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин. ***Требования к операционной платформе и аппаратной части:*** • СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы): o Windows 10; o Windows 8/8.1; o Windows 7 SP1; o Windows Vista SP2; o Windows Server 2012/2012 R2; o Windows Server 2008 SP2/2008 R2 SP1. • Должна быть возможность установки СЗИ по произвольному пути. • СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix. • СЗИ должно поддерживать работу на виртуальных машинах, функционирующих в системах виртуализации, построенных на базе гипервизоров VMware ESX(i) и Microsoft Hyper-V. • СЗИ с централизованным управлением должно функционировать совместно с Microsoft Active Directory; • СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ. • В инфраструктуре должно быть в наличии устройство, считывающее DVD (для чтения установочного диска – хотя бы на одном компьютере в информационной системе). ***Требования к функциональности СЗИ:*** СЗИ должно выполнять следующие функции по защите информации: • Контроль входа пользователей в систему и работа пользователей в системе:

Наименование	Технические требования
	○ проверка пароля пользователя при входе в систему; ○ поддержка аппаратных средств аутентификации: - идентификаторы iButton (типы DS1992 — DS1996); - USB-ключи eToken PRO, eToken PRO (Java), Rutoken, Rutoken S, Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash, JaCarta-2 PKI/ГОСТ, JaCarta SF/ГОСТ, ESMART Token; - контактные смарт-карты eToken PRO, eToken PRO (Java), Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, JaCarta ГОСТ, ESMART Token, ESMART Token ГОСТ с любыми совместимыми USB-считывателями; ○ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора; ○ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI); ○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI); ○ возможность блокирования входа в систему локальных пользователей; ○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей; ○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности; ○ возможность управления политикой сложности паролей; ○ поддержка возможности входа в систему по сертификатам; ○ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей. • Избирательное (дискреционное) управление доступом: ○ возможность назначения прав доступа на файлы, каталоги, принтеры, устройства; ○ возможность наследования прав доступа для файлов, каталогов и устройств; ○ возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту. • Полномочное (мандатное) управление доступом: ○ возможность заведения в системе не менее 10 уровней конфиденциальности; ○ возможность выбора уровня конфиденциальности сессии для пользователя; ○ возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам; ○ возможность изменения количества мандатных меток в системе и их названий; ○ контроль потоков конфиденциальной информации в системе; ○ возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP. • Контроль вывода конфиденциальных данных на печать: ○ возможность ограничить перечень мандатных меток информации для печати на заданном принтере; ○ теневое копирование информации, выводимой на печать; ○ автоматическая маркировка документов, выводимых на печать; ○ управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать: ▪ отдельный вид грифа для каждой мандатной метки; ▪ отдельный вид маркировки для первой страницы документа; ▪ отдельный вид маркировки для последней страницы документа; ▪ вид маркировки для оборота последнего листа; ○ поддержка функции печати в файл; ○ поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях. • Контроль аппаратной конфигурации компьютера и подключаемых устройств: ○ Должны контролироваться следующие устройства: ▪ последовательные и параллельные порты; ▪ локальные устройства; ▪ сменные, физические и оптические диски; ▪ программно реализованные диски; ▪ USB-устройства; ▪ PCMCIA-устройства; ▪ IEEE1394 (FireWire)- устройства;

Наименование	Технические требования
	▪ устройства, подключаемые по шине Secure Digital. ○ Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства. ○ Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации. ○ Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться. ○ Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации. ○ В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя. ○ При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств. • Контроль сетевых интерфейсов: ○ Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394). ○ Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя. • Создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы (EXE-модули), файлы загружаемых библиотек (DLL-модули), запуск скриптов по технологии Active Scripts. ○ Список модулей, разрешенных для запуска, должен строиться: ▪ с помощью явного указания модулей; ▪ по информации об установленных на компьютере программах; ▪ по зависимостям исполняемых модулей; ▪ по ярлыкам в главном меню; ▪ по событиям журнала безопасности. • Контроль целостности файлов, каталогов, элементов системного реестра: ○ Должна быть возможность проведения контроля целостности, в процессе загрузки ОС, в фоновом режиме при работе пользователя. ○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов. ○ Должна быть возможность восстановления исходного состояния контролируемого объекта. ○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП. ○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. • Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей. • Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации. • Автоматическое затирание оперативной памяти компьютера с возможностью настройки количества проходов затирания информации. • Затирание информации на локальных и сменных дисках по команде пользователя. • Возможность настройки количества проходов затирания информации отдельно для локальных дисков, съемных носителей, оперативной памяти. • Затирание данных и имен файлов, каталогов при удалении информации. • Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию. • Функциональный контроль ключевых компонентов системы. • Регистрация событий безопасности в журнале. ○ Должна быть возможность формирования отчетов по результатам аудита. ○ Должна быть возможность поиска и фильтрации при работе с данными

