**Техническое задание**

**на оказание услуг в области защиты информации**

Исполнитель обязуется по заданию Заказчика оказать услуги в области защиты информации (далее – Услуги), а Заказчик обязуется принять и оплатить оказанные Услуги в порядке и на условиях, предусмотренных Договором.

**Цель оказания Услуг:** Реализация защищенного подключения информационной системы электросетевой организации к СМЭВ в соответствии с действующими требованиями нормативных правовых актов и методических документов.

Для информационной системы заранее установлен требуемый **первый класс защищенности**.

**Место доставки товара, выполнения работы или оказания услуги:**

г. Иркутск, \_\_\_\_\_\_\_\_

**Услуги должны соответствовать требованиям следующих нормативных актов:**

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
4. Постановление Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;
5. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
6. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
7. 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»;
8. Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
9. Приказ ФСБ РФ от 9 февраля 2005 г. № 66  
   «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
10. Приказ ФСБ России от 10 июля 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»;
11. Методический документ ФСТЭК России «Методика оценки угроз безопасности информации», утвержденный 05.02.2021;
12. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержденный 11.02.2014;
13. Методический документ 8 Центра ФСБ России № 149/7/2/6-432 «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденный 31.03.2015;
14. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
15. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем.

В соответствии с положениями ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» Исполнитель на всех этапах обязан:

- учитывать возможность реализации действующих требований о защите обрабатываемой информации;

- обеспечивать защиту информации во всех составных частях автоматизированного рабочего места, используемых в обработке защищаемой информации;

- обеспечить внедрение средств защиты информации и контроля эффективности защиты информации без препятствий нормальному функционированию автоматизированной системы;

- обеспечить совместимость программного обеспечения системы защиты информации с иным программным обеспечением автоматизированной системы;

- обеспечить требуемый уровень защищенности информации;

- обеспечить совместимость программно-технических средств автоматизированной системы, используемых для построения системы защиты информации (корректную совместную работу) без снижения уровня защищенности информации.

Документы, передаваемые Исполнителем Заказчику должны быть переданы с соблюдением всех мер конфиденциальности, предусмотренных для документов с ограничительной пометкой «Для служебного пользования».

**Сроки поставки товара или завершения работы либо график оказания услуг:**

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование мероприятия | Сроки проведения |
| 1. | Определение требуемых уровня защищенности персональных данных и класса защищенности информационной системы | 1 неделя |
| 2. | Разработка модели угроз безопасности информации и технического задания на разработку системы защиты информации информационной системы | 7 недель |
| 3. | Поставка средств защиты информации и совместимых программно-аппаратных средств, необходимых для организации защищенного подключения информационной системы к СМЭВ | 4 недели |
| 4. | Внедрение системы защиты информации информационной системы | 4 недели |
| 5. | Разработка организационно-распорядительных документов по защите информации информационной системы | 1 неделя |
| 6. | Проведение предварительных испытаний, опытной эксплуатации, анализа уязвимостей и приемочных испытаний системы защиты информации информационной системы | 3 недели |
| 7. | Проверка возможности эксплуатации средств криптографической защиты информации | 1 неделя |
| 8. | Разработка программы и методик аттестационных испытаний информационной системы на соответствие требованиям по безопасности информации | 1 неделя |
| 9. | Аттестация информационной системы по требованиям безопасности информации | 2 недели |

