|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ: |
|  |  |
|  | МУП УИС |
|  | *(наименование заказчика)* |
|  |  |
|  | *(подпись)* |
|  | Председатель Закупочной комиссии Д. Н. Филиппов |
|  | *(должность, И. О. Фамилия)*«23» марта 2023 г. |
|  |
|  |
| **Извещение** |
| **о закупке путём запроса котировок в электронной форме****по лоту № 6823 «Оказание услуг по обеспечению информационной безопасности » для нужд МУП УИС** |
| Настоящее извещение разработано в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (далее – Федеральный закон от 18.07.2011 г. № 223-ФЗ), Гражданским кодексом РФ, Федеральным законом от 26.07.2006 № 135-ФЗ «О защите конкуренции» и Положением «О закупке товаров, работ, услуг для нужд МУП УИС» |
| **1. Информация о заказчике:** |
| Заказчик: | МУП УИС**Уведомление о статусе Заказчика:**Определением Арбитражного суда Республики Башкортостан от 02.09.2022 по делу № А07-13106/2018 МУП УИС признано несостоятельным (банкротом), открыто конкурсное производство сроком на 6 месяцев.Согласно ч. 1 ст. 126 Федерального закона от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» все требования кредиторов по денежным обязательствам, об уплате обязательных платежей, иные имущественные требования, за исключением текущих платежей, указанных в пункте 1 статьи 134 настоящего Федерального закона, и требований о признании права собственности, об истребовании имущества из чужого незаконного владения, о признании недействительными ничтожных сделок и о применении последствий их недействительности могут быть предъявлены только в ходе конкурсного производства. |
| ЭТП: | ООО «БашЗаказ», bashzakaz.ru |
| Почтовый адрес: | 450080, Республика Башкортостан, город Уфа, улица Степана Злобина, дом № 31/4 |
| Место нахождения: | 450080, Республика Башкортостан, город Уфа, улица Степана Злобина, дом № 31/4 |
| Контактное лицо по организационным вопросам: | Живчук Ольга Владимировна |
| Контактное лицо по техническим вопросам: | начальник отдела безопасности Загидуллин Эраст Робертович тел.: 89177609259, e-mail: mup.uis@yandex.ru |
| Адрес электронной почты: | uiszakupki@gmail.com |
| Контактный телефон: | +79177607750 ([также доступен Telegram](https://t.me/uiszakupki))Внимание! При недоступности данного номера необходимо изложить суть вопроса в письме на электронную почту uiszakupki@gmail.com или в Телеграм [@uiszakupki](https://t.me/uiszakupki) с указанием номера извещения. |
|  |  |
| **2. Источник финансирования:**  | собственные средства Заказчика |
|  |
| **3. Предмет договора:** в соответствии с техническим заданием (приложение №1 к настоящему извещению) |
| **4. Место оказания услуг (выполнения работ):** | в соответствии с техническим заданием (приложение №1 к настоящему извещению) |
|  |
| **5. Срок оказания услуг (выполнения работ):** | в соответствии с техническим заданием |
|  |
| **6. Начальная (максимальная) цена договора: 11 295 187,67 руб.** |
|  |
| **7. Порядок формирования, определения и обоснования начальной (максимальной) цена договора:**В стоимость договора включены: стоимость услуг, работ, налогов и других обязательных платежей, всех затрат и расходов, связанных с надлежащим исполнением договора.Начальная (максимальная) цена договора сформирована Заказчиком методом сопоставимых рыночных цен. |
| **8. Информация об оплате договора:** |
| Срок и условия оплаты: предоплата 50% с окончательным расчётом в течение 7 рабочих дней с момента подписания Заказчиком документа о приёмке оказанных услуг и оборудования |
|  |
| **9. Порядок подачи заявок, форма котировочной заявки:** |
| Котировочные заявки подаются в электронной форме в соответствии с регламентом электронной торговой площадки.Участник закупки вправе подать только одну заявку.Заявка должна быть составлена по форме, приведённой в Приложении № 2 к извещению о проведении запроса котировок.Оценка и сопоставление заявок на участие производится Заказчиком с учётом требований Постановления Правительства РФ от 16.09.2016 № 925 и статьи 18 Положения «О закупке товаров, работ, услуг для нужд МУП УИС».Заявка должна быть подписана участником закупки или лицом, уполномоченным на то участником закупки.Подавая котировочную заявку, участник закупки соглашается с выполнением всех условий запроса котировок, указанных в извещении о проведении запроса котировок и приложениях к нему.Заказчик вправе отказаться от проведения запроса котировок в любое время до истечения срока подачи заявок на участие. Извещение об отказе от проведения запроса котировок размещается в ЕИС в день принятия такого решения. |
| **10.**  **Место, дата начала и дата окончания срока подачи котировочных заявок:** |
| Котировочные заявки принимаются с «24» марта 2023 г. на электронной торговой площадке. |
|  |
| Заявки подаются только по установленной форме (Приложение № 2). Приём заявок заканчивается в 12:00 по местному времени Заказчика «31» марта 2023 г. |
|  |
| **11. Срок, место и порядок предоставления документации о проведении запроса котировок** |
| Документация о закупке размещается в единой информационной системе (ЕИС, zakupki.gov.ru) и доступна для скачивания без дополнительной платы. |