Наименование	Технические требования
	аудита. ***Требования к централизованному управлению в доменной сети:*** СЗИ должно предоставлять следующие возможности по управлению системой: • Отображение структуры доменов, организационных подразделений, серверов безопасности и защищаемых компьютеров. • Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты. • Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности. • Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров. • Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер). • Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера. • Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров. • Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования. • Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз. • Централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу, при этом система должна позволять: ○ распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов); ○ посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов); ○ создавать иерархию серверов безопасности с не менее чем 3 уровнями вложенности. • Создавать домены безопасности в территориально распределенной сети, при этом должна предоставляться возможность делегирования административных полномочий лицам, ответственным за подразделения (домены безопасности).
Право на использование модуля обнаружения и предотвращения вторжений Средства защиты информации Secret Net Studio 8 на 1 год Производитель ООО «Код безопасности» Страна происхождения – Россия (или эквивалент)	Должно осуществлять: • контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; • обнаружение и предотвращение вторжений; • регистрацию событий безопасности и аудит. Требования к сертификации и применению в информационных системах: СЗИ должно соответствовать требованиям документов: «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011)» не ниже 4 класса защиты, «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ (ФСТЭК России, 2011). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля. СЗИ должно допускать использование в следующих информационных системах: • автоматизированные системы - до класса 1Г (включительно); • государственные информационные системы – до 1 класса защищенности (включительно); • информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно); • автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно). Требования к функциональности СЗИ: СЗИ должно выполнять следующие функции по защите информации: • Контроль входа пользователей в систему и работа пользователей в системе: ○ проверка пароля пользователя при входе в систему; ○ поддержка персональных идентификаторов (USB-токенов и смарт-карт) для входа в систему и разблокировки компьютера – iButton, eToken Pro (Java), Рутокен S,

Наименование	Технические требования
	Рутокен ЭЦП, Рутокен Lite, Jacarta PKI, Jacarta Gost, Jacarta PKI Flash, Jacarta Gost Flash, Esmart USB Token, Esmart, Esmart ГОСТ; ○ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора; ○ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI); ○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI); ○ возможность блокирования входа в систему локальных пользователей; ○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей; ○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности; ○ возможность управления политикой сложности паролей; ○ поддержка возможности входа в систему по сертификатам; ○ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей. • Контроль целостности файлов, каталогов, элементов системного реестра: ○ Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя. ○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов. ○ Должна быть возможность восстановления исходного состояния контролируемого объекта. ○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП. ○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. • Обнаружение и предотвращение вторжений: ○ Должна обеспечиваться защита от вторжений с помощью сигнатурных и эвристических механизмов. ○ Сигнатурные механизмы должны обеспечивать проверку HTTP-трафика на наличие заданных конструкций как для входящего, так и для исходящего сетевого трафика. При обнаружении признаков атаки прохождение подозрительных сетевых пакетов должно быть заблокировано. ○ Эвристические механизмы должны распознавать и фиксировать следующие типы атак: ▪ сканирование портов; ▪ подделка ARP (ARP-spoofing); ▪ SYN-флуд; ▪ атаки, направленные на отказ в обслуживании (DoS); ▪ распределенные атаки, направленные на отказ в обслуживании (DDoS). При обнаружении признаков атаки эвристическими методами должен осуществляться временный запрет на прием сетевых пакетов с IP-адреса атакующего компьютера. ○ Должны обеспечиваться обнаружение и блокировка аномальных сетевых пакетов. • Функциональный контроль ключевых компонентов системы. • Регистрация событий безопасности в журнале. ○ Должна быть возможность формирования отчетов по результатам аудита. ○ Должна быть возможность поиска и фильтрации при работе с данными аудита.
Право на использование модуля персонального межсетевого экрана Средства защиты информации Secret Net Studio 8 Производитель ООО «Код безопасности» Страна происхождения – Россия (или эквивалент)	***Должно осуществлять:*** • контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; • аутентификацию входящих и исходящих сетевых запросов в локальной сети методами, устойчивыми к пассивному и/или активному прослушиванию сети; • фильтрацию сетевых пакетов; • защиту установленных сетевых соединений; • регистрацию событий безопасности и аудит. ***Требования к сертификации и применению в информационных системах:***

