**УТВЕРЖДАЮ**

**29 ноября 2016 года**

**Документация о проведении открытого аукциона в электронной форме**

**по определению Исполнителя на заключение договора** **по поставке серверного оборудования, дисковой полки для системы хранения данных, программного обеспечения, средств защиты информации и выполнение работ по установке, настройке оборудования, созданию системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия»**

**Адрес официального сайта:** [**www.zakupki.gov.ru**](http://www.zakupki.gov.ru)

г. Улан-Удэ

|  |  |
| --- | --- |
| **Раздел**  **№** | **НАИМЕНОВАНИЕ РАЗДЕЛА ДОКУМЕНТАЦИИ ОБ АУКЦИОНЕ**  **В ЭЛЕКТРОННОЙ ФОРМЕ** |
| **1.** | **Общие положения**  Настоящая документация об открытом аукционе в электронной форме подготовлена в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», Положением о закупках товаров, работ, услуг Государственного автономного учреждения культуры Республики Бурятия «Государственный архив Республики Бурятия»., а также иным законодательством, регулирующим закупочную деятельность.  Термины и понятия, используемые в документации о совместном аукционе в электронной форме (далее по тексту – Документация об аукционе), трактуются в соответствии с положениями Закона.  Все Приложения к Документации об аукционе являются ее неотъемлемой частью. |
| **2.** | **Требования к содержанию и составу заявки** **на участие в электронном аукционе**  **Инструкция по ее заполнению**  Для участия в электронном аукционе участник закупки, получивший аккредитацию на электронной площадке подает заявку на участие в электронном аукционе.  Обмен информацией, связанной с получением аккредитации на электронных площадках и проведения электронного аукциона, между участником аукциона, заказчиком, оператором электронной площадки осуществляется на электронной площадке в форме электронных документов.  Документы и информация, направляемые в форме электронных документов участником электронного аукциона должны быть подписаны усиленной электронной подписью лица, имеющего право действовать от имени соответственно участника аукциона.  Все документы и сведения, входящие в состав заявок на участие в электронном аукционе должны соответствовать требованиям действующего законодательства Российской Федерации и требованиям Документации об аукционе.  Участие в электронном аукционе возможно при наличии на лицевом счете участника закупки, открытом для проведения операций по обеспечению участия в аукционе, денежных средств, в отношении которых не осуществлено блокирование операций по лицевому счету, в размере не менее чем размер обеспечения заявки на участие в аукционе, предусмотренный Документацией об аукционе.  Заявка на участие в электронном аукционе состоит из одной части и должна содержать.  - согласие на выполнение работ, поставку товара и конкретные показатели, соответствующие значениям, установленным документацией об аукционе, и указание на товарный знак (его словесное обозначение) (при наличии), знак обслуживания (при наличии), фирменное наименование (при наличии), патенты (при наличии), полезные модели (при наличии), промышленные образцы (при наличии), наименование страны происхождения товара(в соответствии с Общероссийским классификатором стран мира);  - наименование, фирменное наименование (при наличии), место нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество (при наличии), паспортные данные, место жительства (для физического лица), номер контактного телефона, идентификационный номер налогоплательщика участника аукциона или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика участника аукциона (для иностранного лица), идентификационный номер налогоплательщика (при наличии) учредителей, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа участника аукциона;  - декларация о соответствии участника аукциона требованиям, установленным пунктами 2-6 раздела 30 Документации об аукционе;  - заполненный проект договора от участника закупки с указанием перечня выполняемых работ.  - решение об одобрении или о совершении крупной сделки либо копия данного решения в случае, если требование о необходимости наличия данного решения для совершения крупной сделки установлено федеральными законами и иными нормативными правовыми актами Российской Федерации и (или) учредительными документами юридического лица и для участника аукциона заключаемый договор или предоставление обеспечения заявки на участие в аукционе, обеспечения исполнения договора является крупной сделкой.  -наличие лицензии ФСБ России на 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 (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).  -наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.  *При подготовке заявки на участие в аукционе участники закупки могут использовать формы установленные Приложением №3 к Документации об аукционе.*  Участник электронного аукциона вправе подать заявку на участие в аукционе в любое время с момента размещения извещения о его проведении до предусмотренных Документацией о аукционе даты и времени окончания срока подачи на участие в аукционе заявок.  Заявка на участие в электронном аукционе направляется участником аукциона оператору электронной площадки в форме электронных документов. Указанные электронные документы подаются одновременно.  Участник электронного аукциона вправе подать только одну заявку на участие в аукционе в отношении каждого объекта закупки.  Участник электронного аукциона, подавший заявку на участие в аукционе, вправе отозвать данную заявку не позднее даты окончания срока подачи заявок на участие в аукционе, направив об этом уведомление оператору электронной площадки.  В случае, если по окончании срока подачи заявок на участие в электронном аукционе подана только одна заявка или не подано ни одной заявки, такой аукцион признается несостоявшимся.  В случае установления недостоверности информации, содержащейся в документах, представленных участником электронного аукциона в составе заявки, аукционная комиссия обязана отстранить такого участника от участия в электронном аукционе на любом этапе его проведения. |
| **3.** | **Наименование заказчика:**  Государственное автономное учреждение культуры Республики Бурятия «Государственный архив Республики Бурятия». 670000, Республика Бурятия, г. Улан-Удэ, ул. Сухэ-Батора, 9а. [arhivy03@mail.ru](mailto:arhivy03@mail.ru) |
| **4.** | **Предмет договора:**  Поставкасерверного оборудования, дисковой полки для системы хранения данных, программного обеспечения, средств защиты информации и выполнение работ по установке, настройке оборудования, созданию системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия» |
| **5.** | **Количество и объем поставляемого товара:**  В соответствии с Техническим заданием Заказчика (Приложение № 1 к Документации об аукционе). |
| **6.** | **Описание объекта закупки**  **Функциональные, технические и качественные характеристики,**  **эксплуатационные характеристики объекта закупки**  Выполняемые работы (включая используемые при его изготовлении материалы) должны соответствовать установленным на территории Российской Федерации нормам и правилам. Качество выполняемых работ должно соответствовать установленным в Российской Федерации стандартам, требованиям государственных стандартов (технических регламентов), подтверждающих качество товара, обеспечивающие безопасность для жизни и здоровья пользователей.  Выполняемые работы должны соответствовать описанию, указанному в Техническом задании (Приложение №1 к Документации об аукционе). |
| **7.** | **Требования к сроку и (или) объему предоставления гарантий качества товара**  В соответствии с техническим заданием (Приложение №1 к Документации об аукционе) |
| **8.** | **Условия договора**  Поставщик обязан оказать услуги, являющиеся предметом закупки, в сроки, объеме и качестве которые определены Документацией об аукционе, техническим заданием (Приложение №1 к Документации об аукционе) и проектом договора(Приложение №2 к Документации об аукционе). |
| **9.** | **Место выполняемых работ**  Местомвыполняемых работ являются: Республика Бурятия, г. Улан-Удэ, ул. Ленина, 54. |
| **10.** | **Срок выполняемых работ**  Со дня подписания договора по 15 апреля 2017 г. |
| **11.** | **Форма, сроки, порядок оплаты**  Оплата по договору осуществляется по безналичному расчету путем перечисления Заказчиком денежных средств на расчетный счет Исполнителя, указанный в настоящем договоре за фактически выполненные работы Исполнителя на основании представленных подписанных сторонами Акта (актов) о приемке выполненных работ (без претензий), счета, счета-фактуры, товарной накладной3 в течение 15банковских дней. |
| **12.** | **Начальная (максимальная) цена договора**  Начальная (максимальная) цена договора: 4 242 340,0 (четыре миллиона двести сорок две тысячи триста сорок) руб., ноль коп. с учетом НДС. |
| **13.** | **Обоснование начальной (максимальной) цены договора**  На основании Соглашения о выделении целевой субсидии и в соответствии с методом расчета и анализа рынка. |
| **14.** | **Источник финансирования заказа**  Республиканский бюджет. |
| **15.** | **Информация о валюте, используемой для формирования цены договора**  **и расчетов с поставщиками**  Цены должны быть указаны в валюте Российской Федерации (в рублях). |
| **16.** | **Порядок применения официального курса иностранной валюты к рублю Российской Федерации, установленного Центральным банком Российской Федерации и используемого при оплате договора**  Оплата в иностранной валюте не предусмотрена. |
| **17.** | **Адрес электронной площадки**  **в информационно-телекоммуникационной сети "Интернет"**  ЭТП ОТС Тендер http://tender.otc.ru |
| **18.** | **Дата и время окончания срока подачи заявок на участие в аукционе**  30 декабря 2016 года в 10.00 часов по местному времени. |
| **19.** | **Дата окончания срока рассмотрения на участие в аукционе**  Не позднее 17.00 по местному времени 10 января 2017 года. |
| **20.** | **Дата проведения аукциона и подведения итогов**  Проведение аукциона: 11 января 2017 года с 10.00 по 13.00 местного времени.  Подведение итогов: Не позднее 17.00 по местному времени 13 января 2016года. |
| **21.** | **Порядок, даты начала и окончания срока предоставления**  **участникам аукциона разъяснений положений документации об аукционе**  Любой участник электронного аукциона, получивший аккредитацию на электронной площадке, вправе направить на адрес электронной площадки запрос о даче разъяснений положений Документации об аукционе. При этом участник аукциона вправе направить не более чем три запроса о даче разъяснений положений документации в отношении данного аукциона.  В течение одного часа с момента поступления указанного запроса оператор электронной площадки направляется его заказчику.  В течение двух дней с даты поступления от оператора электронной площадки запроса заказчик размещает в единой информационной системе разъяснения положений Документации об аукционе с указанием предмета запроса, но без указания участника аукциона, от которого поступил указанный запрос, при условии, что указанный запрос поступил заказчику не позднее чем за три дня до даты окончания срока подачи заявок на участие в аукционе. |
| **22.** | **Размер обеспечения заявки на участие в аукционе**  Размер обеспечения заявки на участие в данном аукционе в электронной форме составляет 1% от начальной (максимальной) цены договора.  В денежном выражении – 42 423,40 (сорок две тысячи четыреста двадцать три руб.40 коп.) |
| **23.** | **Размер обеспечения исполнения договора, порядок предоставления обеспечения, требования к такому обеспечению**  Размер обеспечения исполнения договора составляет 10 % от начальной (максимальной) цены договора.  В денежном выражении – 424 234 (четыреста двадцать четыре тысячи двести тридцать четыре руб, 00 коп.) |
| **24.** | **Возможность заказчика изменить условия договора**  Изменение существенных условий договора при его исполнениидопускается. |
| **25.** | **Информация о возможности одностороннего отказа от исполнения договора**  Возможность одностороннего отказа от исполнения договора предусмотрена |
| **26.** | **Информация о контактном лице ответственного за заключение договора:**  контактное лицо Андреева Туяна Владимировна, 8 (3012) 21-29-58 |
| **27.** | **Заключение договора по результатам электронного аукциона.**  **Срок, в течение которого победитель аукциона или иной участник,**  **с которым заключается договор при уклонении победителя аукциона**  **от заключения договора, должен подписать договор**  По результатам аукциона договор заключается с победителем такого аукциона, а в случаях, предусмотренных Законом, с иным участником при уклонении победителя аукциона от заключения договора. Победитель должен подписать договорв течении 10 (десяти) календарных дней со дня подписания итогового протокола о результатах закупки. |
| **28.** | **Условия признания победителя аукциона или иного участника аукциона уклонившимися от заключения договора**  Победитель электронного аукциона признается уклонившимся от заключения договора в случае, если в установленные сроки он не направил заказчику проект договора, подписанный лицом, имеющим право действовать от имени победителя аукциона. |
| **29.** | **Информация о возможности изменения условий договора**  Возможность изменения условий договора не предусмотрена. |
| **30.** | **Требования к участникам аукциона**  1) соответствие требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся объектом закупки;  2) непроведение ликвидации участника закупки - юридического лица и отсутствие решения арбитражного суда о признании участника закупки - юридического лица или индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства;  3) неприостановление деятельности участника закупки в порядке, установленном Кодексом Российской Федерации об административных правонарушениях, на дату подачи заявки на участие в закупке;  4) отсутствие у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признанииобязанностизаявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов участника закупки, по данным бухгалтерской отчетности за последний отчетный период. Участник закупки считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по такому заявлению на дату рассмотрения заявки на участие в определении поставщика (подрядчика, исполнителя) не принято;  5) отсутствие у участника закупки - физического лица либо у руководителя, членов коллегиального исполнительного органа или главного бухгалтера юридического лица - участника закупки судимости за преступления в сфере экономики (за исключением лиц, у которых такая судимость погашена или снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации;  6) отсутствие между участником закупки и заказчиком конфликта интересов, под которым понимаются случаи, при которых руководитель заказчика, член комиссии по осуществлению закупок, руководитель контрактной службы заказчика, контрактный управляющий состоят в браке с физическими лицами, являющимися выгодоприобретателями, единоличным исполнительным органом хозяйственного общества (директором, генеральным директором, управляющим, президентом и другими), членами коллегиального исполнительного органа хозяйственного общества, руководителем (директором, генеральным директором) учреждения илиунитарногопредприятия либо иными органами управления юридических лиц - участников закупки, с физическими лицами, в том числе зарегистрированными в качестве индивидуального предпринимателя, - участниками закупки либо являются близкими родственниками (родственниками по прямой восходящей и нисходящей линии (родителями и детьми, дедушкой, бабушкой и внуками), полнородными и неполнородными (имеющими общих отца или мать) братьями и сестрами), усыновителями или усыновленными указанных физических лиц. Под выгодоприобретателями для целей настоящей статьи понимаются физические лица, владеющие напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном капитале хозяйственного общества;  7) отсутствие в предусмотренном Законом реестре недобросовестных поставщиков (подрядчиков, исполнителей) информации об участнике закупки, в том числе информации об учредителях, о членах коллегиального исполнительного органа, лице, исполняющем функции единоличного исполнительного органа участника закупки - юридического лица;  8) участник закупки не является офшорной компанией.  9) наличие лицензии ФСБ России на 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 (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).  10) наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации. |
| **31.** | **Условия, запреты и ограничения допуска товаров, происходящих из иностранного государства или группы иностранных государств**  Не установлено |
| **32.** | **Ограничение участия в электронном аукционе**  Участники аукциона в электронной форме должны соответствовать требованиям, установленным документацией об аукционе в электронной форме. |
| **33.** | **Идентификационный код закупки**  ОКПД2: 62 |

Приложение №1

к документации об аукционе

**Техническое задание**

**на поставку серверного оборудования, дисковой полки для системы хранения данных, программного обеспечения, средств защиты информации и выполнение работ по установке, настройке оборудования, созданию системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия»**

**Перечень сокращений**

|  |  |
| --- | --- |
| АРМ | – Автоматизированное рабочее место |
| ГИС | – Государственная Информационная Система |
| ИСПДн | – Информационная система персональных данных |
| ФСБ России | – Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | – Федеральная служба по техническому и экспортному контролю Российской Федерации |
| СЗИ | – Система защиты информации |
| ИС | – Информационная система |
| РД | – Руководящий документ |
| ТТ | – Технические требования |
| ЛВС | – Локальная вычислительная сеть |
| ПО | – Программное обеспечение |
| СУБД | – Система управления базами данных |
| БД | – База данных |
| АРМ | – Автоматизированное рабочее место |
| СЗИ | – Средство защиты информации |
| НСД | – Несанкционированный доступ |
| ОС | – Операционная система |
| НДВ | – Недекларированные возможности |

**Используемые термины**

**Организационно-распорядительная документация (ОРД) -** комплекс документов, закрепляющих функции, задачи, цели, а также права и обязанности работников и руководителей по выполнению конкретных действий, необходимость которых возникает в операционной деятельности организации.

**Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

**Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.**

**Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.**

**Заказчик**– Государственное втономное Учреждение Культуры Республики Бурятия «Государственный Архив Республики Бурятия»

**Аттестация объекта информатизации** - комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

**Работы** – проведение обследования объектов информатизации Конечного пользователя, установка и настройка средств защиты информации, разработка ОРД по защите ПДн для Конечного пользователя, аттестация объектов информатизации Конечного пользователя.

**1. Общие сведения**

**1.1. Полное наименование работ**

Поставка серверного оборудования, дисковой полки для системы хранения данных, создание системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия»

**1.2. Наименование Заказчика**

Государственное автономное учреждение культуры Республики Бурятия «Государственный Архив Республики Бурятия»

**1.3. Адрес проведения работ:**

670001, Республика Бурятия, г. Улан-Удэ,, ул. Ленина, дом № 54.

**2. Основные этапы работ**

2.1. Поставка серверного оборудования;

2.2. Поставка лицензий на системное программное обеспечение (не ниже WindowsServer 2012) и программное обеспечение для среды виртуализации (VMware);

2.3. Проектирование системы защиты информации;

2.4. Поставка средств защиты информации;

2.5. Установка и настройка средств защиты информации;

2.6. Проведение аттестации ИС по требованиям безопасности.

**3. Цели создания СЗИ**

3.1. Целями создания СЗИ являются:

- обеспечение защищенности ИС в процессе обработки и хранения информации, обеспечение конфиденциальности информации при ее обработке, а также других необходимых свойств информации (целостности, доступности и т.д.);

- соответствие требованиям обеспечения информационной безопасности при обработке ПДн в ИС, установленных РД ФСТЭК России и ФСБ России.

**4. Результаты создания СЗИ**

4.1. В результате создания СЗИ должно быть обеспечено выполнение требований по защите конфиденциальной информации, содержащейся в государственных информационных системах Конечного пользователя, а также требования по обеспечению безопасности ПДн при их обработке в ИС Конечного пользователя.