| **12. Разъяснение положений документации о закупке и внесение в неё изменений**1. Любой участник закупки вправе направить по электронной почте Заказчику запрос о разъяснении положений документации о закупке.2.Заказчик в приемлемые для него сроки направляет по электронной почте разъяснения положений документации о закупке, если указанный запрос поступил к Заказчику не позднее, чем за 3 рабочих дня до дня окончания подачи заявок на участие в закупке, установленного документацией о закупке. Запросы, поступившие позднее, чем за 3 рабочих дня до дня окончания подачи заявок, не рассматриваются.3.В течение 3 рабочих дней со дня направления разъяснения положений документации о закупке по запросу участника такое разъяснение размещается Заказчиком в ЕИС с указанием предмета запроса, но без указания участника, от которого поступил запрос. 4. Заказчик по собственной инициативе или в соответствии с запросом участника закупки вправе принять решение о внесении изменений в извещение о закупке и/или документацию о закупке в любое время до истечения срока подачи заявок.5. Любые изменения, вносимые в документацию о закупке, являются неотъемлемой ее частью и на них распространяются все указания, содержащиеся в документации о закупке. 6. Изменения, вносимые в извещение о закупке, документацию о закупке, размещаются Заказчиком в ЕИС в день принятия решения о внесении указанных изменений. При этом срок подачи заявок на участие в запросе котировок должен быть продлён так, чтобы с даты размещения в ЕИС указанных изменений до даты истечения срока подачи заявок на участие в запросе котировок этот срок составлял не менее чем 3 рабочих дня.7. Заказчик не несёт ответственности за неознакомление (либо несвоевременное ознакомление) участника закупки с изменениями, размещёнными в ЕИС. Участник самостоятельно отслеживает изменения, размещаемые Заказчиком в ЕИС. |
| **13. Рассмотрение и оценка котировочных заявок** |
| Заказчик начинает процедуру рассмотрения заявок «04» апреля 2023 г. |
| Закупочная комиссия МУП УИС (далее – комиссия) после открытия доступа котировочных заявок рассматривает котировочные заявки на соответствие их требованиям, установленным в извещении о проведении запроса котировок, и оценивает котировочные заявки.Заказчик вправе провести процедуру переторжки в соответствии со ст. 21.1 Положения «О закупке товаров, работ, услуг для нужд МУП УИС».При предложении наиболее низкой цены договора несколькими участниками закупки победителем признаётся участник закупки, котировочная заявка которого поступила ранее котировочных заявок других участников.Комиссия не рассматривает и отклоняет котировочные заявки, если они не соответствуют требованиям, установленным в котировочной документации, или предложенная в котировочных заявках цена договора превышает начальную (максимальную) цену (или цена заявки участника, чьи товары (работы, услуги) не облагаются НДС, превышает начальную (максимальную) цену за вычетом НДС 20%), указанную в извещении о проведении запроса котировок, либо участник закупки не соответствует требованиям, предъявляемым к участникам в соответствии с извещением о закупке.Результаты рассмотрения и оценки котировочных заявок оформляются протоколом рассмотрения и оценки котировочных заявок, который подписывается всеми присутствующими на заседании членами комиссии и не позднее 3 дней со дня подписания размещается в ЕИС.Заявки на участие в запросе котировок рассматриваются Заказчиком в срок, не превышающий 10 рабочих дней с установленной в извещении даты начала рассмотрения заявок.Заказчик направляет победителю запроса котировок проект договора на электронной торговой площадке, который составляется путём включения в него условий исполнения договора, предусмотренных, и цены, предложенной победителем запроса котировок в заявке. |
| **14. Заключение договора** |
| Договор по результатам закупки заключается не ранее чем через десять дней и не позднее чем через двадцать дней с даты размещения в ЕИС итогового протокола.Проведением запроса котировок Заказчик не берёт на себя обязательств по приобретению полного объёма работ, услуг.При заключении договора Заказчик включает условия, предложенные победителем в заявке на участие в закупке, в проект договора, являющийся неотъемлемой частью документации о закупке и направляет проект договора победителю закупочной процедуры для дальнейшего подписания на электронной торговой площадке.Заказчик обязан отказаться от заключения договора с победителем проведенной закупочной процедуры в случае установления факта несоответствия победителя требованиям установленным Положением и документацией о закупке. В этом случае комиссия оформляет протокол об отказе от заключения договора, в котором должны содержаться сведения о месте, дате и времени его составления, о лице, с которым Заказчик отказывается заключить договор, сведения о фактах, являющихся основанием для отказа от заключения договора. Протокол размещается в ЕИС не позднее чем через 3 дня после его подписания. |
|  |
| **15. Требования к участнику закупки:** |
| 1. Участник закупки не должен находиться в процессе ликвидации, в отношении участника не должно быть принято арбитражным судом решения о признании участника закупки банкротом и об открытии конкурсного производства, деятельность участника не должна быть приостановлена в порядке, предусмотренном Кодексом РФ об административных правонарушениях.2. У участника закупки не должно быть просроченной задолженности по налогам, сборам и иным обязательным платежам в бюджеты любого уровня и государственные внебюджетные фонды.3. Сведения об участнике закупки должны отсутствовать в реестре недобросовестных поставщиков, предусмотренном Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» и (или) в реестре недобросовестных поставщиков, предусмотренном Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».4. Наличие действующей лицензии, выданной Федеральной службой по техническому и экспортному контролю в соответствии с Постановлением Правительства РФ от 03 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» на осуществление деятельности по технической защите конфиденциальной информации, с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:* контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