Наименование	Технические требования
	СЗИ должно соответствовать требованиям руководящего документов: «Требования к межсетевым экранам» (ФСТЭК России, 2016) не ниже 4 класса защиты, «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля. СЗИ должно допускать использование в следующих информационных системах: • автоматизированные системы - до класса 1Г (включительно); • государственные информационные системы – до 1 класса защищенности (включительно); • информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно); • автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно). СЗИ должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин. ***Требования к операционной платформе и аппаратной части:*** • СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы): ○ Windows 10; ○ Windows 8.1; ○ Windows 7 SP1; ○ Windows Server 2019; ○ Windows Server 2016 ○ Windows Server 2012/2012 R2; ○ Windows Server 2008 R2 SP1. • Должна быть возможность установки СЗИ по произвольному пути. • СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix. • СЗИ должно поддерживать работу на виртуальных машинах, функционирующих в системах виртуализации, построенных на базе гипервизоров VMware ESX(i) и Microsoft Hyper-V. • СЗИ должно поддерживать работу с технологией Personal vDisk Citrix XenDesktop. • СЗИ с централизованным управлением должно функционировать совместно с Microsoft Active Directory; • СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ. • СЗИ не должно требовать при развертывании модификации топологии локальной вычислительной сети. • СЗИ должно иметь в составе дистрибутива драйвера для поддержки аппаратных идентификаторов. • В инфраструктуре должно быть в наличии устройство, считывающее DVD (для чтения установочного диска – хотя бы на одном компьютере в информационной системе). ***Требования к функциональности СЗИ:*** СЗИ должно выполнять следующие функции по защите информации: • Контроль входа пользователей в систему и работа пользователей в системе: ○ проверка пароля пользователя при входе в систему; ○ поддержка аппаратных средств аутентификации: - идентификаторы iButton (типы DS1992 — DS1996); - USB-ключи eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta PKI/ГОСТ, JaCarta ГОСТ Flash, JaCarta-2 ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta SF/ГОСТ, JaCarta PRO, JaCarta-2 PRO/ГОСТ, JaCarta WebPass, JaCarta-2 SE, JaCarta U2F, JaCarta LT, Rutoken S, Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken ЭЦП Touch, Rutoken ЭЦП PKI, Rutoken ЭЦП Flash 2.0, Rutoken ЭЦП Bluetooth, Rutoken Lite, ESMART Token, ESMART Token ГОСТ, ESMART Token D. - смарт-карты eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta PRO, JaCarta-2 PRO/ГОСТ, Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken Lite, ESMART Token, ESMART Token ГОСТ, ESMART Token D, с любыми