**Объем оказываемых Услуг и требования к ним:**

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование мероприятия | Планируемый результат |
| 1. | Определение требуемых уровня защищенности персональных данных и класса защищенности информационной системы | Готовые документы, передаваемые в электронном виде:  - приказ о назначении комиссии по классификации и сопровождению аттестации объекта информатизации;  - приказ о создании информационной системы и назначении ответственных лиц;  - акт классификации информационной (автоматизированной) системы (выполненный в соответствии с приказом ФСТЭК России от 29 апреля 2021 г. N 77, постановлением Правительства РФ от 1 ноября 2012 г. № 1119, приказом ФСТЭК России от 11 февраля 2013 г. № 17). |
| 2. | Разработка модели угроз безопасности информации и технического задания на разработку системы защиты информации информационной системы | Готовые документы, передаваемые в электронном виде:  - модель угроз безопасности информации информационной системы (выполненная в соответствии с методическими документами ФСТЭК России «Методика оценки угроз безопасности информации», утвержденный 05.02.2021 и 8 Центра ФСБ России № 149/7/2/6-432 «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденный 31.03.2015);  - техническое задание на создание системы защиты информации информационной системы (выполненное в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 и ГОСТ 34.603-92);  Результатом оказания услуги является положительный ответ от ФСТЭК России в части согласования указанных документов либо ответ от ФСТЭК России об отсутствии необходимости такого согласования (на основании Требований, утвержденных постановлением Правительства РФ от 6 июля 2015 г. № 676).  Согласование с ФСБ России не требуется в соответствии с методическим документом 8 Центра ФСБ России № 149/7/2/6-432. |
| 3. | Поставка средств защиты информации и совместимых программно-аппаратных средств, необходимых для организации защищенного подключения информационной системы к СМЭВ | Передача заказчику:  - сертифицированного дистрибутива средства антивирусной защиты;  - лицензии на право использования и сертифицированного дистрибутива средства защиты информации от несанкционированного доступа;  - лицензии на право использования и сертифицированного дистрибутива средства программного модуля доверенной загрузки;  - лицензии на право использования и сертифицированного дистрибутива сканера сетевой безопасности;  - программно-аппаратного комплекса межсетевого экранирования, обнаружения вторжений и шифрования информации;  - серверов (2 шт.).  Требуемые характеристики на вышеперечисленные средства указаны в соответствующем разделе. |
| 4. | Внедрение системы защиты информации информационной системы | Готовые документы, передаваемые в электронном виде:  - акт установки и настройки средств защиты информации (должен содержать сведения о результатах установки и настройки всех сертифицированных средств защиты информации с указанием результатов снятия контрольных сумм (при наличии контрольных сумм в документации на средства защиты информации)). |
| 5. | Разработка организационно-распорядительных документов по защите информации информационной системы | Разработка организационно-распорядительных документов, необходимых для успешного прохождения аттестации по требованиям безопасности информации (в случае, если указанные документы отсутствуют либо не соответствуют предъявляемым требованиям).  Готовые документы, передаваемые в электронном виде:  - технический паспорт информационной системы (выполненный в соответствии с приказом ФСТЭК России от 29 апреля 2021 г. N 77);  - инструкция по безопасной эксплуатации информационной системы (выполненная в соответствии с приказом ФСТЭК России от 29 апреля 2021 г. N 77);  - матрица доступа к ресурсам информационной системы;  - сведения об уровне подготовки кадров, обеспечивающих защиту информации;  - план мероприятий по защите информации на объекте информатизации;  - перечни лиц, имеющих право доступа в помещения;  - перечень пользователей информационной системы;  - перечень пользователей средств криптографической защиты информации;  - журнал учета машинных носителей конфиденциальной информации;  - журнал учета паролей;  - проект приказа о вводе информационной системы в постоянную эксплуатацию;  - иные документы, предусмотренные действующими требованиями. |
| 6. | Проведение предварительных испытаний, опытной эксплуатации, анализа уязвимостей и приемочных испытаний системы защиты информации информационной системы | Готовые документы, передаваемые в виде твердой копии:  - акт приемки системы защиты информации в опытную эксплуатацию (в соответствии с ГОСТ 34.603-92);  - журнал опытной эксплуатации (при необходимости, в соответствии с ГОСТ 34.603-92);  - акт о завершении опытной эксплуатации системы защиты информации (в соответствии с ГОСТ 34.603-92);  - заключение по результатам анализа уязвимостей системы защиты информации (выполненное в соответствии с приказом ФСТЭК России от 29 апреля 2021 г. N 77);  - акт приемки системы защиты информации в постоянную эксплуатацию (в соответствии с ГОСТ 34.603-92). |
| 7. | Проверка возможности эксплуатации средств криптографической защиты информации | Готовые документы, передаваемые в виде твердой копии (выполненные в соответствии с приказом ФАПСИ от 13 июня 2001 г. N 152):  - заключение по уровню подготовки пользователей средств криптографической защиты информации;  - заключение о возможности эксплуатации средств криптографической защиты информации;  - журнал учета средств криптографической защиты информации;  - журнал учета хранилищ. |
| 8. | Разработка программы и методик аттестационных испытаний информационной системы на соответствие требованиям по безопасности информации | Готовые документы, передаваемые в виде твердой копии (выполненные в соответствии с приказом ФСТЭК России от 29 апреля 2021 г. N 77):  - программа и методики аттестационных испытаний информационной системы. |
| 9. | Аттестация информационной системы по требованиям безопасности информации | Готовые документы, передаваемые в виде твердой копии (выполненные в соответствии с приказом ФСТЭК России от 29 апреля 2021 г. N 77):  - протокол оценки соответствия принятых технических мер по защите информации от несанкционированного доступа;  - заключение по результатам аттестационных испытаний;  - аттестат соответствия требованиям по безопасности информации (приказ ФСТЭК России от 11 февраля 2013 г. № 17, приказ ФСТЭК России от 18 февраля 2013 г. № 21). |