**или*** услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

**либо**наличие выписки из реестра лицензий, на осуществление деятельности по технической защите конфиденциальной информации, с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:* контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

**или*** услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

5. Наличие действующей лицензий, выданной Федеральной службой безопасности в соответствии с Постановлением Правительства РФ от 16 апреля 2012 года № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (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) с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:* монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

**или*** монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

**либо**Наличие выписки из реестра лицензий, на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (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) с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:* монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

**или*** монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.
 |
| **16. Перечень документов, необходимых к предоставлению в составе заявки участниками закупки:** |
| 1. Котировочная заявка (**скан в формате PDF**) строго по форме Заказчика, содержащая согласие на оказание услуг, выполнение работ на условиях, предусмотренных извещением о закупке, техническим заданием и проектом договора.2. Котировочная заявка **в формате Word** (без заверения, подписей и печатей), соответствующая отсканированному оригиналу котировочной заявки.3. Учредительные документы (устав, положения, свидетельство о регистрации в налоговом органе, приказ о назначении директора, протокол собрания и др.).4. Выписка из единого реестра юридических лиц, либо из реестра индивидуальных предпринимателей, полученная не ранее чем за 6 месяцев до размещения извещения о запросе котировок (с ЭЦП ФНС, без заверения).5. Документ, подтверждающий полномочия руководителя участника закупки.6. Документ, подтверждающий полномочия лица на подписание котировочной заявки, если заявка подписывается не руководителем (либо надлежащим образом заверенная копия доверенности от руководителя с указанием полномочий на подписание заявки).7. Решение об одобрении или о совершении крупной сделки в случае, если требование о необходимости наличия такого решения для совершения крупной сделки установлено законодательством РФ, учредительными документами участника закупки и если для участника закупки оказание услуг (выполнение работ), являющихся предметом договора, является крупной сделкой.8. Выписка из единого реестра субъектов малого и среднего предпринимательства с сайта <https://rmsp.nalog.ru/> (с ЭЦП ФНС, без заверения), если участник относится к таковым субъектам.9. Документы, подтверждающие соответствие участника требованиям, указанным в п. 4-5 раздела 15 извещения о закупке.При отсутствии в составе заявки любого из документов, указанных в разделе 16, Заказчик вправе отклонить заявку без рассмотрения. Исключение из данного правила составляют только документы, наличие которых не предусмотрено организационно-правовой формой участника и документ, указанный в п. 8 раздела 16 (если участник не является субъектом МСП).Документы предоставляются в виде надлежащим образом заверенных копий (заверенная руководителем организации или уполномоченным лицом), кроме документов, указанных в п. 2, 4, 8 раздела 16 извещения о закупке. |
| К настоящему извещению прилагаются: |
| - Приложение № 1 «Техническое задание» |
| - Приложение № 2 «Форма котировочной заявки»; |
| - Приложение № 3 «Проект договора». |
|  |
|  |