Наименование	Технические требования
	совместимыми USB-считывателями; ○ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора; ○ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI); ○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI); ○ возможность блокирования входа в систему локальных пользователей; ○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей; ○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности; ○ возможность управления политикой сложности паролей; ○ поддержка возможности входа в систему по сертификатам; ○ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей; ○ возможность оповещения пользователя о последнем успешном входе в систему; ○ возможность выдачи пользователю предупреждения в виде сообщения о том, что в информационной системе реализованы меры защиты информации. • Контроль целостности файлов, каталогов, элементов системного реестра: ○ Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя. ○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов. ○ Должна быть возможность восстановления исходного состояния контролируемого объекта. ○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП. ○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. • Защита сетевого взаимодействия и фильтрация трафика: ○ Должны быть механизмы аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети. ○ Должны удостоверяться субъекты доступа (пользователи и компьютеры) и защищаемые объекты (компьютеры). ○ Механизмы должны быть защищены от прослушивания, попыток подбора и перехвата паролей, подмены защищаемых объектов, подмены MAC- и IP-адресов. ○ Должны быть предусмотрены механизмы защиты установленных сетевых соединений между субъектами доступа (пользователями и компьютерами) и защищаемыми объектами (серверами и информационными системами) на основе открытых стандартов протоколов семейства IPsec, которые позволяют контролировать аутентичность и целостность передаваемых данных. ○ Должна быть предусмотрена настройка режима защиты сетевого взаимодействия, при этом должны быть предусмотрены следующие режимы защиты: ▪ соединение без защиты; ▪ маркируется каждый пакет; ▪ подписывается заголовок каждого пакета; ▪ подписывается каждый пакет целиком. ○ Должна быть возможность ограничивать сетевые соединения по правилам фильтрации: ▪ на уровне отдельных протоколов из стека TCP/IP; ▪ на уровне параметров протоколов стека TCP/IP; ▪ на уровне параметров служебных протоколов стека TCP/IP; ▪ на уровне периодов времени; ▪ на уровне пользователей или групп пользователей; ▪ на уровне параметров прикладных протоколов; ▪ на уровне исполняемого файла/процесса; ▪ на уровне сетевого адаптера. ○ Должна быть возможность осуществлять фильтрацию команд, параметров и последовательностей команд, а также обеспечивать блокировку мобильного кода. ○ Должна быть возможность маркировки сетевого трафика метками

Наименование	Технические требования
	конфиденциальности. ○ Должен быть предусмотрен выбор действий для определения реакции системы на срабатывание правил фильтрации: ▪ регистрация информации в журнале; ▪ звуковая сигнализация; ▪ запуск программы или сценария. ● Функциональный контроль ключевых компонентов системы. ● Регистрация событий безопасности в журнале. ○ Должна быть возможность формирования отчетов по результатам аудита. ○ Должна быть возможность поиска и фильтрации при работе с данными аудита. ●
Сертификат активации сервиса технической поддержки СЗИ Secret Net Studio 8 Производитель ООО «Код безопасности» Страна происхождения – Россия (или эквивалент)	Сертификат активации сервиса совместной технической поддержки должен поставляться на бумажном носителе, выпущенном производителем - ООО «Код безопасности», сроком действия не менее 1 года. Техническая поддержка работоспособности средств защиты информации должна осуществляться в течение срока действия сертификата. Сертификат активации сервиса совместной технической поддержки должен предоставлять возможность обращаться в техническую поддержку Исполнителя по вопросам: – консультации работников Заказчика по электронной почте.
Kaspersky Стандартный Certified Media Pack Производитель АО «Лаборатория Касперского» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	Компакт-диск с дистрибутивом программного обеспечения и формуляром.
Передача неисключительных прав на использование ПО ViPNet Client 4.x (КС2) Производитель ОАО «Инфотекс» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	Программное обеспечение, реализующее функции криптографического клиента, должно интегрироваться и расширять уже существующую систему защиты каналов связи (ViPNet сеть № 2057), построенную на базе продуктов ViPNet, а также отвечать следующим требованиям: – совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью (ViPNet Administrator), обновления программного обеспечения, обновления справочно-ключевой информации, управление политиками безопасности; – совместимо (полностью) с программно-аппаратным комплексом, реализующим функции шифрование/дешифрование направляемого/принимаемого IP-трафика (ViPNet Coordinator HW1000); – поддержка операционных систем: Microsoft Windows – наличие сертификата ФСБ России по классу КС1/КС2; – предоставлять функции контроля запускаемых в операционной системе приложений; – предоставлять функции контентной фильтрации прикладных протоколов http, ftp; – программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; – взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»).
Сертификат активации сервиса совместной технической поддержки ПО ViPNet Client на 1 год* Производитель ОАО «Инфотекс» Страна происхождения –	Сертификат активации сервиса совместной технической поддержки (Уровень – Расширенная) должен поставляться на бумажном носителе, выпущенном производителем - ОАО «ИнфоТеКС» (ViPNet сеть - 2057), сроком действия не менее 1 года. Техническая поддержка работоспособности средств защиты информации должна осуществляться в течение срока действия сертификата. Сертификат активации сервиса совместной расширенной технической поддержки