4.2. Критериями оценки достижения поставленных целей по созданию СЗИ являются:

– соответствие требованиям по защите информации, установленным приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», - соответствие требованиям по защите информации;

соответствие требованиям по защите персональных данных, установленным приказом 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»;

- соответствие иным требованиям по защите информации, установленным РД ФСТЭК России и ФСБ России;

– выполнение всех требований настоящих Требований;

4.3. Подтверждением соответствия результатов работ в рамках настоящих Требований является аттестация ИС на соответствие требованиям безопасности информации.

**5. Обязательные требования к СЗИ**

5.1. Создаваемая СЗИ должна обеспечивать выполнение всех требований, установленных нормативными правовыми актами, руководящими документами, указанными в пункте 8.2. настоящих Требований.

5.2. Создаваемая СЗИ должна обеспечивать возможность:

– работы в сети «Интернет» (электронной почты) на каждом АРМ;

– поступления и обработки запросов, поступающих из Федеральных органов исполнительной власти, органов государственных внебюджетных фондов Российской Федерации в рамках межведомственного электронного взаимодействия;

– осуществления безопасной передачи сведений в электронной форме по каналу связи (в том числе сети «Интернет») с электронной подписью и шифрованием;

– возможность поэтапного подключения образовательных учреждений в защищенную сеть (масштабируемость);

– организации взаимодействия с организациями-участниками.

5.3. Состав программного обеспечения

* Microsoft Windows Server 2008/2012 Standard R2 насерверахИС.
* MicrosoftWindows 7/8/8.1 Prof на рабочих местах.

**6. Состав работ по проектированию системы защиты**

**6.1. Работы по проектированию СЗИ должны включать в себя:**

– предпроектное обследование;

– разработка технического задания;

– разработка организационно-распорядительной документации.

Во время проведения предпроектного обследования должны быть проведены следующие работы:

– определен состав обрабатываемых ПДн в ИС;

– определена граница контролируемой зоны;

– определено используемое в ИС программное обеспечение;

– определены используемые в ИС информационные технологии.

– определены состав и тип применяемых в ИС средств защиты информации;

– определены технологические процессы обработки ПДн в ИС;

– определены внешние и внутренние информационные потоки;

– определен необходимый класс защищенности ИС;

– определен необходимый уровень защищенности ПДн;

– определен состав, содержание и сроки проведения мероприятий по этапам модернизации СЗИ.

**6.2. Техническое задание**

Разрабатываемое Исполнителем Техническое задание должно соответствовать требованиям следующих нормативных правовых актов (в редакциях с изменениями, вступившими в силу на момент проведения работ):

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

– постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»;

– ГОСТ 19.201-78 ЕСПД. Техническое задание. Требования к содержанию и оформлению;

– руководящего документа РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;

– приказа ФСБ России от 10.07.2014 № 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»;

– приказа ФАПСИ от 13.06.2001 № 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»;

– приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– нормативно-методического документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного приказом заместителя директора ФСТЭК от 15.02.2008;

– нормативно-методического документа «Базовая модель угроз безопасности персональных данных в информационных системах персональных данных», утвержденного приказом заместителя директора ФСТЭК от 15.02.2008;

– руководящего документа «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282;

– иных нормативных правовых актов, руководящих документов, устанавливающих требования по защите ПДн, обрабатываемых в ИС.

Техническое задание должно включать:

– исходные данные, описывающие существующие у Конечного пользователя ИСПДн, их характеристики и количество обрабатываемых ПДн;

– перечень применяемых Конечным пользователем программных средств и информационных технологий;

– перечень технических средств, их размещение относительно контролируемой зоны;

– информационные потоки ПДн;

– описание технологических процессов обработки данных по каждой ИСПДн;

– определение требуемых классов защищенности;

– общие требования, предъявляемые к СЗИ;

– перечень необходимых мер защиты, которые должна реализовывать СЗИ;

– перечень предполагаемых к использованию средств защиты информации.

Техническое задание должно быть согласовано с Заказчиком.

**6.3. Организационная распорядительная документация**

Исполнителем должны быть разработаны и предоставлены на согласование Конечному пользователю проекты организационных распорядительных документов по обеспечению безопасности персональных данных в ИС.

Организационные меры при проектировании СЗИ должны включать в себя разработку следующих ОРД:

**6.3.1. Базовые документы, на основе и в соответствии с которыми разрабатывается система защиты информации:**

1. Концепция информационной безопасности;
2. Политика информационной безопасности;
3. Частная модель угроз безопасности ПДн при их обработке в ИС;
4. Модель нарушителя;
5. Описание технологического процесса;
6. Техническое задание;
7. Матрица разграничения доступа;

**6.3.2. Приказы:**

1. Приказ о назначении лиц, ответственных за обработку ПДн в ИС;
2. Приказ о назначении лиц, имеющих доступ к ПДн;
3. Приказ о назначении комиссии по классификации ИС;
4. Приказ об утверждении мест хранения материальных носителей ПДн;

**6.3.3. Положения:**

1. Положение об обработке ПДн субъектов ПДн;
2. Положение о защите ПДн в ИС;
3. Положение о подразделении по защите ПДн в ИС;
4. Положение о режиме безопасности в помещениях;
5. Положение об обработке ПДн без использования средств автоматизации;

**6.3.4. Планы:**

1. План мероприятий по защите ПДн;
2. Порядок проведения внутренних проверок защиты ПДн;

**6.3.5. Журналы:**

1. Журнал учета съемных носителей;
2. Журнал учета применяемых СЗИ, эксплуатационной и технической документации к ним;
3. Журнал по учету мероприятий по контролю обеспечения защиты ПДн в ИС;
4. Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке ПДн в ИС;
5. Журнал обращений пользователей информационной системы к ПДн;
6. Журнал поэкземплярного учета СКЗИ;
7. Журнал учета хранилищ;
8. Технический (аппаратный) журнал;

**6.3.6. Инструкции:**

1. Инструкция администратора информационной безопасности ИС;
2. Инструкция пользователя ИС;
3. Инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций;
4. Правила рассмотрения запросов субъектов ПДн;

**6.3.7. Перечни:**

1. Перечень защищаемых ресурсов;

**6.3.8. Акты:**

1. Акт классификации ИС;
2. Акт уничтожения документов, содержащих ПДн субъектов.

**7. Поставка средств защиты информации**

7.1. В рамках поставки по настоящим Требованиям должны быть поставлены необходимые средства защиты информации, прошедшие в установлено порядке сертификационные испытания в соответствии с действующим законодательством Российской Федерации.

7.2. Исполнитель должен поставить средства защиты информации, соответствующие требованиям (характеристикам), указанным в Таблице 2 настоящих Требований.