**Требования, предъявляемые к поставляемым программно-аппаратным средствам и средствам защиты информации:**

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование мероприятия | Планируемый результат |
| 1. | Сертифицированный дистрибутив средства антивирусной защиты | Дистрибутив Kaspersky Стандартный Certified Media Pack Russian Edition в комплектации:  - диск в конверте с записанными сертифицированными программами последней версии, прошедшей сертификационные испытания;  - формуляр с идентификатором ФСТЭК России;  - копию действительного сертификата соответствия ФСТЭК России по профилям средств антивирусной защиты типа А, Б, В, Г второго класса (А2, Б2, В2, Г2).  В составе дистрибутива должны быть следующие программы:  - Kaspersky Endpoint Security для Windows;  - Kaspersky Security Center;  - Kaspersky Security для Windows Server;  - Kaspersky Endpoint Security для Linux.  Поставка эквивалента недопустима по причине несовместимости товара с уже используемыми товарами (лицензией на средство антивирусной защиты). |
| 2. | Лицензия на право использования и сертифицированный дистрибутив средства защиты информации от несанкционированного доступа | Средство защиты должно иметь возможность установки на персональные компьютеры, портативные и мобильные ПК (ноутбуки и планшетные ПК), серверы (файловые, контроллеры домена, терминального доступа) и виртуальные машины (например, VMware), работающие как в автономном режиме, так и в составе локально-вычислительной сети.  Поддерживаемые ОС:  - Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);  - Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);  - Windows 8 (Core, Pro, Enterprise);  - Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);  - Windows 8.1 (Core, Pro, Enterprise);  - Windows Server 2012 (R2) (Foundation, Essentials, Standard, Datacenter);  - Windows 10 (Enterprise, Education, Pro, Home) и Windows 10 Creators Update;  - Windows 11 (Enterprise, Education, Pro, Home);  - Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);  - Windows Server 2019 (Essentials, Standard, Datacenter);  - Windows Server 2022 (Standart, Datacenter).  Поддерживаемые аппаратные идентификаторы:  - USB-флэш-накопители;  - электронные ключи Touch Memory (iButton);  - HID Proximity-карты;  - USB-ключи и смарт-карты Aladdin eToken;  - USB-ключи и смарт-карты Рутокен;  - USB-ключи и смарт-карты JaCarta;  - USB-ключи и смарт-карты ESMART;  - NFC-метки и смарт-карты семейства MIFARE.  Комплект поставки должен включать:  - лицензию на право использования компонентов средства защиты информации от несанкционированного доступа (СЗИ НСД) и контроля съемных машинных носителей информации (СКН);  - диск с записанными сертифицированными программами последней версии, прошедшей сертификационные испытания;  - формуляр с идентификатором ФСТЭК России;  - копию действительного сертификата соответствия ФСТЭК России 5 классу защищенности СВТ от НСД, 4 классу защиты МЭ (ИТ.МЭ.В4.ПЗ), 4 классу защиты СОВ (ИТ.СОВ.У4.ПЗ), 4 классу защиты СКН (ИТ.СКН.П4.ПЗ, ИТ.СКН.Н4.ПЗ), 4 уровню доверия (УД 4). |
| 3. | Лицензия на право использования и сертифицированный дистрибутив средства программного модуля доверенной загрузки | Программный модуль доверенной загрузки (ПМДЗ) должен иметь возможность установки в UEFI BIOS различных производителей, в том числе UEFI BIOS поставляемых серверов.  Требуемые функции: идентификация и аутентификация пользователей; доверенная загрузка операционной системы; контроль целостности; управление учетными записями пользователей; управление настройками аутентификации; удаленное управление; управление сертификатами; проверка и установка обновлений.  Комплект поставки должен включать:  - лицензию на право использования ПМДЗ;  - диск с записанными сертифицированными программами последней версии, прошедшей сертификационные испытания;  - формуляр с идентификатором ФСТЭК России;  - копию действительного сертификата соответствия ФСТЭК России (Требования доверия (2), Требования к СДЗ, Профиль защиты СДЗ (базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ)). |