Приложение № 1 к извещению

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

1. Наименование

Оказание услуг по обеспечению информационной безопасности.

1. **Ответственные лица**

Ответственное лицо:

начальник отдела безопасности Загидуллин Эраст Робертович

тел.: 89177609259, e-mail: mup.uis@yandex.ru

1. Объем и сроки выполнения

Для оказания услуг и выполнение работ по обеспечению информационной безопасности необходимо выполнить следующее:

* 1. **Поставка межсетевого экрана. Многофункциональный узел безопасности. Установка и настройка.**

Узел безопасности (далее - УБ) должен быть выполнен в виде законченного аппаратно-программного комплекса с предварительно установленным программным обеспечением.

Общее количество поставляемых комплексов - 4 (четыре) шт.:

* комплекс № 1 - 2 (две) шт.;
* комплекс № 2 - 2 (две) шт.
	+ 1. **Комплекс № 1 и № 2 должен обеспечивать:**
* межсетевое экранирование;
* создание и поддержание VPN-каналов с криптографической защитой передаваемых данных;
* обнаружение и предотвращение сетевых атак;
* централизованное управление всеми компонентами комплекса, аудитом и мониторингом состояния узлов корпоративной сети;
* обеспечение защищенного межсетевого взаимодействия удаленных пользователей с корпоративными ресурсами (Remote Access VPN);
* сбор информации о пакетах данных;
* визуализация собранной информации;
* оперативное реагирование на выявленные вторжения;
* оповещение центра управления сетью о своей активности и о событиях, требующих оперативного вмешательства в режиме реального времени;
* регистрация событий, связанных с работой УБ;
* идентификация и аутентификация администратора при подключении к УБ;
* контроль целостности программного обеспечения УБ.
* аутентификацию УБ комплекса;
* централизованное управление сетью УБ;
* мониторинг и протоколирование состояния сети УБ;
* получение и хранение журналов УБ;
* регистрацию событий, связанных с управлением УБ;
* хранение конфигураций УБ;
* рассылку конфигурационной информации на УБ и резервные центры управления сетью (далее - ЦУС);
* восстановление информации о состоянии комплекса из резервной копии;
* возможность синхронизации времени ЦУС с заданным сервером точного времени по протоколу NTP с возможностью аутентификации.
	+ 1. **Требования к аппаратной части комплекса № 1:**
* исполнение: для установки в монтажную стойку, высота не более 1U;
* наличие крепежного комплекта для установки в монтажный шкаф 19'';
* компактное исполнение формата mini-ITX предусматривающее возможность встраивания;
* не менее одного процессора: Intel Atom C3758;
* не менее 16 ГБ оперативной памяти;
* не менее 8 (восьми) сетевых интерфейсов в конфигурации:
	+ 4 x 1000BASE-T RJ45;
	+ 2 х Combo 1G RJ45/SFP;
	+ 2 x 10G SFP+;
* не менее 2 (двух) модуль трансиверов (SFP+ - модуль) 10 Гбит/с для каждого УБ;
* не менее 1 (одного) дискового накопителя объемом не менее 256 ГБ;
* не менее 2 (двух) портов USB 2.0;
* не менее 2 (двух) портов USB 3.0;
* не менее 1 (одного) COM порта RJ45;
* не менее 1 (одного) видео порта VGA;
* носитель информации типа USB Flash Drive;
* потребляемая мощность не более 36 Вт;
* блок питания: внешний адаптер переменного тока. Входные параметры: ~100–240 В, 1,2 А, 50–60 Гц. Выходные параметры: 12 В, 3 А;
* шнур питания европейского стандарта длиной не менее 1 метра;
* Платформа должна обеспечивать среднее время наработки на отказ (MTBF) не менее 50 000 часов.
	+ 1. **Требования к аппаратной части комплекса № 2:**
* исполнение: mini-ITX, высота не более 1U;
* наличие крепежного комплекта для установки в монтажный шкаф 19'';
* не менее одного процессора Intel Atom C3538;
* не менее 16 ГБ оперативной памяти;
* не менее 5 (пяти) сетевых интерфейсов:
	+ 4x 10/100/1000BASE-T RJ45;
	+ 1x 1G SFP;
* не менее 1 (одного) модуль трансивера (SFP - модуль) 1 Гбит/с для каждого УБ;
* не менее 1 (одного) дискового накопителя объемом не менее 64 ГБ;
* не менее 2 (двух) портов USB 2.0;
* не менее 1 (одного) видео порта VGA;
* не менее 1 (одного) последовательного (COM) порта с разъемом RJ45;
* носитель информации типа USB Flash Drive;
* потребляемая мощность не более 36 Вт;
* блок питания: внешний адаптер переменного тока. Входные параметры: ~100–240 В, до 1,5 А, 50–60 Гц. Выходные параметры: 12 В, не менее 3 А.;
* шнур питания европейского стандарта длиной не менее 1 метра;
* платформа должна обеспечивать среднее время наработки на отказ (MTBF) не менее 50 000 часов.
	+ 1. **Требования к общей функциональности комплекса № 1 и № 2:**
* прием и передача IP-пакетов по протоколам семейства TCP/IP;
* прием и передача Ethernet-кадров;
* возможность маршрутизации IP-трафика;
* создание VPN-каналов с криптографической защитой передаваемых данных;
* поддержка Jumbo frame (MTU 9000 байт);
* возможность агрегации интерфейсов по протоколу LACP (802.3ad);
* возможность идентификации и аутентификации пользователей (из локальной базы пользователей ЦУС и/или из MS Active Directory), работающих на компьютерах в защищаемой сети Узла Безопасности, с помощью Агентов аутентификации, установленных на компьютерах пользователей и/или Captive Portal;
* возможность использовать двухфакторную аутентификацию от Multifactor;
* фильтрация IP-пакетов в соответствии с заданными правилами фильтрации на основе:
* IP-адресов отправителя и получателя;
* протоколов;
* номеров портов UDP/TCP;
* флагов TCP/IP-пакетов;
* временного интервала;
* принадлежности пользователей к группам пользователей, определенным администратором комплекса;
* типа приложений;
* url адреса;
* доменного имени (FQDN);
* фильтрация пакетов с контролем состояния соединений (stateful inspection);
* поддержка функции контроля приложений, позволяющей разграничивать доступ к наиболее популярным сайтам и приложениям;
* возможность использования приложений и категорий приложений в правилах межсетевого экрана:
* контроль приложений - поддержка более 200 приложений и протоколов;
* возможность просмотра средствами локального управления таблицы состояний TCP соединений (stateful);
* наличие встроенного DHCP-сервера;
* поддержка режима DHCP Relay;
* поддержка расширенного набора опций DHCP;
* возможность указывать время жизни DNS-записи;
* возможность закреплять статические IP-адреса для объектов типа доменное имя (FQDN);
* возможность настраивать антиспуфинг на сетевых интерфейсах;
* возможность сброса флага DF для транзитного трафика;
* возможность использования паттернов сканирования для обнаружения аномалий трафика и защиты от flood атак;
* возможность настраивать список параметров для детектирования атак типа DoS;
* возможность передачи файлов для анализа во внешние системы по протоколу ICAP;
* возможность ограничивать размер файлов, передаваемых на внешний ICAP-сервер;
* возможность отправлять на внешний ICAP-сервер файлы с определенным расширением или определенными mime-типами данных;
* фильтрация прикладных протоколов с использованием регулярных выражений;
* возможность работы с VoIP трафиком;
* криптографическое преобразование передаваемых и принимаемых IP-пакетов и Ethernet-кадров;
* шифрование информации на сетевом уровне (L3 модели OSI);
* поддерживаемый алгоритм шифрования – ГОСТ 34.12-2018 (Магма) в режиме гаммирования с обратной связью по шифртексту по ГОСТ 34.13-2018;
* длина ключа шифрования – 256 бит;
* алгоритм имитозащиты данных – на базе ГОСТ 34.12-2018 (Магма) в режиме выработки имитовставки;
* поддержка стандарта хеширования ГОСТ Р 34.11-2012;