Таблица 1. Требования к СЗИ

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Наименование СЗИ** | **Количество** |
| 1 | СЗИ от НСД должна представлять собой программный комплекс средств защиты информации в операционных системах (ОС) семейства Windows с возможностью подключения аппаратных идентификаторов.  СЗИ от НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением ОС Windows XP, WindowsServer  2003, WindowsVista, WindowsServer 2008, Windows 7, WindowsServer 2008 R2, Windows 8, WindowsServer 2012 в многопользовательском режиме их эксплуатации.  СЗИ от НСД должна поддерживать 32- и 64-битные версии ОС.  Система должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию WindowsToGo.  СЗИ от НСД должны быть сертифицированы по требованиям РД ФСБ России, ФСТЭК России, Гостехкомиссии России по 3 классу защиты от НСД для СВТ и 2 уровню контроля отсутствия НДВ, разрабатываться и производиться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере.  Сертификат соответствия должен позволять использовать СЗИ от НСД для защиты:  - конфиденциальной информации и государственной тайны в автоматизированных системах до класса защищенности 1Б включительно;  - в государственных информационных системах 1 класса защищенности;  - для обеспечения 1 уровня защищенности персональных данных.  СЗИ от НСД должна обеспечивать:  - регистрацию различных пользователей: локальных, доменных, сетевых.  - определение количества одновременных сеансов для пользователя;  - идентификацию и проверку подлинности пользователей при входе в ОС, а также аутентификацию при входе на ПЭВМ до начала загрузки ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор;  - реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;  - должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;  - для предотвращения утечки информации с использованием сменных накопителей СЗИ от НСД должна позволять разграничивать доступ как к отдельным типам накопителей, так и к конкретным экземплярам;  - в соответствии с требованиями к СЗИ от НСД должны использоваться два принципа контроля доступа: мандатный и дискреционный;  - возможность ограничивать средствами СЗИ от НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);  - регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение компьютера, вход/выход пользователей, доступ к ресурсам, печать документов с возможностью добавления штампов и сохранение теневых копий распечатываемых документов, запуск/остановка процессов, администрирование).  - должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей.  - возможность организации замкнутой программной среды и различные способы ее настройки;  - возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);  - возможность контроля целостности программно-аппаратной среды при загрузке ПЭВМ по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при  выявлении изменений;  - очистку остаточной информации (освобождаемого дискового пространства, зачистку определённых файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Запрет смены пользователей без перезагрузки;  - возможность самодиагностики основного функционала СЗИ от НСД с формированием отчета;  - возможность добавления штампа на распечатываемые документы (произвольного или по ГОСТ). | 3 |
| 2 | * Двухфакторную аутентификацию пользователя в системе, должен выполнять аппаратный ключ со следующими техническими требованиями: * Интерфейс: USB 1.1 и выше; * Объем доступной EEPROM память не менее: 60 Кбайт; * Габаритные размеры (не более): 60х20х10 мм; * Наличие 32-битового уникального серийного номера; * Поддержка стандартов: ISO/IEC 7816, PC/SC, ГОСТ 28147-89, MicrosoftCrypto API и MicrosoftSmartcard API, PKCS#15 (v. 2.10+); * Аппаратная реализация ГОСТ 28147-89; * Защищенное хранение ключей шифрования; * Встроенная файловая система по стандарту ISO/IEC 7816; * Прозрачное шифрование файловой системы по ГОСТ 28147-89; * Двухфакторная аутентификация с использованием PIN кода и носителя; * Ограничение числа попыток ввода PIN-кода; * 3 уровня доступа к токену: Гость, Пользователь, Администратор; * Потребляемая мощность до 120 mW; * Диапазон рабочих температур/ температур хранения От 0 до +70 o C / От –10 до +80 o C; * Допустимая относительная влажность от 0 до 100 % (без конденсата); * Наличие автоматической блокировки PIN после 15 неверных попыток ввода; * Количество циклов записи в память /чтения из памяти не менее 1,000,000 / не ограничено; * Гарантированное количество подключений к USB порту не менее 5,000; * Поддержка стандарта X.509. * Реализация функционала должна быть максимально безопасной необходимые алгоритмы должны изначально присутствовать в микропрограмме, а не добавляться дополнительными загружаемыми модулями (аплетами, плагинами и т.п.); * Наличие энергонезависимой памяти не менее  64 Кб.  Требование по наличию сертификата ФСТЭК России Средство защиты должно соответствовать классам не ниже: 4 уровня контроля отсутствия НДВ и возможность применения в ИСПДн до 1 класса включительно. | 2 |
| 3 | Средство для обеспечения защиты виртуальной инфраструктуры должно представлять программный комплекс со следующими характеристиками:  ***Требования к поддержке платформ виртуализации:***   * VMware vSphere 4.1 Update 3 (VMware ESXi Server 4.1) * VMware vSphere 5 (VMware ESXi Server 5.0 Update 3) * VMware vSphere 5.1 (VMware ESXi Server 5.1 Update 2) * VMware vSphere 5.5 (VMware ESXi Server 5.5 Update 1) * VMware vSphere 6.0 (VMware ESXi Server 6.0) * VMware View 4.5 * VMware View 5 * VMware View 5.1 * VMware Horizon View 5.2   ***Должно осуществлять:***   * Аутентификацию администраторов виртуальной инфраструктуры и администраторов безопасности; * Защиту средств управления виртуальной инфраструктурой от НСД; * Защиту ESX-хостов от НСД; * Контроль целостности конфигурации виртуальных машин и их доверенную загрузку; * Мандатный принцип контроля доступа; * Регистрацию событий, связанных с информационной безопасностью; * Контроль целостности и защиту от НСД компонентов СЗИ; * Централизованное управление и мониторинг; * Возможность построения отчетов.   ***Требования к функциональности:***  - **Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности**  В ПО должна быть реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью (для ограничения на использование привилегий суперпользователя). Должна быть возможность выделить 2 основные роли — администратор виртуальной инфраструктуры и администратор безопасности. Должна быть поддержка аппаратных идентификаторов eToken и iButton.  *Реализация принципа разделения ролей*  Доступ на управление виртуальной инфраструктурой или параметрами безопасности должен предоставляться только для аутентифицированных пользователей. Для этого в СЗИ должна быть предусмотрена процедура аутентификации пользователей и компьютеров (рабочих мест администраторов), которая должна осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа ManintheMiddle.  Процедура аутентификации должна осуществляется с помощью отдельной программы, которую требуется запустить и ввести учетные данные до того, как осуществляется соединение с виртуальной инфраструктурой.  Функционал аутентификации на рабочем месте администратора должен предоставлять возможность надежно сохранить учетные данные.  СЗИ должно иметь собственную систему учетных записей или иметь возможность интегрироваться с MicrosoftActiveDirectory.  СЗИ должно поддерживать работу администраторов виртуальной инфраструктуры как через «толстый» клиент (vSphereclient), так и через «тонкий» (vSphereWeb-client).  **- Защита средств управления виртуальной инфраструктурой от НСД**  К средствам управления виртуальной инфраструктурой относятся:   * ESX-хосты, предназначенные для запуска виртуальных машин; * серверы vCenter, предназначенные для централизованного управления виртуальной инфраструктурой; * серверы vSphereWebClient, предназначенные для поддержки управления виртуальной инфраструктурой через «тонкий» клиент; * средства, предназначенные для обслуживания инфраструктуры, например, VMwareConsolidatedBackup, VMwareUpdateManager; * сторонние средства мониторинга и управления инфраструктурой.   Компрометация любого из этих средств приводит к компрометации группы виртуальных машин или всей виртуальной инфраструктуры.  Для обеспечения защиты средств управления виртуальной инфраструктурой должен применяется функционал мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Для этого весь управляющий трафик должен проходить через компонент СЗИ, осуществляющий этот контроль. Правила разграничения доступа должны работать на основе меток и уровней безопасности, а также заданных ACL и параметров соединения (протоколов, портов).  Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами должен подписываться, для обеспечения защиты от атак типа ManintheMiddle в процессе сетевого взаимодействия.  В ПО должен присутствовать механизм блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой. Тем самым должна обеспечивается защита средств управления виртуальной инфраструктурой от НСД со стороны скомпрометированной виртуальной машины.  **- Защита ESX-хостов от НСД**  В рамках обеспечения защиты ESX-хостов от НСД в СЗИ должны быть реализованы следующие механизмы:   * Возможность создания списка разрешенных программ; * Возможность создания списков запрещенных и разрешенных устройств: * Возможность создания списка пользователей, которым разрешен локальный вход на ESX-сервер; * Возможность блокирования подключения USB-носителей к ESX-серверу; * Возможность осуществления контроля за правилами встроенного межсетевого экрана; * Возможность запрета клонирования и создания снимков виртуальных машин; * Возможность очистки внешней и оперативной памяти при окончании работы с виртуальной машиной; * Возможность контроля обеспечения обязательной аутентификации в однопользовательском режиме; * Возможность ограничения доступа к конфигурационным файлам служб; * Возможность контроля использования протокола SSH версии 2; * Возможность модификации файла /etc/securetty для ограничения входа в систему под учетной записью root; * Возможность запрета на выполнение операций с буфером обмена для каждой виртуальной машины; * Возможность ограничения списка пользователей, которым разрешено выполнять назначенные задания; * Возможность ограничения доступа к конфигурационным файлам планировщика заданий; * Возможность установки ограниченных полномочий на файлы по умолчанию для демонов и root; * Возможность контроля использования разных сетей для Service Console и виртуальных машин; * Возможность контроля использования CHAP для проверки подлинности при подключении iSCSI-устройств; * Возможность контроля установленных параметров журналирования, требований к сложности пароля и доступа по сети; * Возможность запрета просмотра, изменения и выполнения vmdk-файлов; * Возможность запрета изменения vmx-файлов; * Возможность защиты от нехватки места на корневой файловой системе ESX-сервера; * Возможность контроля наличия пароля загрузчика ESX-сервера; * Возможность контроля настроенных параметров ядра ESX-сервера; * Возможность запрета контроля устройств ESX-сервера со стороны виртуальных машин; * Возможность запрета отсылки сообщений ESX-серверу со стороны виртуальных машин; * Возможность контроля прав на файлы журнала событий ESX-сервера; * Возможность задания приглашения для сетевого и локального доступа к ESX-серверу; * Возможность контроля настроек синхронизации времени; * Возможность контроля доступа к файлам, содержащим пароли пользователей; * Возможность ограничения доступа к конфигурационным файлам протокола SNMP; * Возможность настройки параметров безопасности для протокола SSH; * Возможность ограничения на удаление файлов ESX-сервера; * Возможность контроля отсутствия программ с setuid или setgid флагами; * Возможность ограничения права перезаписи файлов ESX-сервера; * Возможность запрета отсутствия файлов без владельца на ESX-сервере;   **- Контроль целостности конфигурации виртуальных машин и доверенная загрузка**  Для обеспечения контроля целостности программной среды и обеспечения доверенной загрузки операционной системы (ОС) в «физическом мире» традиционно используются аппаратные электронные замки для шин PCI или PCI-E. Подобные аппаратные СЗИ невозможно использовать для защиты виртуальных машин по техническим причинам. Тем не менее, данный функционал защиты должен быть обеспечен и в виртуальной среде.  ПО должно содержать компоненты, устанавливаемые на каждый ESX-хост и реализующие следующие механизмы защиты:   * Контроль целостности настроек виртуальной машины перед ее загрузкой. Должен контролироваться файл \*.vmx, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров. * Контроль образа BIOS виртуальной машины. Поскольку несанкционированная подмена BIOS является угрозой безопасности, СЗИ должно контролировать целостность файла \*.nvram, в котором содержится образ BIOS виртуальной машины. * Доверенная загрузка ОС должна осуществляться путем контроля целостности загрузочного сектора виртуального диска \*.vmdk. * Контроль целостности файлов гостевой ОС внутри виртуальных машин.   При изменении одного из перечисленных объектов как санкционированном, так и несанкционированном, СЗИ должно предоставить администратору безопасности возможность данные изменения отменить или принять. До того, как администратор безопасности примет решение, вносимые изменения применяться к объекту не должны.  **- Мандатный принцип контроля доступа**  В СЗИ должен быть реализован мандатный принцип контроля доступа на основе меток конфиденциальности. Должно присутствовать два вида меток конфиденциальности: иерархические (далее просто метки) и неиерархические (далее просто категории).  Должна быть реализована возможность пометить метками следующие субъекты, объекты, контейнеры:   * Администраторы ВИ * ESX-хосты * Сетевые карты ESX-хоста или VLAN * Разделы хранилищ (Datastore) * ВМ   Права доступа субъектов и объектов должны проверяться на основе меток и категорий автоматически и запрещать несанкционированные действия. Субъект может получить доступ к объекту, только если выполняется условие соответствия их меток конфиденциальности. Для категорий – это совпадение хотя бы одной из категорий субъекта и объекта, для меток – это уровень иерархии субъекта должен быть равен (или выше, в зависимости от настроек СЗИ) уровню объекта.  Категории должны отличаться от меток следующими параметрами:   * Метки должны быть иерархическими, категории равноправными. * Механизмы работы меток должны зависеть не только от пользователя, но и от его меток его текущей сессии. Категории от сессии зависеть не должны. * Любой субъект, объект, контейнер может быть помечен несколькими категориями и только одной меткой.   **- Регистрация событий, связанных с информационной безопасностью**  В СЗИ должен быть реализован механизм регистрации следующих групп событий:   * События аутентификации и разграничения доступа; * Средство должно регистрировать как удачные, так и неудачные попытки доступа к инфраструктуре (с указанием имени учетной записи, даты, имени компьютера или его IP-адреса) * Средство должно регистрировать события изменений конфигурации параметров безопасности и учетных записей администраторов инфраструктуры * События контроля целостности СЗИ, контроля целостности и доверенной загрузки виртуальных машин; * События, связанные с установкой, удалением, включением, остановом и сбоем компонентов СЗИ, а также с изменением настроек СЗИ.   Регистрация событий на всех компонентах СЗИ должна осуществляется в едином журнале. Для всех групп событий должны регистрироваться как факты НСД, так и правомочные действия.  **- Контроль целостности и защита от НСД компонентов СЗИ**  СЗИ должен содержать собственные механизмы контроля целостности компонентов СЗИ. Механизмы должны действовать на всех компонентах СЗИ — рабочем месте администратора, сервере авторизации, ESX-хостах и vCenter-серверах.  - **Централизованное управление и мониторинг**  СЗИ должно содержать Консоль управления, устанавливающуюся на рабочее место администратора безопасности со следующим функционалом:   * управление пользователями и компьютерами (пользователями в данном случае будут администраторы виртуальной инфраструктуры и администраторы безопасности, а компьютеры — это их рабочие места); * назначение прав на доступ к защищаемым объектам; * развертывание и настройка компонентов защиты ESX-хостов; * настройка правил разграничения запуска виртуальных машин и утверждение изменений параметров виртуальных машин, произведенных администраторами ВИ; * просмотр журнала регистрации событий.   Все изменения, произведенные администратором безопасности, должны сохраняться централизованно.  - **Возможность построения отчетов**  СЗИ должно предоставлять возможность генерации отчетов на основании произошедших в системе событий. В перечень отчетов должны входить следующие отчеты:   * Изменение конфигурации политик безопасности. * Использование учетных записей VMware. * Мониторинг учетных записей СЗИ. * Проблемы с доверенной загрузкой ВМ. * Настройка правил сетевой безопасности. * Настройки доступа к защищаемым объектам. * Соответствие стандартам безопасности. * Изменение мандатных правил доступа в СЗИ * Logon в нерабочее время * Изменение сетевых правил доступа в СЗИ * Попытки несанкционированного изменения настроек, контролируемых политиками * Применение политик безопасности * Проблемы с Logon в СЗИ. (В отчёте нужно задать число неоднократных попыток) * Проблемы с Logon в vSphere (В отчёте нужно задать число неоднократных попыток) * Проблемы со сменой пароля * Наиболее активные пользователи * Список наиболее используемых видов доступа (порты/протоколы) к защищаемым объектам * Список наиболее частых событий ИБ * Отчеты по соответствию лучшим практикам и стандартам   ***Требования по сертификации:***  - должен быть сертифицирован на соответствие требованиям ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа (далее – НСД) к информации. Показатели защищенности от НСД к информации» по классу не ниже 5-го;  - должен быть сертифицирован на соответствие требованиям ФСТЭК России «Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню не ниже 4-го;  - должен быть сертифицирован на соответствие требованиям ФСТЭК России для защиты информационных систем персональных данных (ИСПДн) с уровнем защищенности персональных данных до 1-го включительно;  - должен быть сертифицирован на соответствие требованиям ФСТЭК России для защиты государственных и муниципальных информационных систем (ГИС) до 1 класса включительно;  - должно подтверждаться соответствующими действующими сертификатами ФСТЭК  ***Комплект поставки:***   * Право на использование СЗИ для защиты ESX-хостов (за 1 физический процессор на защищаемом ESX-хосте) – 4 шт. * Установочный комплект, включающий: диск с ПО и документацией, формуляр, наклейка и сертификат (ФСТЭК) – 1 шт. | 1 |
| 4 | Передача неисключительных прав на воспроизведение программного обеспечения, реализующего функции криптографического клиента, отвечающего следующим требованиям:   * совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящей конкурсной документации: обновление программного обеспечения, обновление справочно-ключевой информации, управлением политиками безопасности; * совместимо (полностью) с программным комплексом, реализующим функции криптографического шлюза, представленным в настоящей конкурсной документации: шифрование/дешифрование направляемого/принимаемого IP-трафика; * поддержка операционных систем: * MicrosoftWindows 2000 Professional; * Microsoft Windows XP Home/Professional; * Microsoft Windows Vista (всялинейка); * MicrosoftWindows 7 (вся линейка). * MicrosoftWindows8/8.1(вся линейка). * наличие сертификата ФСТЭК России по требованиям к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно; * наличие сертификата ФСБ России по классу КС2; * иметь встроенный персональный экран, соответствующий 3-ому классу по требованиям ФСТЭК России; * предоставлять функции клиента службы обмена файлами и сообщениями, защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами; * 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; * возможность удаленного централизованного обновления адресной и ключевой информации комплекса с контролем прохождения обновления; * автоматическое распределение симметричной ключевой информации при появлении в сети новых пользователей, задании в Центре управления сетью новых связей или удалении существующих связей, компрометации ключей или штатных процедурах смены ключевой информации. * взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (бех использования криптографического шлюза»). | 2 |
| 5 | сертифицированная комплексная защита компьютера с помощью межсетевого экрана, системы обнаружения вторжений  ***Должно осуществлять защиту компьютера от внешних угроз:***  - межсетевое экранирование для рабочего места в сетях TCP/IP;  - защиту компьютера от атак по сети TCP/IP;  - антивирусную защиту от вредоносного программного обеспечения;  - защиту от спама и вредоносного контента веб-серверов;  - самозащиту от воздействия со стороны вредоносного программного обеспечения;  - регистрацию событий безопасности;  - иметь соответствующие сертификаты ФСТЭК;  ***Требования к операционной платформе и аппаратной части***:  - Windows 8, 7, Vista, XP x86/x64; Windows Server 2012 x64; Windows Server 2008 R2 x64, Server 2008 x86/x64; Windows Server 2003 R2 x86/x64, Server 2003 x86/x64;  - наличие привода CD-ROM;  - минимально необходимый размер оперативный памяти: 512 Мбайт.  ***Требования к централизованному управлению:***  - должно обеспечивать централизованную установку, удаление и обновление ПО на защищаемых рабочих станциях как в доменных сетях с MicrosoftActiveDirectory, так и в сетях с рабочими группами;  - должно обеспечивать удаленную настройку и управление с рабочего места администратора, объектами управления могут быть отдельные компьютеры, группы компьютеров (организационные подразделения);  - должно обеспечивать отслеживание событий безопасности.  ***Требования к функциональности средства межсетевого экранирования:***  - должно иметь сертификат ФСТЭК в соответствии с руководящим документом "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (Гостехкомиссия России, 1997) не ниже, чем по 4-му классу защищенности;  - должно соответствовать: классификация по уровню отсутствия недекларированных возможностей (Гостехкомиссия России, 1999) не ниже, чем по 4-му уровню контроля;  - должно контролировать входящие и исходящие соединения;  - должно обеспечивать контроль для приложений, использующихся на компьютере, при обращении к сети и создание правил сетевого доступа для приложений;  - режим обучения для сетевого доступа для приложений;  - разделение доступа к узлам сети;  - создание разрешенного и запрещенного списков сетевых ресурсов;  - возможность экспорта/импорта настроек межсетевого экрана с одного компьютера на другой;  - должно обеспечивать блокировку активного содержимого страниц веб-серверов;  - должно обеспечивать блокировку активного содержимого входящих электронных писем;  - должно обеспечивать регистрацию событий безопасности.  ***Требования к функциональности системы обнаружения вторжений:***  - должно соответствовать: требованиями руководящего документа "Требования к системам обнаружения вторжений" (утвержден приказом ФСТЭК России от 6 декабря 2011 г. № 638) для уровня узла по 4-му классу защиты;  - должно обеспечивать настройку на обнаружение типовых сетевых атак;  - должно обеспечивать блокировку сетевых сканеров;  - должно обеспечивать блокировку вредоносных процессов при их попытках воздействия на рабочие процессы;  - должно обеспечивать непрерывный мониторинг;  - должно обеспечивать регистрацию событий безопасности. | 1 |
| 6 | Система антивирусной защиты, в которую входят:  1. Лицензия для Серверных ОС – 1шт.  2. Лицензия для рабочих мест – 2 шт.  **Антивирусная защита должна обеспечивать:**  - обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;  - защиту от еще неизвестных вредоносных программ, принадлежащих зарегистрированным семействам, как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;  **- обнаружение угроз направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля**  Используемое антивирусное ядро:  - не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;  - в целях оптимального расхода ресурсов должно, в зависимости от загрузки системы, выбирать уровень анализа упакованных объектов;  - в целях оптимального расхода ресурсов должно использовать механизм уменьшения размера промежуточных файлов;  **- в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;**  - Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов  - Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий  - управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов  - экспорта и импорта базы данных антивирусного сервера в XML-файл.  - создания иерархической сети антивирусных серверов. В случае реализации иерархической сети Система должна иметь возможность:  - объединения информации от нескольких серверов на одном.  - распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть.  - обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий  - контроля отсутствия связанных серверов в расписании антивирусного сервера.  - построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне;  **- централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line.**  - наличия множественных путей уведомления пользователей и администраторов путем посылки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap;  **- оповещения о возникновении эпидемий (множественных инфекций)**  **- оповещения о наличии обновлений сервера ESS**  - управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений  - контроля результатов обновления антивирусного ПО на станциях антивирусной сети.  - организации межсерверного обмена согласно расписанию  - ограничения канала связи по группам  - наличия возможности групповых обновлений  **- обновлений по защищенному каналу с использованием SSL-сертификатов**  - организации отложенного обновления  - проверки обновлений на выбранных администратором компьютерах/группах перед распространением их на все клиентские компьютеры  - централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на станции, находящиеся в разных доменах.  **Система управления должна поддерживать возможность:**  - создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера;  - восстановления удаленных станций.  **Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью:**  - прямого их указания в системе управления в результате сканирования локальной сети, MicrosoftActiveDirectory,  - политикMicrosoft Active Directory  - синхронизациистанцийс Microsoft Active Directory  - установки с помощью дистрибутива, содержащего все компоненты защиты  - рассылки инсталляционных файлов из системы управления по электронной почте  - возможностей службы распределенной файловой системы (DFS).  - Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу  - Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов. cистема управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети  - В целях ограничения использования серверного пространства должна иметься возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя)  - Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль.  - Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов ActiveDirectory, LDAP и RADIUS  - возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах  - возможностьмножественности путей обновления, в том числе по каналам связи и на съемных электронных носителях информации;  - возможность обновления через прокси-серверы, в том числе прокси-серверы MSISA/TMG.  - проверка целостности и подлинности обновлений средствами электронной цифровой подписи.  - в Системе, не имеющей доступа к сети Интернет, должна быть реализована возможность обновления вирусных баз путём скачивания их с сервера разработчика Системы с возможностью последующего их переноса в Систему с помощью любого носителя информации, в том числе с помощью мобильного сервера обновлений, созданного на основе flash-диска;  - В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория;  - Система должна иметь возможность перезагрузки защищаемой станции через систему управления  **Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства MicrosoftWindows**  Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:  - осуществление антивирусной (включая **постоянную защиту от руткит-технологий**) и антиспам защиты на рабочих станциях.  - Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки без существенного снижения производительности защищаемых рабочих станций. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.  - Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.  - непрерывное фоновое сканирование в целях нейтрализации активных угроз  - ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию  - помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»;  - просмотр местоположения станций и серверов на карте, если заданы географические координаты станции  - Система защиты рабочих станций должна обеспечивать проверку протоколов:  - HTTP;  - IMAP, SMTP, POP3 независимо от используемого почтового клиента;  - NNTP (только проверка на вирусы), независимо от почтового клиента.  - Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макровирусов, опасных Java-апплетов, ActiveX и др.) посредством:  - антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;  - проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.  - В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.  - **Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе семейств Trojan.Encoder, Trojan.Inject и Trojan.Winlock) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов**  **Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства MicrosoftWindows**  Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:  Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий.  Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.  Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию, должна обеспечивать защиту серверов под управлением операционных систем:  Microsoft Windows Server 2000;  Microsoft Windows Server 2003;  Microsoft Windows Server 2008.  Microsoft Windows Server 2012  Компоненты Системы должны устойчиво функционировать на серверах в условиях их минимальной и максимальной загрузки без существенного снижения производительности.  Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.  Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках, имеющихся у них прав.  Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы.  В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.  Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.  Система должна обеспечивать:  поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;  проверку всех скриптов, обрабатываемых в MicrosoftInternetExplorer, а также любых WSH-скриптов (JavaScript, VisualBasicScript и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;  блокировку опасных макросов VBA в реальном времени;  защиту от вредоносных сценариев, загружаемых с веб-страниц;  помещение найденных зараженных файлов в специальное место на жестком диске —«карантин»;  автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;  запуск задач по расписанию и/или сразу после загрузки операционной системы.  Система защиты серверов под управлением семейства ОС MicrosoftWindows должна обеспечивать реализацию следующих функциональных возможностей:  проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством:  антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;  проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.  В Системе должна быть реализована самозащита для всех ее объектов, в том числе критических файлов, процессов, окон, ключей и прочего, от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.  **Требования по комплектности поставке**  В состав Системы должны входить:  программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;  программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;  программные средства централизованного управления, мониторинга и обновления;  обновляемые базы данных сигнатур всевозможных вредоносных программ.  Комплект поставки должен содержать:   1. Установочный диск с дистрибутивом 2. Формуляр 3. Специальный защитный знак   Сертификат соответствия требованиям безопасности информации  необходимый набор серийных номеров либо ключевых файлов;  Система должна быть сертифицирована уполномоченным органом (ФСТЭК) на соответствие ТУ и НДВ 2 на применение в составе подсистемы антивирусной защиты информационных системах персональных данных (ИСПДн) класса К1.  Система должна быть сертифицирована уполномоченным органом (ФСТЭК) на соответствие требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 2 и требованиям технических условий.  **Требования по технической поддержке Системы**  Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.  Техническая поддержка должна включать возможность предоставления выделенного специалиста, доступного в режиме 5/8  Техническая поддержка должна включать возможность проведения расследования компьютерных инцидентов  Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе:  ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения;  ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определение того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения.  Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя. | 1 |
| 7 | Криптографический клиент необходимый для защищенного подключения Разработчиков ИС:  Программное обеспечение (ПО) должно уметь выполнять следующие функции: межсетевое экранирование, построение виртуальных частных сетей (VPN), обеспечение стойкого шифрования передаваемой информации.  ПО должно иметь возможность обеспечения защиты и фильтрации трафика сетей и служебного трафика.  ПО должно обеспечивать пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней.  ПО должно уметь маскировать реальный IP адрес (туннелирование трафика).  ПО должно поддерживать технологии протоколирования событий (syslog) и мониторинга глобальной статистики по протоколу SNMP.  ПО должно поддерживать установку в режиме One-Click-Installation (OCI) с использованием WindowsInstaller (MSI)  ПО должно поддерживать следующие алгоритмы:  шифрование ГОСТ 28147-89,  электронно-цифровая подпись ГОСТ Р 34.10-2001,  вычисление хэш сумм ГОСТ Р 34.11-94.  Комбинированный алгоритм шифрования с проверкой целостности ESP\_CIMIT G2814789CPRO1-K288-CNTMAC-253  ПО должно поддерживать работу через NAT.  ПО должно поддерживать работу по протоколам IKE/IPsec согласно cтандартамRFC 2401 – 2412.  ПО должно иметь возможность получения сертификатов открытых ключей по протоколу LDAP, возможность импорта и доставки через PKCS#7, PKCS#12.  ПО должно поддерживать использование списка отозванных сертификатов CRL.  ПО должно задавать независимые правила классификации и маркирования для входящего и исходящего трафика  ПО должно быть совместим с ОС:  MS Windows XP Professional (SP3)  MS Windows Vista (SP2)  MS Windows 7  MS Windows 8  Microsoft Windows Server 2003/2008/2008R2/2012  в т.ч. виртуальной среде  (VMWare/ HyperV/ Xen).  ПО должно быть совместим с программным комплексом CSPVPNClient  ПО должно поставляться на съемном CD носителе  Гарантийный срок не менее 12 мес.  ПО должно иметь сертификат ФСБ России на соответствие требованиям к СКЗИ класса КС1 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.  ПО должно иметь сертификат ФСТЭК на соответствие требованиям к межсетевым экранам по 3-ему классу защищенности.  ПО должно иметь сертификат ФСТЭК на соответствие классификации по уровню контроля отсутствия недекларированных возможностей по 3 уровню контроля и может использоваться в автоматизированных системах класса защищенности до 1В включительно, а также в государственных информационных системах до 1 класса защищенности включительно, в том числе, обеспечивающих 1, 2, 3 и 4 уровни защищенности персональных данных.  На ПО должны распространяться стандартные обязательства годовой технической поддержки. | 1 |
| 8 | Операционная система должна отвечать следующим функциональным возможностям:  - Условия поставки должны соответствовать правилам лицензирования производителя программного обеспечения;  - Совместимость со всеми поставляемыми в данном ТЗ средствами защиты информации;  - Интуитивно понятный пользовательский интерфейс;  - Поддержка подключения нескольких мониторов;  - Наличие функции быстрого переключения между пользователями;  - Эмулятор запуска приложений в текущей системе,  совместимые с разными версиями OC Windows;  - Наличие функции диагностирования, восстановления при сбое загрузки системы;  - Наличие функции создания точек восстановления системы.  - Наличие встроенной функции шифрования файлов;  - Наличие встроенной функции предоставления удаленного управления системой;  - Наличие встроенной функции защиты от вредоносного программного обеспечения;  - Возможность автоматического переключения принтера в зависимости от сетевого расположения;  - Возможность работы в качестве терминального сервера и сервера приложений;  - Возможность использования виртуализации штатными средствами с поддержкой x64-операционных гостевых систем. Лицензия должна обеспечивать возможность бесплатного запуска двух серверных гостевых ОС в рамках двухсокетного сервера;  - Возможность включения и отключения графического интерфейса операционной системы в рамках одного рестарта ОС;  - Возможность агрегации сетевых интерфейсов штатными средствами для повышения отказоустойчивости и производительности;  - Возможность объединения дисков в единый пул для оптимизации дисковой подсистемы;  - Возможность выступать в качестве Контроллера Домена ActiveDirectory;  - Возможность изменения версии на более раннюю (Даунгрэйда). | 3 |
| 9 | Лицензия должна предоставлять право подключения к любому количеству серверов с одного устройства любому количеству пользователей. | 60 |