| 4. | Лицензия на право использования и сертифицированный дистрибутив сканера сетевой безопасности | Сканер сетевой безопасности должен иметь возможности: идентификации узлов и сетевых служб; выявления уязвимостей и ошибок конфигурирования в сервисах SMB, RDP, HTTP, SNMP, FTP, SSH; планирования и автоматизации сканирования; формирования отчетов; разграничения доступа к функциям программы.  Комплект поставки должен включать:  - лицензию на право использования сканера сетевой безопасности;  - диск с записанными сертифицированными программами последней версии, прошедшей сертификационные испытания;  - формуляр с идентификатором ФСТЭК России;  - копию действительного сертификата соответствия ФСТЭК России (Требования доверия (4), ТУ). |
| 5. | Программно-аппаратный комплекс межсетевого экранирования, обнаружения вторжений и шифрования информации | Комплект поставки должен включать:  - аппаратную платформу Российского производства в корпусе промышленного PC (1U), интерфейсы 4x1000BASE-T RJ45, 1x1G SFP; возможности L3VPN, МЭ, СОВ, расширенный контроль приложений, GeoProtection, сервер доступа на 2 подключения, работа в кластере; производительность МЭ + СОВ на смешанном трафике до 300 Мбит/сек;  - комплект для монтажа в серверную стойку;  - лицензия на право управления; лицензия на обновление базы решающих правил (сигнатур) СОВ, базы приложений и базы GeoProtection срок действия 1 год; сертификат на право использования прямой (от производителя) технической поддержки уровня «Базовый» на 1 год;  - формуляр (паспорт) с идентификатором ФСТЭК России;  - копия действительного сертификата соответствия ФСТЭК России (МЭ А4, СОВ4, УД4). |
| 6. | Сервер | Корпус:  Высота: не более 1U;  Количество корзин 3,5” с горячей заменой: не менее 4;  Охлаждение: не менее 4 вентиляторов диаметром не менее 40 мм;  Количество слотов расширения: не менее 3;  Глубина: не более 650 мм;  Индикатор питания: наличие;  Индикатор ошибок: наличие;  Индикатор активности сети: наличие;  Комплект телескопических направляющих для установки в стойку: наличие.  Блок питания:  Количество блоков питания: не менее 2;  Возможность горячей замены: наличие;  Мощность блоков питания: не менее 750 Вт;  Стандарт 80Plus: не менее Platinum.  Процессоры:  Количество установленных процессоров: не менее 2;  Базовая частота: не менее 3,2 ГГц;  Максимальная частота: не менее 4 ГГц;  Количество ядер: не менее 8;  Количество потоков: не менее 16;  Объем кэш-памяти L3: не менее 11 Мб;  Техпроцесс: не более 14 нм;  Поддержка ECC: наличие;  Тепловыделение: не более 130 Вт;  Количество каналов памяти: не менее 6.  Оперативная память:  Общий объем: не менее 128 Гб;  Тип памяти: DDR4;  Формат: DIMM;  Частота: не менее 3200 МГц;  Поддержка ECC: наличие;  Буферизованная (Registered): наличие.  Жесткие диски:  Количество установленных накопителей: не менее 2;  Объем каждого накопителя: не менее 2 Тб;  Скорость вращения: не менее 7200 об/мин;  Форм-фактор: 3,5";  Интерфейс: не менее SATA-III;  Объем кэш-памяти: не менее 128 Мб;  Время наработки на отказ: не менее 2 000 000 часов;  Ударостойкость при работе: не менее 65 G;  Ударостойкость при хранении: не менее 300 G;  Энергопотребление: не более 8.1 Вт.  