Наименование	Технические требования
Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	должен предоставлять возможность обращаться в техническую поддержку Исполнителя по вопросам: - консультации работников Заказчика по электронной почте; - консультации работников Заказчика по телефону.
Передача права на использование ПО ViPNet Client 4.x (КС2)** Производитель ОАО «Инфотекс» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	Программное обеспечение, реализующее функции криптографического клиента, должно интегрироваться и расширять уже существующую систему защиты каналов связи (ViPNet сеть № 1274), построенную на базе продуктов ViPNet, а также отвечать следующим требованиям: – совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью (ViPNet Administrator), обновления программного обеспечения, обновления справочно-ключевой информации, управление политиками безопасности; – совместимо (полностью) с программно-аппаратным комплексом, реализующим функции шифрование/дешифрование направляемого/принимаемого IP-трафика (ViPNet Coordinator HW1000); – поддержка операционных систем: Microsoft Windows – наличие сертификата ФСБ России по классу КС1/КС2; – предоставлять функции контроля запускаемых в операционной системе приложений; – предоставлять функции контентной фильтрации прикладных протоколов http, ftp; – программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; – взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»).
Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client на 1 год** Производитель ОАО «Инфотекс» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	Сертификат активации сервиса прямой технической поддержки (Уровень – Расширенная) должен поставляться на бумажном носителе, выпущенном производителем - ОАО «ИнфоТеКС» (ViPNet сеть - 1274), сроком действия не менее 1 года. Техническая поддержка работоспособности средств защиты информации должна осуществляться в течение срока действия сертификата. Сертификат активации сервиса прямой расширенной технической поддержки должен предоставлять возможность обращаться в техническую поддержку Производителя по вопросам: - консультации работников Заказчика по электронной почте; - консультации работников Заказчика по телефону.
Компакт-диск с дистрибутивом ПО ViPNet** Производитель ОАО «Инфотекс» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	Компакт-диск с дистрибутивом программного обеспечения и формуляром.
Передача неисключительных прав на использование ПО ViPNet Client 4.x (КС1)*** Производитель ОАО «Инфотекс» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью	Программное обеспечение, реализующее функции криптографического клиента, должно интегрироваться и расширять уже существующую систему защиты каналов связи (ViPNet сеть № 3395), построенную на базе продуктов ViPNet, а также отвечать следующим требованиям: – совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью (ViPNet Administrator), обновления программного обеспечения, обновления справочно-ключевой информации, управление политиками безопасности; – совместимо (полностью) с программно-аппаратным комплексом,

Наименование	Технические требования
совместимости с уже имеющимся программным обеспечением)	реализующим функции шифрование/дешифрование направляемого/принимаемого IP-трафика (ViPNet Coordinator HW1000); – поддержка операционных систем: Microsoft Windows – наличие сертификата ФСБ России по классу КС1/КС2; – предоставлять функции контроля запускаемых в операционной системе приложений; – предоставлять функции контентной фильтрации прикладных протоколов http, ftp; – программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; – взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»).
Компакт-диск с дистрибутивом ПО ViPNet*** Производитель ОАО «Инфотекс» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	Компакт-диск с дистрибутивом программного обеспечения и формуляром.
Сертификат активации сервиса прямой технической поддержки ПО ViPNet Client 4.x (КС1) на 1 год*** Производитель ОАО «Инфотекс» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	Сертификат активации сервиса прямой технической поддержки (Уровень – Расширенная) должен поставляться на бумажном носителе, выпущенном производителем - ОАО «ИнфоТеКС» (ViPNet сеть - 3395), сроком действия не менее 1 года. Техническая поддержка работоспособности средств защиты информации должна осуществляться в течение срока действия сертификата. Сертификат активации сервиса прямой расширенной технической поддержки должен предоставлять возможность обращаться в техническую поддержку Производителя по вопросам: – консультации работников Заказчика по электронной почте; – консультации работников Заказчика по телефону.