**8. Требование к серверному оборудованию, дисковой полке для системы хранения данных и программному обеспечению среды виртуализации**

1) ПОсредывиртуализации - VMware vSphere 6 Standard for 1 processor\* - 4 штуки;

2) Сертификатподдержки Basic Support/Subscription VMware vSphere 6 Standard for 1 processor for 1 year\* - 4 штуки;

3) Сервер виртуализации - 2 штуки, удовлетворяющий следующим требованиям:

|  |  |
| --- | --- |
| Типоразмер | Не более 1U |
| Блок питания | Не менее двух от 400 до 550 Ватт каждый. С возможностью «горячей» замены и резервированием.  Эффективность не менее 94% при полной нагрузке. |
| Цвет передней панели корпуса | Черный |
| Глубина сервера | Не более 610 мм |
| Встроенные вентиляторы | Не менее 6 с возможностью горячей замены |
| Число отсеков 3,5" с возможностью горячей замены | Не менее 4 для SAS/SATA HDD |
| Число экспандеров SAS3 12Гб/с | Не менее 1 шт |
| Комплект для монтажа в 19" стойку | Наличие |
| Количество ядер процессора | Не менее 20 ядер или 10 ядер и 20 потоков |
| Максимальная тактовая частота | Не менее 2.2 ГГц |
| Кэш процессора | Не менее 25 МБ |
| Технология виртуализации | Наличие |
| Поддержка 64-разрядных приложений | Наличие |
| Технология защиты системы от программных ошибок | Наличие |
| Новые команды AES | Наличие |
| Встроенный контроллер памяти | Наличие |
| Макс. пропускная способность памяти | Не менее 68Гб/с |
| Поддержка памяти ECC | Наличие |
| Кол-во каналов памяти на каждый процессор | Не менее 4 |
| Количество установленных процессоров | Не менее 2 |
| Максимальное количество процессоров | Не менее 2 |
| Кол-во слотов под оперативную память | Не менее 12 |
| Тип оперативной памяти | DDR4 с функцией коррекции ошибок |
| Объем установленной оперативной памяти | Не менее 32 ГБ |
| Тактовая частота оперативной памяти | Не менее 2400 МГц |
| Обнаружение ошибок | Исправление однобитных ошибок  Обнаружение двухбитных ошибок |
| Количество разъемов PCI Express | Не менее 2 слотов PCI-E 3.0 x16 |
| Привод DVD-RW | Наличие |
| Raid-контроллер | Наличие |
| Ключевые характеристики Raid-контроллера | Не менее 1 ГБ кэш-памяти с защитой на базе флэш-памяти  RAID уровнй 0, 1, 5, 6, 10, 50 и 60  Поддерживает до 255 дисков SATA или SAS при использовании SAS-экспандеров  Hybrid RAID 1 и 10  Быстрая инициализация  OnlineCapacityExpansion (увеличение емкости RAID-массива без выключения сервера)  HotSpare (автоматическое копирование данных с диска "горячего" резерва обратно на новый диск, установленный вместо отказавшего)  Алгоритм динамического кэширования  NativeCommandQueuing (NCQ)  Фоновая инициализация  Поддержка "горячего подключения" дисков  RAID Level Migration (миграцияуровней RAID)  Различные типы дисков "горячего" резерва – глобальный, выделенный, объединенные в пул  Автоматическое и ручное восстановление "горячего" резерва  Управление дисковой системoи хранения с помощью SES и SAF-TE  Конфигурирование размера полосы  Поддержка S.M.A.R.T.  Многие и разные типы RAID-массивов на дисках  Таблица дефектных полос  Динамическое восстановление дефектных секторов диска  Поддержка StaggeredDriveSpin-Up (постепенная раскрутка дисков)  Поддержка загрузочного массива  Поддержка накопителей на ленте, автозагрузчиков  Поддержка безопасной загрузки для BIOS uEFI  Cовместимость с VMwarevSphereESXi 6.0 |
| Управление | Аппаратная реализация удаленного управления сервером, обеспечивающая следующие функции:   • Поддержка IPMI over LAN  • Поддержка Serial over LAN  • Поддержка KVM over LAN  • Поддержка Virtual Media over LAN  • Поддержка LAN Alerting-SNMP Trap  • Поддержка журнала событий  • Независимость от ОС (Операционная система)  • Обеспечение удаленного аппаратного мониторинга через IPMI.  Включая следующее:  - Состояние датчиков температуры (процессор, системная плата)  - Состояние датчиков скорости вращения вентиляторов корпуса сервера  - Состояние датчиков напряжения (материнская плата, модули управления питанием процессора)  - Определение ошибок памяти ECC  - Состояние питания (блоки питания)  - Состояние датчика вскрытия корпуса  - Удаленное управление питанием: включение питания, выключение питания или перезагрузка системы  - Удаленный доступ к текстовой или графической системной информации, включая настройку BIOS и информацию о работе ОС (KVM)  - Удаленное управление программными приложениями   • Обеспечение безопасное сетевое управление через удаленное управление/перенаправление консоли   Наличие выделенного сетевого порта для управления, не менее 100 Мбит/с. Наличие всего необходимого программного обеспечения, рекомендуемого производителем платформы. |
| Сетевой контроллер Тип 1 | Не менее 1 Гбит/с на порт |
| Сетевой контроллер Тип 2 | Не менее четырех портов должны работать в соответствии с стандартами: IEEE 802.3ae, IEEE 802.1q (VLAN), IEEE 802.3ad, IEEE 802.3x, IEEE 802.3an, IEEE 802.3ab 1000BASE-T. |
| Сетевой контроллер Тип 3 | Не менее двух портов SFP+ 10GbE |
| Сетевой контроллер Тип 4 | Не менее двух портов с FC-интерфейсом, не менее 8 Гбит/с |
| Порты на задней панели | Не менее 4x USB 2.0, не менее 1x COM, не менее 3x RJ-45, не менее 2x VGA порта |
| Дисковый массив | Не менее 3 жестких дисков. Не менее 300 ГБ каждый.  Предназначен для построения рейд-массивов и использования в серверных платформах.  Возможность работы в режиме 24x7 (24 часа, 7 дней в неделю)  Скорость вращения шпинделя - не менее 10000 оборотов/мин. |
| Комплект пачкордов | 1. Патчкорд (цвет красный) RJ-45 для DMZ зоны длина 20 метров.  2. Патчкорд для 10 Гбит карт SFP+ – 4 штуки, длина 3 метра.  3. Пачкорд оптический – LC-LC дуплекс – OM3 многомод – 4 штуки, длина 3 метра.  4. Пачкорд RJ-45 (цвет синий) – 2 штуки, длина 3 метра.  5. Пачкорд оптический – LC-LC дуплекс – OM4 многомод – 16 штук, длина 20 метров. |
| Общие требования к серверному оборудованию: | |
| Оборудование должно быть новым, не восстановленным, не допускается поставка выставочных образцов. Оборудование должно быть поставлено комплектно и обеспечивать конструктивную и функциональную совместимость. | |
| Поставляемое оборудование должно соответствовать действующим стандартам и нормам по пожарной, санитарной и электрической безопасности, а также электромагнитной совместимости, в соответствии с номенклатурой продукции, в отношении которой законодательными актами Российской Федерации предусмотрена обязательная сертификация с документальным подтверждением. Наличие у поставляемого оборудования действующих сертификатов соответствия требованиям: ТР ТС 004/2011 «О безопасности низковольтного оборудования»; ТР ТС 020/2011 «Электромагнитная совместимость технических средств». | |
| Гарантия на поставляемое серверное оборудование не менее 36 месяцев. | |

4) Дисковая полка для системы хранения данных EMC VNX5500 6GSDAE15 в комплекте с 15 дисками 2TB NL SAS 3.5IN\*\* - 1 штука.

\* В соответствии с пунктом 1 статьи №33 Федерального закона от 05.04.2013 N 44-ФЗ (ред. от 03.07.2016) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения взаимодействия с программным обеспечением, используемым заказчиком, эквивалент на указанное оборудование не предусмотрен.

\*\* В соответствии с пунктом 1 статьи №33 Федерального закона от 05.04.2013 N 44-ФЗ (ред. от 03.07.2016) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения взаимодействия с СХД EMC S/N CKM00134200229, используемым заказчиком, эквивалент на указанное оборудование не предусмотрен.

**9. Установка и настройка СЗИ**

9.1. Установка и настройка СЗИ должна производиться Исполнителем в соответствии с эксплуатационной документацией, разработанным техническим проектом и должны реализовывать все определенные в техническом проекте и техническом задании меры по обеспечению безопасности информации.

9.2. Установка и настройка средств криптографической защиты должна осуществляться Исполнителем на основании действующей лицензии ФСБ России на 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 (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).

9.3. Работы по установке, настройке СЗИ должны осуществляться Исполнителем на основании действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

**10. Аттестация информационной системы**

10.1. При аттестации информационных систем Исполнитель проводит комплексную проверку объектов информатизации для оценки соответствия требованиям по защите информации от несанкционированного доступа.

10.2. Аттестационные испытания проводятся исполнителем на объекте информатизации по адресу нахождения заказчика.

10.3. Комплекты аттестационных документов предоставляются Конечному пользователю по результатам проведения аттестационных испытаний и включают следующие документы:

- программа и методики проведения аттестационных испытаний;

**–** протоколы испытаний системы защиты от НСД;

**–** заключение по результатам аттестационных испытаний;

**–** аттестаты соответствия требованиям информационной безопасности.

**11. Гарантийные обязательства и техническая поддержка СЗИ**

11.1. После завершения работ Исполнителем должно быть обеспечено гарантийное обслуживание работ в течение 12 месяцев с момента подписания Акта сдачи-приемки выполненных работ.

Гарантийное обслуживание работ должно осуществляться без дополнительной оплаты.

11.2. Исполнитель на постоянной основе должен обеспечивать Конечному пользователю техническую поддержку, консультирование (по телефону «горячей линии», электронной почте, иными способами) по всем вопросам работы с СЗИ, в течение 12 месяцев с момента подписания Акта сдачи-приемки выполненных работ.

11.3. Время прибытия сотрудника на площадку заказчика при возникновении критичных проблем в работе системы защиты информации не должно превышать 3-х часов.

Техническая поддержка и консультирование должны осуществляться без дополнительной оплаты.

**12. Требования к обучению администраторов, пользователей**

12.1. После проведения всех работ, предусмотренных настоящим техническим заданием, Исполнитель должен провести базовое обучение работников Заказчика (администраторов по безопасности и пользователей).

12.2. Список обучаемых сотрудников Исполнитель предварительно согласовывает с Заказчиком

**Приложение №2**

**к документации об аукционе**

**проект**

**Договор №\_\_\_\_**

**на поставку серверного оборудования с установкой и настройкой**

г. Улан-Удэ «\_\_\_\_» \_\_\_\_\_\_\_\_\_2016 г.

Государственное автономное учреждение культуры Республики Бурятия «Государственный архив Республики Бурятия», именуемое в дальнейшем «Заказчик», в лице директора Жалсановой Бутит Цыдыпмункуевны, действующей на основании Устава с одной стороны, и\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем "Исполнитель", в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые в дальнейшем "Стороны", в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и Положением о закупке товаров, работ, услуг ГАУК РБ «ГАРБ», утвержденного наблюдательным советом от 26 января 2016 года, заключили настоящий договор (далее - Договор) о нижеследующем:

**1.Предмет Договора**

1.1. Исполнитель принимает на себя обязательства по поставке серверного оборудования, дисковой полки для системы хранения данных, программного обеспечения, средств защиты информации и выполнение работ по установке, настройке оборудования, созданию системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия»в соответствии с Техническим заданием (Приложение№1 к договору №\_\_от \_\_\_\_), являющемся неотъемлемой частью договора.

1.2. Заказчик обязуется обеспечить приёмку и оплату поставленного товара.

**2. Цена Договора и порядок расчетов**

2.1. Цена Договора устанавливается в сумме \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Стоимость поставляемого товара указана с учетом всех расходов поставщика, в том числе доставки, упаковки, хранения, погрузочно-разгрузочных работ, страхования, уплаты всех налогов, сборов и других обязательных платежей.

2.2. Цена Договора является твёрдой, индексации не подлежит и определяется на весь срок исполнения Договора.

2.3. Оплата производится по факту поставки товара в течение 15 банковских дней с момента предоставления Заказчику счета и счета-фактуры, товарной накладной и Акта выполненных работ, а в случае начисления Исполнителю неустойки (штрафа, пени), Заказчик оставляет за собой право произвести оплату по настоящему Договору после перечисления суммы неустойки на расчетный счет Заказчика.

2.4. Оплата осуществляется путем перечисления денежных средств на расчетный счет Поставщика.

2.5. Цена Договора может быть снижена по соглашению сторон без изменения предусмотренных настоящим Договором количества товаров и иных условий исполнения настоящего Договора.

**3. Порядок поставки и приемки товара**

3.1.Товар поставляется Исполнителем Заказчику до 15 апреля 2017 г. с даты заключения настоящего Договора по адресу: 670001, г. Улан-Удэ, ул. Ленина, 54.

3.1.2. Поставка товара включает в себя доставку товара, погрузочно-разгрузочные работы, установку, настройку программного обеспечения. Поставка товара осуществляется силами и средствами Исполнителя по рабочим дням с 09ºº час. до 17ºº час. по местному времени.

Товар поставляется по предварительному согласованию с Заказчиком даты и времени поставки.

3.2. Исполнитель несет обязанность по доставке Товара собственным транспортом либо организует доставку Товара транспортом иной организации на свое усмотрение и за свой счет. Риск утраты или порчи Товара в процессе его доставки несет Исполнитель.

3.2.1. Товар должен отгружаться в стандартной упаковке с учетом необходимых маркировок в соответствии с требованиями стандартов и технических условий. Поставка Товара должна быть осуществлена Исполнителем в полном объеме, в соответствии с условиями договора.

3.3. Приемка товара осуществляется Заказчиком в день поставки товара.

3.4. При приемке Товара, он должен быть осмотрен Заказчиком. Оформление результатов приемки Товара осуществляется двусторонним актом приема-передачи товара, подписанным в течении 3 (трех) рабочих дней с момента поставки Товара представителями Исполнителя и Заказчика, который подтверждает приемку Товара. В случае обнаружения несоответствия поставленного Товара условиям Договора, техническому заданию, а также сведениям, указанным в транспортных и сопроводительных документах об этом Заказчик уведомляет Исполнителя в течение 3 (трех) рабочих дней.

3.5. Если товар не будет соответствовать установленным требованиям (условиям Договора и/или техническому заданию, сведениям, указанным в транспортных и сопроводительных документах), Заказчик может отказаться от него и Исполнитель должен будет заменить Товар или допоставить (доукомплектовать) товар без каких-либо дополнительных затрат со стороны Заказчика. Срок замены товара ненадлежащего качества или допоставки (доукомплектования) устанавливается в течение 3 (трех) рабочих дней с момента предъявления соответствующей претензии (уведомления).

3.6. Одновременно с передачей товара Исполнитель обязан передать Заказчику сопроводительные документы на товар, сертификаты соответствия.

3.7. Право собственности на Товар переходит от Исполнителя Заказчику в момент передачи Товара, подписания товарно-транспортных накладных, счетов-фактур, счетов, Акта приема-передачи.