Твердотельные накопители:  Количество установленных накопителей: не менее 2;  Форм-фактор: 2,5";  Интерфейс: не менее SATA-III;  Объем: не менее 960 Гб;  Тип памяти: 3D TLC;  Скорость чтения: не менее 560 Мб/с;  Скорость записи: не менее 510 Мб/с;  Ресурс DWPD: не менее 3;  Ресурс TBW: не менее 6144 Тб;  Время наработки на отказ: не менее 2 млн часов;  Шифрование данных: наличие.  Материнская плата:  Количество сокетов: не менее 2;  Количество слотов DDR4: не менее 12;  Максимальный объем памяти: не менее 3 Тб;  Возможность построения Raid 0, 1, 5, 10 из SATA устройств: наличие;  Количество слотов PCI-E 3.0: не менее 1;  Количество слотов M.2 2280 M-Key: не менее 1;  Порты USB 3.0 на задней панели: не менее 4;  Внутренний порт USB Type-A: наличие;  Порт VGA: наличие;  Порты 1GbLAN: не менее 2;  Порт RJ-45 Management: наличие;  Слот для подключения Raid-контроллера, не занимающего задние слоты расширения: наличие. |
| 7. | Сервер | Максимальное количество процессоров: ≥ 2;  Количество установленных процессоров: ≥ 2;  Количество ядер каждого установленного процессора: ≥ 16;  Количество потоков каждого установленного процессора: ≥ 32;  Базовая частота каждого установленного процессора (без учета технологии динамического изменения частоты): ≥ 2.4 Гигагерц;  Объем кэш памяти третьего уровня (L3) каждого установленного процессора: ≥ 24 Мегабайт;  Количество слотов для модулей оперативной памяти: ≥ 32;  Объем каждого установленного модуля оперативной памяти: ≥ 32 Гигабайт;  Суммарный объем установленной оперативной памяти: ≥ 256 Гигабайт;  Скорость передачи данных каждого установленного модуля оперативной памяти, МТ/с: ≥ 3200;  Поддержка функции обнаружения и коррекции ошибок в оперативной памяти: Да;  Максимальный общий поддерживаемый объем оперативной памяти: ≥ 4096 Гигабайт;  Интерфейс поддерживаемых накопителей: M.2, NVMe, PCIe, SAS, SATA;  Количество LFF (3,5) слотов для накопителей на лицевой панели: ≥ 12;  Количество SFF (2,5) слотов для накопителей на задней панели: ≥ 2;  Максимальное количество накопителей в корпусе: ≥ 16;  Тип установленных накопителей (тип 1): HDD;  Интерфейс установленных накопителей (тип 1): SAS;  Количество установленных накопителей (тип 1) с поддержкой горячей замены: ≥ 8;  Объем каждого установленного накопителя (тип 1): ≥ 2400 Гигабайт;  Скорость вращения дисков в накопителе HDD или SSHD (тип 1): ≥ 10000 Оборот в минуту;  Наличие установленного аппаратного дискового контроллера: Да;  Наличие защиты кэш-памяти дискового контроллера при потере питания сервером: Да;  Объем кэш-памяти установленного дискового контроллера: ≥ 1 Гигабайт;  Поддерживаемые дисковым контроллером типы RAID: 0, 1, 10, 5, 50, 6, 60;  Количество сетевых портов (тип 1): ≥ 2;  Поддерживаемые протоколы сетевого порта (тип 1): Ethernet;  Скорость сетевого порта Ethernet (тип 1): ≥ 10 Гигабит в секунду;  Тип среды передачи для сетевого порта (тип 1): Медь-витая пара;  Количество установленных блоков питания с поддержкой горячей замены, шт.: ≥ 2;  Номинальная мощность одного блока питания: ≥ 1600 Ватт;  Уровень резервирования установленных блоков питания: N+1;  Тип сервера: Стоечный;  Тип корпуса: Rack;  Количество занимаемых юнитов в стойке: ≤ 2;  Система удаленного управления сервером: Да;  Выделенный порт удалённого управления сервером: Да;  Возможность установки плат стандарта PCIe: 4.0;  Количество USB 3.x портов: ≥ 4;  Количество слотов для установки плат расширения PCIe x16: ≥ 1;  Количество слотов для установки плат расширения PCIe x8: ≥ 5;  Наличие интегрированного видеоадаптера: Да;  Наличие направляющих для установки в шкаф телекоммуникационный: Да;  Сервисные или вспомогательные разъемы подключения: VGA;  Тип размещения USB портов: На задней панели, На передней панели;  Уровень резервирования установленных блоков охлаждения: N+1; |