3.8. Момент перехода риска, случайной гибели или случайного повреждения Товара переходит от Исполнителя Заказчику одновременно с переходом права собственности на Товар.

3.9. При нарушении Исполнителем сроков поставки Товара сроки оплаты за Товар переносятся соразмерно нарушенным срокам поставки товара согласно условиям п. 3.1.

**4.Обязанности Сторон**

* 1. **Заказчик**:
     1. Обязан осуществить приемку Товара, надлежащего качества, в соответствии с условиями Договора.
     2. Обязан оплатить принятый Товар в соответствии с условиями Договора.
     3. Вправе требовать надлежащего выполнения Исполнителем обязательств в соответствии с Договором.
     4. Вправе осуществлять контроль за порядком и сроками поставки Товара, не вмешиваясь в оперативно-хозяйственную деятельность Исполнителя.
     5. Вправе отказаться от принятия и оплаты товара, несоответствующего условиям Договора.
     6. Вправе требовать от Исполнителя представления надлежащим образом оформленных документов, подтверждающих исполнение обязательств по Договору в соответствии с условиями Договора.
  2. Исполнитель:
     1. Обязан поставить Заказчику качественный товар в соответствии с условиями Договора, в ассортименте, в сроки и по адресу, определенному Договором.
     2. При поставке товара обязан осуществить доставку товара по адресу, определенному Договором, погрузочно-разгрузочные работы, включающие в себя выгрузку из транспортного средства и размещение (складирование) в месте (помещении), указанном Заказчиком, сборку его и установку товара в указанное Заказчиком место (помещение) в случае поставки товара в разобранном виде.
     3. При поставке товара Исполнитель обязан передать Заказчику относящиеся к товару принадлежности и (или) документы, которые он должен передать в соответствии с действующим законодательством или условиями Договора.
     4. Обязан осуществить сдачу-приемку товара в порядке, определенном Договором.
     5. Не позднее, чем за 3 (три) часа до предполагаемого времени поставки товара, согласовать с Заказчиком по телефону дату и время доставки товара.
     6. Обязан поставить недопоставленный товар в течение 3 рабочих дней с момента уведомления Заказчиком о недопоставке (в т.ч. нарушении комплектации).
     7. Обязан за свой счет и своими силами заменить товар ненадлежащего качества на товар надлежащего качества в течение 3 рабочих дней с момента уведомления заказчиком.

1. **Ответственность Сторон**

5.1. За неисполнение, либо ненадлежащее исполнение обязательств по настоящему договору Стороны несут ответственность, предусмотренную законодательством Российской Федерации и настоящим договором РФ.

5.2.В случае просрочки исполнения Заказчиком обязательств, предусмотренных договором, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных договором, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного договором, начиная со дня, следующего после дня истечения установленного договором срока исполнения обязательства. Такая пеня установлена в размере 1/300, действующей на дату уплаты пеней, ставки рефинансирования Центрального банка Российской Федерации от не уплаченной в срок суммы. Штрафы начисляются за ненадлежащее исполнение Заказчиком обязательств, предусмотренных договором, за исключением просрочки исполнения обязательств, предусмотренных договором. Штраф устанавливается в размере 2,5 % цены договора и составляет\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей.

5.3. В случае просрочки исполнения Исполнителем обязательств (в том числе гарантийных обязательств), предусмотренных договором, а также в иных случаях не исполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных договором, Заказчик направляет Исполнителю требование об уплате неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного договором, начиная со дня, следующего после дня истечения установленного договором срока исполнения обязательства. Такая пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного договором, и устанавливается в размере не менее 1/300 действующей на дату уплаты пени [ставки](consultantplus://offline/ref=CA5DF5E0A05B3B3A324B0E9C7125629323DA7268F74104E1336B3A12f2jBA) рефинансирования Центрального банка Российской Федерации от цены договора, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных договором и фактически исполненных Исполнителем. (Постановление Правительства РФ от 25.11.2013 N 1063 "Об утверждении Правил определения размера штрафа, начисляемого в случае ненадлежащего исполнения заказчиком, поставщиком (подрядчиком, исполнителем) обязательств, предусмотренных договором (за исключением просрочки исполнения обязательств заказчиком, поставщиком (подрядчиком, исполнителем), и размера пени, начисляемой за каждый день просрочки исполнения поставщиком (подрядчиком, исполнителем) обязательства, предусмотренного договором"). Штрафы начисляются за ненадлежащее исполнение Исполнителем обязательств, предусмотренных договором, за исключением просрочки исполнения Исполнителем обязательств, предусмотренных договором. Штраф устанавливается в размере 10 % цены договора и составляет\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей.

5.4. Сторона освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного договором, произошло вследствие непреодолимой силы или по вине другой стороны.

**6. Требования к гарантийному сроку и объему предоставления**

**гарантий качества товара**

6.1. Исполнитель осуществляет обслуживание товара в течение всего гарантийного срока. Исполнитель гарантирует качество товара в соответствии с действующими нормами и техническими условиями, своевременное устранение недостатков, обнаруженных в пределах гарантийного срока. Наличие гарантии качества удостоверяется выдачей гарантийного талона (паспорта, сертификата и т.п.). Срок гарантии качества на поставляемый по договору товар составляет 12 месяцев с даты подписания акта ввода Товара в эксплуатацию. Гарантии включают в себя исправление любых недостатков товара, которые не вызваны неправильной эксплуатацией товара. В период гарантийного срока Исполнитель обязуется производить необходимый ремонт, устранение недостатков, в соответствии с требованиями действующего законодательства. В случае невозможности произвести ремонт в указанный срок, заказчику представляется функционально аналогичный товар на время ремонта. Наличие недостатков, сроки их устранения или замены фиксируются Сторонами в двухстороннем акте выявленных недостатков.

6.2. Исполнитель в течение гарантийного срока обязан за свой счет устранить недостатки и / или произвести необходимый ремонт. Все работы и сопутствующие товары по обслуживанию товара, не включенные в объем предоставления гарантии качества товара, оплачиваются Заказчиком.

6.3. Срок предоставления гарантии в полном объеме составляет 12 месяцев, но не менее срока, установленного производителем, с момента подписания акта ввода Товара в эксплуатацию, при этом предоставление такой гарантии осуществляется вместе с товаром.

Способ обеспечения гарантии определяется Исполнителем самостоятельно.

**7.Обеспечение исполнения договора**

7.1. По настоящему договору предусмотрено обеспечение его исполнения в размере 10% от первоначальной (максимальной) цены лота и составляет \_\_\_\_ (\_\_\_\_) рублей 00 копеек.

7.2. Исполнение Договора может быть обеспечено: залогом денежных средств, безотзывной банковской гарантией.

Способ обеспечения исполнения договора **определяется Исполнителем самостоятельно.**

7.3. Порядок предоставления обеспечения исполнения договора - документы, подтверждающие обеспечения исполнения договора, направляются оператору электронной площадки, на которой проводились торги.

В случае если обеспечение исполнения договора предоставляется в виде залога денежных средств, сумма обеспечения должна быть перечислена по следующим банковским реквизитам:

УФК Республики Бурятия (ГАУК РБ «Государственный архив Республики Бурятия» л/с 30026Э43680)

БанкОТДЕЛЕНИЕ-НБ РЕСПУБЛИКА БУРЯТИЯ Г.УЛАН-УДЭ

Р/с: 40601810000001000001

БИК 048142001;

ИНН 0326473404;

КПП 032601001

7.4. Обеспечение исполнения Договора возвращается Исполнителю путем перечисления денежных средств на расчетный счет, указанный Исполнителем, либо в виде возврата оригинала банковской гарантии в течение пятнадцати рабочих дней со дня выполнения Исполнителем всех обязательств по Договору.

7.5. Датой возврата обеспечения считается дата представления платежных документов Заказчиком в обслуживающее финансово-кредитное учреждение (дата почтового отправления).

7.6. Срок предоставления обеспечения исполнения договора – до исполнения Исполнителем своих обязательств по договору.

7.7. В случае если по каким-либо причинам обеспечение исполнения договора стало недействительным или стало ненадлежащим, Исполнитель обязуется в течение 10 (десяти) банковских дней предоставить заказчику иное надлежащее обеспечение исполнения договора.

Обеспечение исполнения договора возвращается в течение пяти рабочих дней со дня окончания срока его предоставления.

Обеспечение исполнения договора Заказчиком не возвращается в случае неисполнения поставщиком (подрядчиком, исполнителем) обязательств по договору.

**8. Действие обстоятельств непреодолимой силы**

8.1.Ни одна из сторон не несет ответственности перед другой Стороной за неисполнение обяза­тельств по настоящему договору, обусловленное действием обстоятельств непреодолимой силы, т.е. чрезвычайных и непредотвратимых при данных условиях обстоятельств, в том числе пожары, землетрясения, наводнения и другие природные стихийные бедствия, а также издание актов государственных органов**.**

8.2.Сторона, которая не исполняет своего обязательства вследствие действия непреодолимой си­лы, должна незамедлительно известить другую Сторону о таких обстоятельствах и об их влиянии на исполнение обязательств по договору.

**9. Порядок разрешения споров**

9.1.Все споры или разногласия, возникшие между Сторонами по настоящему договору или в связи с ним, разрешаются путем переговоров между ними.

9.2.Срок ответа на Претензию составляет 5 дней с момента получения.

9.3. В случае невозможности разрешения разногласий путем переговоров они подлежат рассмотре­нию в Арбитражном суде Республики Бурятия.

**10. Порядок изменения и расторжения договора**

10.1.Расторжение договора допускается

- по соглашению сторон

- по решению суда

- в связи с односторонним отказом стороны договора от исполнения договора в соответствии с гражданским законодательством Российской Федерации.

10.2. Допускается изменение существенных условий договора по соглашению сторон при его исполнении в следующих случаях:

а) при снижении цены договора без изменения предусмотренных договором количества товара, качества поставляемого товара, выполняемой работы, оказываемой услуги и иных условий договора;

б) если по предложению заказчика увеличиваются предусмотренные договором количество товара, не более чем на десять процентов или уменьшаются предусмотренные договором количество поставляемого товара, не более чем на десять процентов. При этом по соглашению сторон допускается изменение с учетом

положений бюджетного законодательства Российской Федерации цены договора пропорционально дополнительному количеству товара, исходя из установленной в договоре цены единицы товара, но не более

чем на десять процентов цены договора. При уменьшении предусмотренных договором количества товара, стороны договора обязаны уменьшить цену договора исходя из цены единицы товара. Цена единицы дополнительно поставляемого товара или цена единицы товара при уменьшении предусмотренного договором количества поставляемого товара должна определяться как частное от деления первоначальной цены договора на предусмотренное в договоре количество такого товара.

10.3. Заказчик обязан принять решение об одностороннем отказе от исполнения договора, если в ходе исполнения договора установлено, что Исполнитель не соответствует установленным документацией о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своем соответствии таким требованиям, что позволило ему стать победителем данного электронного аукциона.

10.4. Решение Сторон об одностороннем отказе от исполнения договора вступает в силу и Договор считается расторгнутым через 10 (десять) дней с даты надлежащего уведомления одной из сторон об одностороннем отказе от исполнения договора.

**11. Срок действия договора**

11.1.Настоящий Договор вступает в силу с момента его подписания Сторонами и действует до исполнения сторонами своих обязательств по настоящему Договору.

11.2. В случае установления нецелесообразности, либо установления неизбежности получения отрицательного результата, либо изменения законодательства, Стороны в срок, установленный Заказчиком, обязаны привести настоящий договор в полное соответствие с целесообразностью и/или изменениями в законодательстве, произошедшими после заключения настоящего договора или расторгнуть его.

**12. Особые условия**

12.1. В случае изменения у какой - либо из Сторон юридического адреса, названия, банковских реквизитов и прочего она обязана в течение 10 (десяти) дней письменно известить об этом другую Сторону.

12.2. При выполнении настоящего договора стороны руководствуются законодательством Российской Федерации.

12.3. Все указанные в договоре обязательные приложения являются его неотъемлемой частью.

**Приложение №1 к договору № « » \_\_\_\_\_\_\_\_\_2016 г.** Техническое задание по поставке серверного оборудования, дисковой полки для системы хранения данных, программного обеспечения, средств защиты информации и выполнение работ по установке, настройке оборудования, созданию системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия».

12.4**.** Настоящий договор заключен в электронной форме и подписан электронными под­писями лиц, имеющих право действовать от имени Заказчика и Исполнителя.

12.5.При согласии Исполнителя договор может быть составлен также в письменной форме на бумажном носителе в 2 (двух) экземплярах, имеющих одинаковую юридическую силу по одному для каждой из сторон.

**13. АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН**

|  |  |
| --- | --- |
| **Заказчик:** ГАУК РБ «ГАРБ» Адрес: 670000 г. Улан-Удэ, ул. Сухэ-Батора, 9а  🕾. 21-29-58, ф. 21-46-34  ИНН 0326473404 КПП 032601001  УФК по Республике Бурятия (ГАУК РБ «ГАРБ» л/с 30026Э43680)  ОТДЕЛЕНИЕ - НБ РЕСПУБЛИКА БУРЯТИЯ  Г. УЛАН-УДЭ  БИК 048142001  Р/СЧ. 40601810000001000001  Директор ГАУК РБ «ГАРБ»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Б.Ц. Жалсанова  М.П. | **Исполнитель:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/  М.П. |

**Приложение №1**

**К договору № \_\_\_\_ «\_\_» \_\_\_\_\_ 2016г.**

**Техническое задание**

**на поставку серверного оборудования, дисковой полки для системы хранения данных, программного обеспечения, средств защиты информации и выполнение работ по установке, настройке оборудования, созданию системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия»**

**Перечень сокращений**

|  |  |
| --- | --- |
| АРМ | – Автоматизированное рабочее место |
| ГИС | – Государственная Информационная Система |
| ИСПДн | – Информационная система персональных данных |
| ФСБ России | – Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | – Федеральная служба по техническому и экспортному контролю Российской Федерации |
| СЗИ | – Система защиты информации |
| ИС | – Информационная система |
| РД | – Руководящий документ |
| ТТ | – Технические требования |
| ЛВС | – Локальная вычислительная сеть |
| ПО | – Программное обеспечение |
| СУБД | – Система управления базами данных |
| БД | – База данных |
| АРМ | – Автоматизированное рабочее место |
| СЗИ | – Средство защиты информации |
| НСД | – Несанкционированный доступ |
| ОС | – Операционная система |
| НДВ | – Недекларированные возможности |

**Используемые термины**

**Организационно-распорядительная документация (ОРД) -** комплекс документов, закрепляющих функции, задачи, цели, а также права и обязанности работников и руководителей по выполнению конкретных действий, необходимость которых возникает в операционной деятельности организации.

**Объект информатизации** – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

**Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.**

**Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.**

**Заказчик**– Государственное втономное Учреждение Культуры Республики Бурятия «Государственный Архив Республики Бурятия»

**Аттестация объекта информатизации** - комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

**Работы** – проведение обследования объектов информатизации Конечного пользователя, установка и настройка средств защиты информации, разработка ОРД по защите ПДн для Конечного пользователя, аттестация объектов информатизации Конечного пользователя.

**1. Общие сведения**

**1.1. Полное наименование работ**

Поставка серверного оборудования, дисковой полки для системы хранения данных, создание системы защиты персональных данных, обрабатываемых в ГАУК РБ «Государственный архив Республики Бурятия»

**1.2. Наименование Заказчика**

Государственное автономное учреждение культуры Республики Бурятия «Государственный Архив Республики Бурятия»

**1.3. Адрес проведения работ:**

670001, Республика Бурятия, г. Улан-Удэ,, ул. Ленина, дом № 54.

**2. Основные этапы работ**

2.1. Поставка серверного оборудования;

2.2. Поставка лицензий на системное программное обеспечение (не ниже WindowsServer 2012) и программное обеспечение для среды виртуализации (VMware);

2.3. Проектирование системы защиты информации;

2.4. Поставка средств защиты информации;

2.5. Установка и настройка средств защиты информации;

2.6. Проведение аттестации ИС по требованиям безопасности.

**3. Цели создания СЗИ**

3.1. Целями создания СЗИ являются:

- обеспечение защищенности ИС в процессе обработки и хранения информации, обеспечение конфиденциальности информации при ее обработке, а также других необходимых свойств информации (целостности, доступности и т.д.);

- соответствие требованиям обеспечения информационной безопасности при обработке ПДн в ИС, установленных РД ФСТЭК России и ФСБ России.

**4. Результаты создания СЗИ**

4.1. В результате создания СЗИ должно быть обеспечено выполнение требований по защите конфиденциальной информации, содержащейся в государственных информационных системах Конечного пользователя, а также требования по обеспечению безопасности ПДн при их обработке в ИС Конечного пользователя.

4.2. Критериями оценки достижения поставленных целей по созданию СЗИ являются:

– соответствие требованиям по защите информации, установленным приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», - соответствие требованиям по защите информации;

соответствие требованиям по защите персональных данных, установленным приказом 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»;

- соответствие иным требованиям по защите информации, установленным РД ФСТЭК России и ФСБ России;

– выполнение всех требований настоящих Требований;

4.3. Подтверждением соответствия результатов работ в рамках настоящих Требований является аттестация ИС на соответствие требованиям безопасности информации.

**5. Обязательные требования к СЗИ**

5.1. Создаваемая СЗИ должна обеспечивать выполнение всех требований, установленных нормативными правовыми актами, руководящими документами, указанными в пункте 8.2. настоящих Требований.

5.2. Создаваемая СЗИ должна обеспечивать возможность:

– работы в сети «Интернет» (электронной почты) на каждом АРМ;

– поступления и обработки запросов, поступающих из Федеральных органов исполнительной власти, органов государственных внебюджетных фондов Российской Федерации в рамках межведомственного электронного взаимодействия;

– осуществления безопасной передачи сведений в электронной форме по каналу связи (в том числе сети «Интернет») с электронной подписью и шифрованием;

– возможность поэтапного подключения образовательных учреждений в защищенную сеть (масштабируемость);

– организации взаимодействия с организациями-участниками.

5.3. Состав программного обеспечения

* Microsoft Windows Server 2008/2012 Standard R2 насерверахИС.
* MicrosoftWindows 7/8/8.1 Prof на рабочих местах.

**6. Состав работ по проектированию системы защиты**

**6.1. Работы по проектированию СЗИ должны включать в себя:**

– предпроектное обследование;

– разработка технического задания;

– разработка организационно-распорядительной документации.

Во время проведения предпроектного обследования должны быть проведены следующие работы:

– определен состав обрабатываемых ПДн в ИС;

– определена граница контролируемой зоны;

– определено используемое в ИС программное обеспечение;

– определены используемые в ИС информационные технологии.

– определены состав и тип применяемых в ИС средств защиты информации;

– определены технологические процессы обработки ПДн в ИС;

– определены внешние и внутренние информационные потоки;

– определен необходимый класс защищенности ИС;

– определен необходимый уровень защищенности ПДн;

– определен состав, содержание и сроки проведения мероприятий по этапам модернизации СЗИ.

**6.2. Техническое задание**

Разрабатываемое Исполнителем Техническое задание должно соответствовать требованиям следующих нормативных правовых актов (в редакциях с изменениями, вступившими в силу на момент проведения работ):

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

– постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»;

– ГОСТ 19.201-78 ЕСПД. Техническое задание. Требования к содержанию и оформлению;

– руководящего документа РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;

– приказа ФСБ России от 10.07.2014 № 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»;

– приказа ФАПСИ от 13.06.2001 № 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»;

– приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– нормативно-методического документа «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного приказом заместителя директора ФСТЭК от 15.02.2008;

– нормативно-методического документа «Базовая модель угроз безопасности персональных данных в информационных системах персональных данных», утвержденного приказом заместителя директора ФСТЭК от 15.02.2008;

– руководящего документа «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282;

– иных нормативных правовых актов, руководящих документов, устанавливающих требования по защите ПДн, обрабатываемых в ИС.

Техническое задание должно включать:

– исходные данные, описывающие существующие у Конечного пользователя ИСПДн, их характеристики и количество обрабатываемых ПДн;

– перечень применяемых Конечным пользователем программных средств и информационных технологий;

– перечень технических средств, их размещение относительно контролируемой зоны;

– информационные потоки ПДн;

– описание технологических процессов обработки данных по каждой ИСПДн;

– определение требуемых классов защищенности;

– общие требования, предъявляемые к СЗИ;

– перечень необходимых мер защиты, которые должна реализовывать СЗИ;

– перечень предполагаемых к использованию средств защиты информации.

Техническое задание должно быть согласовано с Заказчиком.

**6.3. Организационная распорядительная документация**

Исполнителем должны быть разработаны и предоставлены на согласование Конечному пользователю проекты организационных распорядительных документов по обеспечению безопасности персональных данных в ИС.

Организационные меры при проектировании СЗИ должны включать в себя разработку следующих ОРД:

**6.3.1. Базовые документы, на основе и в соответствии с которыми разрабатывается система защиты информации:**

1. Концепция информационной безопасности;
2. Политика информационной безопасности;
3. Частная модель угроз безопасности ПДн при их обработке в ИС;
4. Модель нарушителя;
5. Описание технологического процесса;
6. Техническое задание;
7. Матрица разграничения доступа;

**6.3.2. Приказы:**

1. Приказ о назначении лиц, ответственных за обработку ПДн в ИС;
2. Приказ о назначении лиц, имеющих доступ к ПДн;
3. Приказ о назначении комиссии по классификации ИС;
4. Приказ об утверждении мест хранения материальных носителей ПДн;

**6.3.3. Положения:**

1. Положение об обработке ПДн субъектов ПДн;
2. Положение о защите ПДн в ИС;
3. Положение о подразделении по защите ПДн в ИС;
4. Положение о режиме безопасности в помещениях;
5. Положение об обработке ПДн без использования средств автоматизации;

**6.3.4. Планы:**

1. План мероприятий по защите ПДн;
2. Порядок проведения внутренних проверок защиты ПДн;

**6.3.5. Журналы:**

1. Журнал учета съемных носителей;
2. Журнал учета применяемых СЗИ, эксплуатационной и технической документации к ним;
3. Журнал по учету мероприятий по контролю обеспечения защиты ПДн в ИС;
4. Журнал учета обращений субъектов персональных данных о выполнении их законных прав, при обработке ПДн в ИС;
5. Журнал обращений пользователей информационной системы к ПДн;
6. Журнал поэкземплярного учета СКЗИ;
7. Журнал учета хранилищ;
8. Технический (аппаратный) журнал;

**6.3.6. Инструкции:**

1. Инструкция администратора информационной безопасности ИС;
2. Инструкция пользователя ИС;
3. Инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций;
4. Правила рассмотрения запросов субъектов ПДн;

**6.3.7. Перечни:**

1. Перечень защищаемых ресурсов;

**6.3.8. Акты:**

1. Акт классификации ИС;
2. Акт уничтожения документов, содержащих ПДн субъектов.

**7. Поставка средств защиты информации**

7.1. В рамках поставки по настоящим Требованиям должны быть поставлены необходимые средства защиты информации, прошедшие в установлено порядке сертификационные испытания в соответствии с действующим законодательством Российской Федерации.

7.2. Исполнитель должен поставить средства защиты информации, соответствующие требованиям (характеристикам), указанным в Таблице 2 настоящих Требований.