**Участник закупки должен соответствовать требованиям**, установленным Федеральным законом РФ от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» и:

1.Постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» к лицам, осуществляющим деятельность по технической защите конфиденциальной информации, в том числе иметь действующую лицензию (или выписку из реестра лицензий), дающую право участнику закупки оказывать услуги в соответствии с требованиями настоящей документации, в том числе на:

• услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам (п. а) в средствах и системах информатизации (пп. а1);

• услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации (п. б);

• работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации (п. г) средств и систем информатизации (пп. г1);

• услуги по установке, монтажу, испытаниям, ремонту средств защиты информации (п. е) технических средств защиты информации (пп. е1), защищенных технических средств обработки информации (пп. е2), технических средств контроля эффективности мер защиты информации (пп. е3), программных (программно-технических) средств защиты информации (пп. е4), защищенных программных (программно-технических) средств обработки информации (пп. е5), программных (программно-технических) средств контроля эффективности защиты информации (пп. е6).

2.Постановлением Правительства Российской Федерации от 16.04.2012 № 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)» к лицам, осуществляющим деятельность 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, в том числе иметь действующую лицензию (или выписку из реестра лицензий), дающую право участнику закупки оказывать услуги в соответствии с требованиями настоящей документации, в том числе на:

• монтаж, установку (инсталляцию), наладку шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации (п. 12);

• монтаж, установку (инсталляцию), наладку защищенных с использованием шифровальных (криптографических) средств информационных систем (п. 13);

• работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) (п. 20);

• передачу шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации (п. 21);

• передачу защищенных с использованием шифровальных (криптографических) средств информационных систем (п. 22).