Таблица 1. Требования к СЗИ

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Наименование СЗИ** | **Количество** |
| 1 | СЗИ от НСД должна представлять собой программный комплекс средств защиты информации в операционных системах (ОС) семейства Windows с возможностью подключения аппаратных идентификаторов.  СЗИ от НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением ОС Windows XP, WindowsServer  2003, WindowsVista, WindowsServer 2008, Windows 7, WindowsServer 2008 R2, Windows 8, WindowsServer 2012 в многопользовательском режиме их эксплуатации.  СЗИ от НСД должна поддерживать 32- и 64-битные версии ОС.  Система должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию WindowsToGo.  СЗИ от НСД должны быть сертифицированы по требованиям РД ФСБ России, ФСТЭК России, Гостехкомиссии России по 3 классу защиты от НСД для СВТ и 2 уровню контроля отсутствия НДВ, разрабатываться и производиться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере.  Сертификат соответствия должен позволять использовать СЗИ от НСД для защиты:  - конфиденциальной информации и государственной тайны в автоматизированных системах до класса защищенности 1Б включительно;  - в государственных информационных системах 1 класса защищенности;  - для обеспечения 1 уровня защищенности персональных данных.  СЗИ от НСД должна обеспечивать:  - регистрацию различных пользователей: локальных, доменных, сетевых.  - определение количества одновременных сеансов для пользователя;  - идентификацию и проверку подлинности пользователей при входе в ОС, а также аутентификацию при входе на ПЭВМ до начала загрузки ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор;  - реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;  - должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;  - для предотвращения утечки информации с использованием сменных накопителей СЗИ от НСД должна позволять разграничивать доступ как к отдельным типам накопителей, так и к конкретным экземплярам;  - в соответствии с требованиями к СЗИ от НСД должны использоваться два принципа контроля доступа: мандатный и дискреционный;  - возможность ограничивать средствами СЗИ от НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);  - регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение компьютера, вход/выход пользователей, доступ к ресурсам, печать документов с возможностью добавления штампов и сохранение теневых копий распечатываемых документов, запуск/остановка процессов, администрирование).  - должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей.  - возможность организации замкнутой программной среды и различные способы ее настройки;  - возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);  - возможность контроля целостности программно-аппаратной среды при загрузке ПЭВМ по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при  выявлении изменений;  - очистку остаточной информации (освобождаемого дискового пространства, зачистку определённых файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Запрет смены пользователей без перезагрузки;  - возможность самодиагностики основного функционала СЗИ от НСД с формированием отчета;  - возможность добавления штампа на распечатываемые документы (произвольного или по ГОСТ). | 3 |
| 2 | * Двухфакторную аутентификацию пользователя в системе, должен выполнять аппаратный ключ со следующими техническими требованиями: * Интерфейс: USB 1.1 и выше; * Объем доступной EEPROM память не менее: 60 Кбайт; * Габаритные размеры (не более): 60х20х10 мм; * Наличие 32-битового уникального серийного номера; * Поддержка стандартов: ISO/IEC 7816, PC/SC, ГОСТ 28147-89, MicrosoftCrypto API и MicrosoftSmartcard API, PKCS#15 (v. 2.10+); * Аппаратная реализация ГОСТ 28147-89; * Защищенное хранение ключей шифрования; * Встроенная файловая система по стандарту ISO/IEC 7816; * Прозрачное шифрование файловой системы по ГОСТ 28147-89; * Двухфакторная аутентификация с использованием PIN кода и носителя; * Ограничение числа попыток ввода PIN-кода; * 3 уровня доступа к токену: Гость, Пользователь, Администратор; * Потребляемая мощность до 120 mW; * Диапазон рабочих температур/ температур хранения От 0 до +70 o C / От –10 до +80 o C; * Допустимая относительная влажность от 0 до 100 % (без конденсата); * Наличие автоматической блокировки PIN после 15 неверных попыток ввода; * Количество циклов записи в память /чтения из памяти не менее 1,000,000 / не ограничено; * Гарантированное количество подключений к USB порту не менее 5,000; * Поддержка стандарта X.509. * Реализация функционала должна быть максимально безопасной необходимые алгоритмы должны изначально присутствовать в микропрограмме, а не добавляться дополнительными загружаемыми модулями (аплетами, плагинами и т.п.); * Наличие энергонезависимой памяти не менее  64 Кб.  Требование по наличию сертификата ФСТЭК России Средство защиты должно соответствовать классам не ниже: 4 уровня контроля отсутствия НДВ и возможность применения в ИСПДн до 1 класса включительно. | 2 |
| 3 | Средство для обеспечения защиты виртуальной инфраструктуры должно представлять программный комплекс со следующими характеристиками:  ***Требования к поддержке платформ виртуализации:***   * VMware vSphere 4.1 Update 3 (VMware ESXi Server 4.1) * VMware vSphere 5 (VMware ESXi Server 5.0 Update 3) * VMware vSphere 5.1 (VMware ESXi Server 5.1 Update 2) * VMware vSphere 5.5 (VMware ESXi Server 5.5 Update 1) * VMware vSphere 6.0 (VMware ESXi Server 6.0) * VMware View 4.5 * VMware View 5 * VMware View 5.1 * VMware Horizon View 5.2   ***Должно осуществлять:***   * Аутентификацию администраторов виртуальной инфраструктуры и администраторов безопасности; * Защиту средств управления виртуальной инфраструктурой от НСД; * Защиту ESX-хостов от НСД; * Контроль целостности конфигурации виртуальных машин и их доверенную загрузку; * Мандатный принцип контроля доступа; * Регистрацию событий, связанных с информационной безопасностью; * Контроль целостности и защиту от НСД компонентов СЗИ; * Централизованное управление и мониторинг; * Возможность построения отчетов.   ***Требования к функциональности:***  - **Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности**  В ПО должна быть реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью (для ограничения на использование привилегий суперпользователя). Должна быть возможность выделить 2 основные роли — администратор виртуальной инфраструктуры и администратор безопасности. Должна быть поддержка аппаратных идентификаторов eToken и iButton.  *Реализация принципа разделения ролей*  Доступ на управление виртуальной инфраструктурой или параметрами безопасности должен предоставляться только для аутентифицированных пользователей. Для этого в СЗИ должна быть предусмотрена процедура аутентификации пользователей и компьютеров (рабочих мест администраторов), которая должна осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа ManintheMiddle.  Процедура аутентификации должна осуществляется с помощью отдельной программы, которую требуется запустить и ввести учетные данные до того, как осуществляется соединение с виртуальной инфраструктурой.  Функционал аутентификации на рабочем месте администратора должен предоставлять возможность надежно сохранить учетные данные.  СЗИ должно иметь собственную систему учетных записей или иметь возможность интегрироваться с MicrosoftActiveDirectory.  СЗИ должно поддерживать работу администраторов виртуальной инфраструктуры как через «толстый» клиент (vSphereclient), так и через «тонкий» (vSphereWeb-client).  **- Защита средств управления виртуальной инфраструктурой от НСД**  К средствам управления виртуальной инфраструктурой относятся:   * ESX-хосты, предназначенные для запуска виртуальных машин; * серверы vCenter, предназначенные для централизованного управления виртуальной инфраструктурой; * серверы vSphereWebClient, предназначенные для поддержки управления виртуальной инфраструктурой через «тонкий» клиент; * средства, предназначенные для обслуживания инфраструктуры, например, VMwareConsolidatedBackup, VMwareUpdateManager; * сторонние средства мониторинга и управления инфраструктурой.   Компрометация любого из этих средств приводит к компрометации группы виртуальных машин или всей виртуальной инфраструктуры.  Для обеспечения защиты средств управления виртуальной инфраструктурой должен применяется функционал мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Для этого весь управляющий трафик должен проходить через компонент СЗИ, осуществляющий этот контроль. Правила разграничения доступа должны работать на основе меток и уровней безопасности, а также заданных ACL и параметров соединения (протоколов, портов).  Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами должен подписываться, для обеспечения защиты от атак типа ManintheMiddle в процессе сетевого взаимодействия.  В ПО должен присутствовать механизм блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой. Тем самым должна обеспечивается защита средств управления виртуальной инфраструктурой от НСД со стороны скомпрометированной виртуальной машины.  **- Защита ESX-хостов от НСД**  В рамках обеспечения защиты ESX-хостов от НСД в СЗИ должны быть реализованы следующие механизмы:   * Возможность создания списка разрешенных программ; * Возможность создания списков запрещенных и разрешенных устройств: * Возможность создания списка пользователей, которым разрешен локальный вход на ESX-сервер; * Возможность блокирования подключения USB-носителей к ESX-серверу; * Возможность осуществления контроля за правилами встроенного межсетевого экрана; * Возможность запрета клонирования и создания снимков виртуальных машин; * Возможность очистки внешней и оперативной памяти при окончании работы с виртуальной машиной; * Возможность контроля обеспечения обязательной аутентификации в однопользовательском режиме; * Возможность ограничения доступа к конфигурационным файлам служб; * Возможность контроля использования протокола SSH версии 2; * Возможность модификации файла /etc/securetty для ограничения входа в систему под учетной записью root; * Возможность запрета на выполнение операций с буфером обмена для каждой виртуальной машины; * Возможность ограничения списка пользователей, которым разрешено выполнять назначенные задания; * Возможность ограничения доступа к конфигурационным файлам планировщика заданий; * Возможность установки ограниченных полномочий на файлы по умолчанию для демонов и root; * Возможность контроля использования разных сетей для Service Console и виртуальных машин; * Возможность контроля использования CHAP для проверки подлинности при подключении iSCSI-устройств; * Возможность контроля установленных параметров журналирования, требований к сложности пароля и доступа по сети; * Возможность запрета просмотра, изменения и выполнения vmdk-файлов; * Возможность запрета изменения vmx-файлов; * Возможность защиты от нехватки места на корневой файловой системе ESX-сервера; * Возможность контроля наличия пароля загрузчика ESX-сервера; * Возможность контроля настроенных параметров ядра ESX-сервера; * Возможность запрета контроля устройств ESX-сервера со стороны виртуальных машин; * Возможность запрета отсылки сообщений ESX-серверу со стороны виртуальных машин; * Возможность контроля прав на файлы журнала событий ESX-сервера; * Возможность задания приглашения для сетевого и локального доступа к ESX-серверу; * Возможность контроля настроек синхронизации времени; * Возможность контроля доступа к файлам, содержащим пароли пользователей; * Возможность ограничения доступа к конфигурационным файлам протокола SNMP; * Возможность настройки параметров безопасности для протокола SSH; * Возможность ограничения на удаление файлов ESX-сервера; * Возможность контроля отсутствия программ с setuid или setgid флагами; * Возможность ограничения права перезаписи файлов ESX-сервера; * Возможность запрета отсутствия файлов без владельца на ESX-сервере;   **- Контроль целостности конфигурации виртуальных машин и доверенная загрузка**  Для обеспечения контроля целостности программной среды и обеспечения доверенной загрузки операционной системы (ОС) в «физическом мире» традиционно используются аппаратные электронные замки для шин PCI или PCI-E. Подобные аппаратные СЗИ невозможно использовать для защиты виртуальных машин по техническим причинам. Тем не менее, данный функционал защиты должен быть обеспечен и в виртуальной среде.  ПО должно содержать компоненты, устанавливаемые на каждый ESX-хост и реализующие следующие механизмы защиты:   * Контроль целостности настроек виртуальной машины перед ее загрузкой. Должен контролироваться файл \*.vmx, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров. * Контроль образа BIOS виртуальной машины. Поскольку несанкционированная подмена BIOS является угрозой безопасности, СЗИ должно контролировать целостность файла \*.nvram, в котором содержится образ BIOS виртуальной машины. * Доверенная загрузка ОС должна осуществляться путем контроля целостности загрузочного сектора виртуального диска \*.vmdk. * Контроль целостности файлов гостевой ОС внутри виртуальных машин.   При изменении одного из перечисленных объектов как санкционированном, так и несанкционированном, СЗИ должно предоставить администратору безопасности возможность данные изменения отменить или принять. До того, как администратор безопасности примет решение, вносимые изменения применяться к объекту не должны.  **- Мандатный принцип контроля доступа**  В СЗИ должен быть реализован мандатный принцип контроля доступа на основе меток конфиденциальности. Должно присутствовать два вида меток конфиденциальности: иерархические (далее просто метки) и неиерархические (далее просто категории).  Должна быть реализована возможность пометить метками следующие субъекты, объекты, контейнеры:   * Администраторы ВИ * ESX-хосты * Сетевые карты ESX-хоста или VLAN * Разделы хранилищ (Datastore) * ВМ   Права доступа субъектов и объектов должны проверяться на основе меток и категорий автоматически и запрещать несанкционированные действия. Субъект может получить доступ к объекту, только если выполняется условие соответствия их меток конфиденциальности. Для категорий – это совпадение хотя бы одной из категорий субъекта и объекта, для меток – это уровень иерархии субъекта должен быть равен (или выше, в зависимости от настроек СЗИ) уровню объекта.  Категории должны отличаться от меток следующими параметрами:   * Метки должны быть иерархическими, категории равноправными. * Механизмы работы меток должны зависеть не только от пользователя, но и от его меток его текущей сессии. Категории от сессии зависеть не должны. * Любой субъект, объект, контейнер может быть помечен несколькими категориями и только одной меткой.   **- Регистрация событий, связанных с информационной безопасностью**  В СЗИ должен быть реализован механизм регистрации следующих групп событий:   * События аутентификации и разграничения доступа; * Средство должно регистрировать как удачные, так и неудачные попытки доступа к инфраструктуре (с указанием имени учетной записи, даты, имени компьютера или его IP-адреса) * Средство должно регистрировать события изменений конфигурации параметров безопасности и учетных записей администраторов инфраструктуры * События контроля целостности СЗИ, контроля целостности и доверенной загрузки виртуальных машин; * События, связанные с установкой, удалением, включением, остановом и сбоем компонентов СЗИ, а также с изменением настроек СЗИ.   Регистрация событий на всех компонентах СЗИ должна осуществляется в едином журнале. Для всех групп событий должны регистрироваться как факты НСД, так и правомочные действия.  **- Контроль целостности и защита от НСД компонентов СЗИ**  СЗИ должен содержать собственные механизмы контроля целостности компонентов СЗИ. Механизмы должны действовать на всех компонентах СЗИ — рабочем месте администратора, сервере авторизации, ESX-хостах и vCenter-серверах.  - **Централизованное управление и мониторинг**  СЗИ должно содержать Консоль управления, устанавливающуюся на рабочее место администратора безопасности со следующим функционалом:   * управление пользователями и компьютерами (пользователями в данном случае будут администраторы виртуальной инфраструктуры и администраторы безопасности, а компьютеры — это их рабочие места); * назначение прав на доступ к защищаемым объектам; * развертывание и настройка компонентов защиты ESX-хостов; * настройка правил разграничения запуска виртуальных машин и утверждение изменений параметров виртуальных машин, произведенных администраторами ВИ; * просмотр журнала регистрации событий.   Все изменения, произведенные администратором безопасности, должны сохраняться централизованно.  - **Возможность построения отчетов**  СЗИ должно предоставлять возможность генерации отчетов на основании произошедших в системе событий. В перечень отчетов должны входить следующие отчеты:   * Изменение конфигурации политик безопасности. * Использование учетных записей VMware. * Мониторинг учетных записей СЗИ. * Проблемы с доверенной загрузкой ВМ. * Настройка правил сетевой безопасности. * Настройки доступа к защищаемым объектам. * Соответствие стандартам безопасности. * Изменение мандатных правил доступа в СЗИ * Logon в нерабочее время * Изменение сетевых правил доступа в СЗИ * Попытки несанкционированного изменения настроек, контролируемых политиками * Применение политик безопасности * Проблемы с Logon в СЗИ. (В отчёте нужно задать число неоднократных попыток) * Проблемы с Logon в vSphere (В отчёте нужно задать число неоднократных попыток) * Проблемы со сменой пароля * Наиболее активные пользователи * Список наиболее используемых видов доступа (порты/протоколы) к защищаемым объектам * Список наиболее частых событий ИБ * Отчеты по соответствию лучшим практикам и стандартам   ***Требования по сертификации:***  - должен быть сертифицирован на соответствие требованиям ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа (далее – НСД) к информации. Показатели защищенности от НСД к информации» по классу не ниже 5-го;  - должен быть сертифицирован на соответствие требованиям ФСТЭК России «Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню не ниже 4-го;  - должен быть сертифицирован на соответствие требованиям ФСТЭК России для защиты информационных систем персональных данных (ИСПДн) с уровнем защищенности персональных данных до 1-го включительно;  - должен быть сертифицирован на соответствие требованиям ФСТЭК России для защиты государственных и муниципальных информационных систем (ГИС) до 1 класса включительно;  - должно подтверждаться соответствующими действующими сертификатами ФСТЭК  ***Комплект поставки:***   * Право на использование СЗИ для защиты ESX-хостов (за 1 физический процессор на защищаемом ESX-хосте) – 4 шт. * Установочный комплект, включающий: диск с ПО и документацией, формуляр, наклейка и сертификат (ФСТЭК) – 1 шт. | 1 |
| 4 | Передача неисключительных прав на воспроизведение программного обеспечения, реализующего функции криптографического клиента, отвечающего следующим требованиям:   * совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящей конкурсной документации: обновление программного обеспечения, обновление справочно-ключевой информации, управлением политиками безопасности; * совместимо (полностью) с программным комплексом, реализующим функции криптографического шлюза, представленным в настоящей конкурсной документации: шифрование/дешифрование направляемого/принимаемого IP-трафика; * поддержка операционных систем: * MicrosoftWindows 2000 Professional; * Microsoft Windows XP Home/Professional; * Microsoft Windows Vista (всялинейка); * MicrosoftWindows 7 (вся линейка). * MicrosoftWindows8/8.1(вся линейка). * наличие сертификата ФСТЭК России по требованиям к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно; * наличие сертификата ФСБ России по классу КС2; * иметь встроенный персональный экран, соответствующий 3-ому классу по требованиям ФСТЭК России; * предоставлять функции клиента службы обмена файлами и сообщениями, защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами; * 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; * возможность удаленного централизованного обновления адресной и ключевой информации комплекса с контролем прохождения обновления; * автоматическое распределение симметричной ключевой информации при появлении в сети новых пользователей, задании в Центре управления сетью новых связей или удалении существующих связей, компрометации ключей или штатных процедурах смены ключевой информации. * взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (бех использования криптографического шлюза»). | 2 |
| 5 | сертифицированная комплексная защита компьютера с помощью межсетевого экрана, системы обнаружения вторжений  ***Должно осуществлять защиту компьютера от внешних угроз:***  - межсетевое экранирование для рабочего места в сетях TCP/IP;  - защиту компьютера от атак по сети TCP/IP;  - антивирусную защиту от вредоносного программного обеспечения;  - защиту от спама и вредоносного контента веб-серверов;  - самозащиту от воздействия со стороны вредоносного программного обеспечения;  - регистрацию событий безопасности;  - иметь соответствующие сертификаты ФСТЭК;  ***Требования к операционной платформе и аппаратной части***:  - Windows 8, 7, Vista, XP x86/x64; Windows Server 2012 x64; Windows Server 2008 R2 x64, Server 2008 x86/x64; Windows Server 2003 R2 x86/x64, Server 2003 x86/x64;  - наличие привода CD-ROM;  - минимально необходимый размер оперативный памяти: 512 Мбайт.  ***Требования к централизованному управлению:***  - должно обеспечивать централизованную установку, удаление и обновление ПО на защищаемых рабочих станциях как в доменных сетях с MicrosoftActiveDirectory, так и в сетях с рабочими группами;  - должно обеспечивать удаленную настройку и управление с рабочего места администратора, объектами управления могут быть отдельные компьютеры, группы компьютеров (организационные подразделения);  - должно обеспечивать отслеживание событий безопасности.  ***Требования к функциональности средства межсетевого экранирования:***  - должно иметь сертификат ФСТЭК в соответствии с руководящим документом "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (Гостехкомиссия России, 1997) не ниже, чем по 4-му классу защищенности;  - должно соответствовать: классификация по уровню отсутствия недекларированных возможностей (Гостехкомиссия России, 1999) не ниже, чем по 4-му уровню контроля;  - должно контролировать входящие и исходящие соединения;  - должно обеспечивать контроль для приложений, использующихся на компьютере, при обращении к сети и создание правил сетевого доступа для приложений;  - режим обучения для сетевого доступа для приложений;  - разделение доступа к узлам сети;  - создание разрешенного и запрещенного списков сетевых ресурсов;  - возможность экспорта/импорта настроек межсетевого экрана с одного компьютера на другой;  - должно обеспечивать блокировку активного содержимого страниц веб-серверов;  - должно обеспечивать блокировку активного содержимого входящих электронных писем;  - должно обеспечивать регистрацию событий безопасности.  ***Требования к функциональности системы обнаружения вторжений:***  - должно соответствовать: требованиями руководящего документа "Требования к системам обнаружения вторжений" (утвержден приказом ФСТЭК России от 6 декабря 2011 г. № 638) для уровня узла по 4-му классу защиты;  - должно обеспечивать настройку на обнаружение типовых сетевых атак;  - должно обеспечивать блокировку сетевых сканеров;  - должно обеспечивать блокировку вредоносных процессов при их попытках воздействия на рабочие процессы;  - должно обеспечивать непрерывный мониторинг;  - должно обеспечивать регистрацию событий безопасности. | 1 |
| 6 | Система антивирусной защиты, в которую входят:  1. Лицензия для Серверных ОС – 1шт.  2. Лицензия для рабочих мест – 2 шт.  **Антивирусная защита должна обеспечивать:**  - обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;  - защиту от еще неизвестных вредоносных программ, принадлежащих зарегистрированным семействам, как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;  **- обнаружение угроз направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля**  Используемое антивирусное ядро:  - не должно допускать снижение скорости проверки при увеличении размера антивирусных баз;  - в целях оптимального расхода ресурсов должно, в зависимости от загрузки системы, выбирать уровень анализа упакованных объектов;  - в целях оптимального расхода ресурсов должно использовать механизм уменьшения размера промежуточных файлов;  **- в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика;**  - Система должна включать поддержку кластерного протокола, с помощью которого координируются действия над агентами защиты с разных антивирусных серверов  - Система управления должна включать систему управления лицензиями, позволяющую распределять между серверами в рамках иерархической сети необходимое количество лицензий  - управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов  - экспорта и импорта базы данных антивирусного сервера в XML-файл.  - создания иерархической сети антивирусных серверов. В случае реализации иерархической сети Система должна иметь возможность:  - объединения информации от нескольких серверов на одном.  - распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть.  - обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий  - контроля отсутствия связанных серверов в расписании антивирусного сервера.  - построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне;  **- централизованной настройки параметров защиты, уникальных для различных групп, в том числе для рабочих станций, находящихся в режиме off-line.**  - наличия множественных путей уведомления пользователей и администраторов путем посылки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap;  **- оповещения о возникновении эпидемий (множественных инфекций)**  **- оповещения о наличии обновлений сервера ESS**  - управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений  - контроля результатов обновления антивирусного ПО на станциях антивирусной сети.  - организации межсерверного обмена согласно расписанию  - ограничения канала связи по группам  - наличия возможности групповых обновлений  **- обновлений по защищенному каналу с использованием SSL-сертификатов**  - организации отложенного обновления  - проверки обновлений на выбранных администратором компьютерах/группах перед распространением их на все клиентские компьютеры  - централизованной удаленной установки и деинсталляции программных средств, антивирусных баз и антивирусного ядра на защищаемые узлы сети – в том числе на станции, находящиеся в разных доменах.  **Система управления должна поддерживать возможность:**  - создания точки восстановления перед установкой антивирусного пакета на защищаемые рабочие станции и сервера;  - восстановления удаленных станций.  **Система должна поддерживать множественную возможность установки своих компонентов на защищаемые рабочие станции – в том числе с помощью:**  - прямого их указания в системе управления в результате сканирования локальной сети, MicrosoftActiveDirectory,  - политикMicrosoft Active Directory  - синхронизациистанцийс Microsoft Active Directory  - установки с помощью дистрибутива, содержащего все компоненты защиты  - рассылки инсталляционных файлов из системы управления по электронной почте  - возможностей службы распределенной файловой системы (DFS).  - Система должна поддерживать возможность настройки правил автоматического распределения станций по пользовательским группам, а также возможность изменения первичной группы при автоматическом подтверждении доступа станций к антивирусному серверу  - Система должна иметь возможность выбора уровня подробности протоколирования своих компонентов. cистема управления должна иметь возможность загрузки архивированных файлов журнала работы всех антивирусных серверов иерархической сети  - В целях ограничения использования серверного пространства должна иметься возможность ротации файлов журнала антивирусного сервера по времени (час, день, неделя)  - Система управления должна обеспечивать защиту от несанкционированного доступа. Авторизация должна обеспечиваться парой логин/пароль.  - Администраторы Системы должны иметь возможность авторизации с помощью ActiveDirectory, LDAP, RADIUS, PAM. Система управления должна иметь возможность предварительного тестирования настроек авторизации внешних администраторов ActiveDirectory, LDAP и RADIUS  - возможность просмотра новостей безопасности, в том числе информирующих об актуальных угрозах  - возможностьмножественности путей обновления, в том числе по каналам связи и на съемных электронных носителях информации;  - возможность обновления через прокси-серверы, в том числе прокси-серверы MSISA/TMG.  - проверка целостности и подлинности обновлений средствами электронной цифровой подписи.  - в Системе, не имеющей доступа к сети Интернет, должна быть реализована возможность обновления вирусных баз путём скачивания их с сервера разработчика Системы с возможностью последующего их переноса в Систему с помощью любого носителя информации, в том числе с помощью мобильного сервера обновлений, созданного на основе flash-диска;  - В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория;  - Система должна иметь возможность перезагрузки защищаемой станции через систему управления  **Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства MicrosoftWindows**  Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:  - осуществление антивирусной (включая **постоянную защиту от руткит-технологий**) и антиспам защиты на рабочих станциях.  - Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки без существенного снижения производительности защищаемых рабочих станций. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.  - Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.  - непрерывное фоновое сканирование в целях нейтрализации активных угроз  - ограничения доступа к сети Интернет или к компьютеру в определенный момент времени по расписанию  - помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»;  - просмотр местоположения станций и серверов на карте, если заданы географические координаты станции  - Система защиты рабочих станций должна обеспечивать проверку протоколов:  - HTTP;  - IMAP, SMTP, POP3 независимо от используемого почтового клиента;  - NNTP (только проверка на вирусы), независимо от почтового клиента.  - Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макровирусов, опасных Java-апплетов, ActiveX и др.) посредством:  - антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;  - проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.  - В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.  - **Система должна обеспечивать защиту от еще не поступивших на анализ в антивирусную лабораторию вредоносных файлов (в том числе семейств Trojan.Encoder, Trojan.Inject и Trojan.Winlock) с помощью превентивной защиты, отслеживающей попытки внедрения вредоносных файлов**  **Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства MicrosoftWindows**  Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:  Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий.  Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.  Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию, должна обеспечивать защиту серверов под управлением операционных систем:  Microsoft Windows Server 2000;  Microsoft Windows Server 2003;  Microsoft Windows Server 2008.  Microsoft Windows Server 2012  Компоненты Системы должны устойчиво функционировать на серверах в условиях их минимальной и максимальной загрузки без существенного снижения производительности.  Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.  Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки с точки зрения безопасности и производительности работы. При этом, в случае необходимости внесения изменений, Система, используя возможности централизованного управления, должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователями в рамках, имеющихся у них прав.  Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы.  В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.  Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.  Система должна обеспечивать:  поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;  проверку всех скриптов, обрабатываемых в MicrosoftInternetExplorer, а также любых WSH-скриптов (JavaScript, VisualBasicScript и др.), запускаемых при работе пользователя на компьютере, в том числе и в Интернете. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;  блокировку опасных макросов VBA в реальном времени;  защиту от вредоносных сценариев, загружаемых с веб-страниц;  помещение найденных зараженных файлов в специальное место на жестком диске —«карантин»;  автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;  запуск задач по расписанию и/или сразу после загрузки операционной системы.  Система защиты серверов под управлением семейства ОС MicrosoftWindows должна обеспечивать реализацию следующих функциональных возможностей:  проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством:  антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;  проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.  В Системе должна быть реализована самозащита для всех ее объектов, в том числе критических файлов, процессов, окон, ключей и прочего, от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.  **Требования по комплектности поставке**  В состав Системы должны входить:  программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;  программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;  программные средства централизованного управления, мониторинга и обновления;  обновляемые базы данных сигнатур всевозможных вредоносных программ.  Комплект поставки должен содержать:   1. Установочный диск с дистрибутивом 2. Формуляр 3. Специальный защитный знак   Сертификат соответствия требованиям безопасности информации  необходимый набор серийных номеров либо ключевых файлов;  Система должна быть сертифицирована уполномоченным органом (ФСТЭК) на соответствие ТУ и НДВ 2 на применение в составе подсистемы антивирусной защиты информационных системах персональных данных (ИСПДн) класса К1.  Система должна быть сертифицирована уполномоченным органом (ФСТЭК) на соответствие требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 2 и требованиям технических условий.  **Требования по технической поддержке Системы**  Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.  Техническая поддержка должна включать возможность предоставления выделенного специалиста, доступного в режиме 5/8  Техническая поддержка должна включать возможность проведения расследования компьютерных инцидентов  Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе:  ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения;  ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определение того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения.  Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя. | 1 |
| 7 | Криптографический клиент необходимый для защищенного подключения Разработчиков ИС:  Программное обеспечение (ПО) должно уметь выполнять следующие функции: межсетевое экранирование, построение виртуальных частных сетей (VPN), обеспечение стойкого шифрования передаваемой информации.  ПО должно иметь возможность обеспечения защиты и фильтрации трафика сетей и служебного трафика.  ПО должно обеспечивать пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней.  ПО должно уметь маскировать реальный IP адрес (туннелирование трафика).  ПО должно поддерживать технологии протоколирования событий (syslog) и мониторинга глобальной статистики по протоколу SNMP.  ПО должно поддерживать установку в режиме One-Click-Installation (OCI) с использованием WindowsInstaller (MSI)  ПО должно поддерживать следующие алгоритмы:  шифрование ГОСТ 28147-89,  электронно-цифровая подпись ГОСТ Р 34.10-2001,  вычисление хэш сумм ГОСТ Р 34.11-94.  Комбинированный алгоритм шифрования с проверкой целостности ESP\_CIMIT G2814789CPRO1-K288-CNTMAC-253  ПО должно поддерживать работу через NAT.  ПО должно поддерживать работу по протоколам IKE/IPsec согласно cтандартамRFC 2401 – 2412.  ПО должно иметь возможность получения сертификатов открытых ключей по протоколу LDAP, возможность импорта и доставки через PKCS#7, PKCS#12.  ПО должно поддерживать использование списка отозванных сертификатов CRL.  ПО должно задавать независимые правила классификации и маркирования для входящего и исходящего трафика  ПО должно быть совместим с ОС:  MS Windows XP Professional (SP3)  MS Windows Vista (SP2)  MS Windows 7  MS Windows 8  Microsoft Windows Server 2003/2008/2008R2/2012  в т.ч. виртуальной среде  (VMWare/ HyperV/ Xen).  ПО должно быть совместим с программным комплексом CSPVPNClient  ПО должно поставляться на съемном CD носителе  Гарантийный срок не менее 12 мес.  ПО должно иметь сертификат ФСБ России на соответствие требованиям к СКЗИ класса КС1 и может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.  ПО должно иметь сертификат ФСТЭК на соответствие требованиям к межсетевым экранам по 3-ему классу защищенности.  ПО должно иметь сертификат ФСТЭК на соответствие классификации по уровню контроля отсутствия недекларированных возможностей по 3 уровню контроля и может использоваться в автоматизированных системах класса защищенности до 1В включительно, а также в государственных информационных системах до 1 класса защищенности включительно, в том числе, обеспечивающих 1, 2, 3 и 4 уровни защищенности персональных данных.  На ПО должны распространяться стандартные обязательства годовой технической поддержки. | 1 |
| 8 | Операционная система должна отвечать следующим функциональным возможностям:  - Условия поставки должны соответствовать правилам лицензирования производителя программного обеспечения;  - Совместимость со всеми поставляемыми в данном ТЗ средствами защиты информации;  - Интуитивно понятный пользовательский интерфейс;  - Поддержка подключения нескольких мониторов;  - Наличие функции быстрого переключения между пользователями;  - Эмулятор запуска приложений в текущей системе,  совместимые с разными версиями OC Windows;  - Наличие функции диагностирования, восстановления при сбое загрузки системы;  - Наличие функции создания точек восстановления системы.  - Наличие встроенной функции шифрования файлов;  - Наличие встроенной функции предоставления удаленного управления системой;  - Наличие встроенной функции защиты от вредоносного программного обеспечения;  - Возможность автоматического переключения принтера в зависимости от сетевого расположения;  - Возможность работы в качестве терминального сервера и сервера приложений;  - Возможность использования виртуализации штатными средствами с поддержкой x64-операционных гостевых систем. Лицензия должна обеспечивать возможность бесплатного запуска двух серверных гостевых ОС в рамках двухсокетного сервера;  - Возможность включения и отключения графического интерфейса операционной системы в рамках одного рестарта ОС;  - Возможность агрегации сетевых интерфейсов штатными средствами для повышения отказоустойчивости и производительности;  - Возможность объединения дисков в единый пул для оптимизации дисковой подсистемы;  - Возможность выступать в качестве Контроллера Домена ActiveDirectory;  - Возможность изменения версии на более раннюю (Даунгрэйда). | 3 |
| 9 | Лицензия должна предоставлять право подключения к любому количеству серверов с одного устройства любому количеству пользователей. | 60 |

**8. Требование к серверному оборудованию, дисковой полке для системы хранения данных и программному обеспечению среды виртуализации**

1) ПОсредывиртуализации - VMware vSphere 6 Standard for 1 processor\* - 4 штуки;

2) Сертификатподдержки Basic Support/Subscription VMware vSphere 6 Standard for 1 processor for 1 year\* - 4 штуки;

3) Сервер виртуализации - 2 штуки, удовлетворяющий следующим требованиям:

|  |  |
| --- | --- |
| Типоразмер | Не более 1U |
| Блок питания | Не менее двух от 400 до 550 Ватт каждый. С возможностью «горячей» замены и резервированием.  Эффективность не менее 94% при полной нагрузке. |
| Цвет передней панели корпуса | Черный |
| Глубина сервера | Не более 610 мм |
| Встроенные вентиляторы | Не менее 6 с возможностью горячей замены |
| Число отсеков 3,5" с возможностью горячей замены | Не менее 4 для SAS/SATA HDD |
| Число экспандеров SAS3 12Гб/с | Не менее 1 шт |
| Комплект для монтажа в 19" стойку | Наличие |
| Количество ядер процессора | Не менее 20 ядер или 10 ядер и 20 потоков |
| Максимальная тактовая частота | Не менее 2.2 ГГц |
| Кэш процессора | Не менее 25 МБ |
| Технология виртуализации | Наличие |
| Поддержка 64-разрядных приложений | Наличие |
| Технология защиты системы от программных ошибок | Наличие |
| Новые команды AES | Наличие |
| Встроенный контроллер памяти | Наличие |
| Макс. пропускная способность памяти | Не менее 68Гб/с |
| Поддержка памяти ECC | Наличие |
| Кол-во каналов памяти на каждый процессор | Не менее 4 |
| Количество установленных процессоров | Не менее 2 |
| Максимальное количество процессоров | Не менее 2 |
| Кол-во слотов под оперативную память | Не менее 12 |
| Тип оперативной памяти | DDR4 с функцией коррекции ошибок |
| Объем установленной оперативной памяти | Не менее 32 ГБ |
| Тактовая частота оперативной памяти | Не менее 2400 МГц |
| Обнаружение ошибок | Исправление однобитных ошибок  Обнаружение двухбитных ошибок |
| Количество разъемов PCI Express | Не менее 2 слотов PCI-E 3.0 x16 |
| Привод DVD-RW | Наличие |
| Raid-контроллер | Наличие |
| Ключевые характеристики Raid-контроллера | Не менее 1 ГБ кэш-памяти с защитой на базе флэш-памяти  RAID уровнй 0, 1, 5, 6, 10, 50 и 60  Поддерживает до 255 дисков SATA или SAS при использовании SAS-экспандеров  Hybrid RAID 1 и 10  Быстрая инициализация  OnlineCapacityExpansion (увеличение емкости RAID-массива без выключения сервера)  HotSpare (автоматическое копирование данных с диска "горячего" резерва обратно на новый диск, установленный вместо отказавшего)  Алгоритм динамического кэширования  NativeCommandQueuing (NCQ)  Фоновая инициализация  Поддержка "горячего подключения" дисков  RAID Level Migration (миграцияуровней RAID)  Различные типы дисков "горячего" резерва – глобальный, выделенный, объединенные в пул  Автоматическое и ручное восстановление "горячего" резерва  Управление дисковой системoи хранения с помощью SES и SAF-TE  Конфигурирование размера полосы  Поддержка S.M.A.R.T.  Многие и разные типы RAID-массивов на дисках  Таблица дефектных полос  Динамическое восстановление дефектных секторов диска  Поддержка StaggeredDriveSpin-Up (постепенная раскрутка дисков)  Поддержка загрузочного массива  Поддержка накопителей на ленте, автозагрузчиков  Поддержка безопасной загрузки для BIOS uEFI  Cовместимость с VMwarevSphereESXi 6.0 |
| Управление | Аппаратная реализация удаленного управления сервером, обеспечивающая следующие функции:   • Поддержка IPMI over LAN  • Поддержка Serial over LAN  • Поддержка KVM over LAN  • Поддержка Virtual Media over LAN  • Поддержка LAN Alerting-SNMP Trap  • Поддержка журнала событий  • Независимость от ОС (Операционная система)  • Обеспечение удаленного аппаратного мониторинга через IPMI.  Включая следующее:  - Состояние датчиков температуры (процессор, системная плата)  - Состояние датчиков скорости вращения вентиляторов корпуса сервера  - Состояние датчиков напряжения (материнская плата, модули управления питанием процессора)  - Определение ошибок памяти ECC  - Состояние питания (блоки питания)  - Состояние датчика вскрытия корпуса  - Удаленное управление питанием: включение питания, выключение питания или перезагрузка системы  - Удаленный доступ к текстовой или графической системной информации, включая настройку BIOS и информацию о работе ОС (KVM)  - Удаленное управление программными приложениями   • Обеспечение безопасное сетевое управление через удаленное управление/перенаправление консоли   Наличие выделенного сетевого порта для управления, не менее 100 Мбит/с. Наличие всего необходимого программного обеспечения, рекомендуемого производителем платформы. |
| Сетевой контроллер Тип 1 | Не менее 1 Гбит/с на порт |
| Сетевой контроллер Тип 2 | Не менее четырех портов должны работать в соответствии с стандартами: IEEE 802.3ae, IEEE 802.1q (VLAN), IEEE 802.3ad, IEEE 802.3x, IEEE 802.3an, IEEE 802.3ab 1000BASE-T. |
| Сетевой контроллер Тип 3 | Не менее двух портов SFP+ 10GbE |
| Сетевой контроллер Тип 4 | Не менее двух портов с FC-интерфейсом, не менее 8 Гбит/с |
| Порты на задней панели | Не менее 4x USB 2.0, не менее 1x COM, не менее 3x RJ-45, не менее 2x VGA порта |
| Дисковый массив | Не менее 3 жестких дисков. Не менее 300 ГБ каждый.  Предназначен для построения рейд-массивов и использования в серверных платформах.  Возможность работы в режиме 24x7 (24 часа, 7 дней в неделю)  Скорость вращения шпинделя - не менее 10000 оборотов/мин. |
| Комплект пачкордов | 1. Патчкорд (цвет красный) RJ-45 для DMZ зоны длина 20 метров.  2. Патчкорд для 10 Гбит карт SFP+ – 4 штуки, длина 3 метра.  3. Пачкорд оптический – LC-LC дуплекс – OM3 многомод – 4 штуки, длина 3 метра.  4. Пачкорд RJ-45 (цвет синий) – 2 штуки, длина 3 метра.  5. Пачкорд оптический – LC-LC дуплекс – OM4 многомод – 16 штук, длина 20 метров. |
| Общие требования к серверному оборудованию: | |
| Оборудование должно быть новым, не восстановленным, не допускается поставка выставочных образцов. Оборудование должно быть поставлено комплектно и обеспечивать конструктивную и функциональную совместимость. | |
| Поставляемое оборудование должно соответствовать действующим стандартам и нормам по пожарной, санитарной и электрической безопасности, а также электромагнитной совместимости, в соответствии с номенклатурой продукции, в отношении которой законодательными актами Российской Федерации предусмотрена обязательная сертификация с документальным подтверждением. Наличие у поставляемого оборудования действующих сертификатов соответствия требованиям: ТР ТС 004/2011 «О безопасности низковольтного оборудования»; ТР ТС 020/2011 «Электромагнитная совместимость технических средств». | |
| Гарантия на поставляемое серверное оборудование не менее 36 месяцев. | |

4) Дисковая полка для системы хранения данных EMC VNX5500 6GSDAE15 в комплекте с 15 дисками 2TB NL SAS 3.5IN\*\* - 1 штука.

\* В соответствии с пунктом 1 статьи №33 Федерального закона от 05.04.2013 N 44-ФЗ (ред. от 03.07.2016) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения взаимодействия с программным обеспечением, используемым заказчиком, эквивалент на указанное оборудование не предусмотрен.

\*\* В соответствии с пунктом 1 статьи №33 Федерального закона от 05.04.2013 N 44-ФЗ (ред. от 03.07.2016) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в связи с необходимостью обеспечения взаимодействия с СХД EMC S/N CKM00134200229, используемым заказчиком, эквивалент на указанное оборудование не предусмотрен.

**9. Установка и настройка СЗИ**

9.1. Установка и настройка СЗИ должна производиться Исполнителем в соответствии с эксплуатационной документацией, разработанным техническим проектом и должны реализовывать все определенные в техническом проекте и техническом задании меры по обеспечению безопасности информации.

9.2. Установка и настройка средств криптографической защиты должна осуществляться Исполнителем на основании действующей лицензии ФСБ России на 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 (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).

9.3. Работы по установке, настройке СЗИ должны осуществляться Исполнителем на основании действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

**10. Аттестация информационной системы**

10.1. При аттестации информационных систем Исполнитель проводит комплексную проверку объектов информатизации для оценки соответствия требованиям по защите информации от несанкционированного доступа.

10.2. Аттестационные испытания проводятся исполнителем на объекте информатизации по адресу нахождения заказчика.

10.3. Комплекты аттестационных документов предоставляются Конечному пользователю по результатам проведения аттестационных испытаний и включают следующие документы:

- программа и методики проведения аттестационных испытаний;

**–** протоколы испытаний системы защиты от НСД;

**–** заключение по результатам аттестационных испытаний;

**–** аттестаты соответствия требованиям информационной безопасности.

**11. Гарантийные обязательства и техническая поддержка СЗИ**

11.1. После завершения работ Исполнителем должно быть обеспечено гарантийное обслуживание работ в течение 12 месяцев с момента подписания Акта сдачи-приемки выполненных работ.

Гарантийное обслуживание работ должно осуществляться без дополнительной оплаты.

11.2. Исполнитель на постоянной основе должен обеспечивать Конечному пользователю техническую поддержку, консультирование (по телефону «горячей линии», электронной почте, иными способами) по всем вопросам работы с СЗИ, в течение 12 месяцев с момента подписания Акта сдачи-приемки выполненных работ.

11.3. Время прибытия сотрудника на площадку заказчика при возникновении критичных проблем в работе системы защиты информации не должно превышать 3-х часов.

Техническая поддержка и консультирование должны осуществляться без дополнительной оплаты.

**12. Требования к обучению администраторов, пользователей**

12.1. После проведения всех работ, предусмотренных настоящим техническим заданием, Исполнитель должен провести базовое обучение работников Заказчика (администраторов по безопасности и пользователей).

12.2. Список обучаемых сотрудников Исполнитель предварительно согласовывает с Заказчиком

**Приложение № 3**

**к документации об аукционе**

**Форма 1**

***ПОКАЗАТЕЛИ ПРЕДЛАГАЕМОГО ДЛЯ ПОСТАВКИ ТОВАРА***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование предлагаемого к поставке товара | Товарный знак (его словесное обозначение) (при наличии), знак обслуживания (при наличии), фирменное наименование (при наличии), патенты (при наличии), полезные модели (при наличии), промышленные образцы (при наличии), предлагаемого для поставки товара | Наименование страны происхождения товара | Характеристика поставляемого товара (конкретные показатели, соответствующие значениям, установленным документацией об аукционе) |
|  |  |  |  |  |

**Форма 2**

***СВЕДЕНИЯ ОБ УЧАСТНИКЕ ЗАКУПКИ***

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование сведений** | **Содержание сведений** |
| для физических лиц | | |
| 1 | Фамилия, имя, отчество (при наличии) |  |
| 2 | Паспортные данные |  |
| 3 | Место жительства |  |
| 4 | Номер контактного телефона |  |
| 5 | ИНН участника |  |
| для юридических лиц | | |
| 6 | Наименование, фирменное наименование (при наличии) |  |
| 7 | Место нахождения |  |
| 8 | Почтовый адрес |  |
| 9 | Номер контактного телефона |  |
| 10 | ИНН участника |  |
| 11 | ИНН (при наличии) учредителей, членов коллегиального исполнительного органа |  |
| 12 | ИНН (при наличии) лица, исполняющего функции единоличного исполнительного органа |  |

**Форма 3**

***ДЕКЛАРАЦИЯ О СООТВЕТСТВИИ УЧАСТНИКА АУКЦИОНА***

|  |
| --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (наименование участника аукциона)  декларирует о своем соответствии следующим требованиям: |

1) непроведение ликвидации участника аукциона - юридического лица и отсутствие решения арбитражного суда о признании участника аукциона - юридического лица или индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства;

2) неприостановление деятельности участника аукциона в порядке, установленном Кодексом Российской Федерации об административных правонарушениях, на дату подачи заявки на участие в аукционе;

3) отсутствие у участника аукциона недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов участника закупки, по данным бухгалтерской отчетности за последний отчетный период. (Участник аукциона считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по такому заявлению на дату рассмотрения заявки на участие в определении поставщика (подрядчика, исполнителя) не принято);

4) отсутствие у участника аукциона - физического лица либо у руководителя, членов коллегиального исполнительного органа или главного бухгалтера юридического лица - участника аукциона судимости за преступления в сфере экономики (за исключением лиц, у которых такая судимость погашена или снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации;

5) отсутствие между участником аукциона и заказчиком конфликта интересов, под которым понимаются случаи, при которых руководитель заказчика, член комиссии по осуществлению закупок, руководитель контрактной службы заказчика, контрактный управляющий состоят в браке с физическими лицами, являющимися выгодоприобретателями, единоличным исполнительным органом хозяйственного общества (директором, генеральным директором, управляющим, президентом и другими), членами коллегиального исполнительного органа хозяйственного общества, руководителем (директором, генеральным директором) учреждения илиунитарногопредприятия либо иными органами управления юридических лиц - участников аукциона, с физическими лицами, в том числе зарегистрированными в качестве индивидуального предпринимателя, - участниками закупки либо являются близкими родственниками (родственниками по прямой восходящей и нисходящей линии (родителями и детьми, дедушкой, бабушкой и внуками), полнородными и неполнородными (имеющими общих отца или мать) братьями и сестрами), усыновителями или усыновленными указанных физических лиц. Под выгодоприобретателями понимаются физические лица, владеющие напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном капитале хозяйственного общества