* увеличение размера пакета с учетом дополнительного IP-заголовка не должно превышать 52 байт для шифрования на сетевом уровне и 70 байт для шифрования на канальном уровне;
* аутентификация удаленных пользователей посредством технологии сертификатов открытых ключей стандарта x509v3;
* сокрытие внутренней структуры защищаемого сегмента сети;
* трансляцию сетевых адресов в соответствии с заданными правилами трансляции (NAT);
* максимальная пропускная способность УБ в режиме работы “UTM” на синтетическом трафике (при включенных компонентах: фиды Касперского, IPS, расширенный контроль приложений) должна составлять 2 000 Мбит/с для комплекса № 1 и 1 000 Мбит/с для комплекса № 2;
* максимальная пропускная способность VPN на синтетическом трафике должна составлять 1 000 Мбит/с для комплекса № 1 и 350 Мбит/с для комплекса № 2;
* максимальная пропускная способность межсетевого экрана на синтетическом трафике должна составлять 8 000 Мбит/с для комплекса № 1 и 4 000 Мбит/с для комплекса № 2;
* поддержка максимум 3 000 000 одновременных stateful TCP сессий для комплекса № 1 и 1 000 000 одновременных stateful TCP сессий для комплекса № 2;
* максимальное количество подключений (удаленных пользователей) к Серверу доступа: 150 для комплекса № 1 и 50 для комплекса № 2;
* поддержка неограниченного числа туннелируемых IP адресов;
* возможность мониторинга состояния УБ из защищенных сетей с помощью средств управления объектами сети по протоколу SNMP (v2, v3);
* уведомление администратора о результате установки и соответствующих изменениях политики по SMTP;
* сбор данных о соседствующих сетевых устройствах и возможности передачи данных другим сетевым устройствам по протоколу LLDP;
* поддержка виртуальных локальных сетей VLAN (IEEE802.1Q), с возможностью создания не менее 1024 VLAN интерфейсов на один физический порт;
* возможность работы с протоколами динамической маршрутизации: OSPFv2, BGPv4;
* поддержка приоритизации трафика (QoS):
	+ обработка входящего сетевого трафика:
		- ограничение полосы пропускания.
	+ обработка исходящего сетевого трафика:
		- распределение сетевого трафика по очередям;
		- классификация сетевого трафика;
		- маркировка и перемаркировка сетевого трафика;
		- ограничение полосы пропускания.
* поддержка подключения к нескольким каналам провайдера (Multi-WAN) в режимах: отказоустойчивость канала связи, балансировка трафика и исключение (передача трафика в соответствии с таблицей маршрутизации);
* поддержка импорта сетевых объектов и правил фильтрации из файла;
* экспорт данных о потоках сетевого трафика по протоколу Netflow;
* генерация файлов конфигурации для большого количества УБ (массовое развертывание);
* импорт списка IP-адресов в каталог объектов из файла;
* возможность удаленного централизованного обновления программного обеспечения УБ;
* возможность полноценного централизованного управления УБ из ЦУС с применением групповых правил;
* отказоустойчивый кластер высокой доступности с синхронизацией состояния сессий (доступен в режимах работы “Высокопроизводительный межсетевой экран” и “UTM” (кроме компонента ЦУС):
	+ возможность назначения интерфейса синхронизации для автоматической синхронизации конфигурации элементов кластера;
	+ доступное количество узлов в кластере – 2;
	+ переключение с узла на узел в кластере не должно превышать 1 секунды;
	+ возможность назначения интерфейса резервирования сети синхронизации;
* возможность «холодного» резервирования аппаратной платформы;
* максимальное время восстановления из бэкапа (без журналов) на подготовленную систему – не более 10 минут;
* возможность использования внешней базы данных для хранения статистики мониторинга;
* возможность резервирования ЦУС:
* возможность иметь не менее 1 резервного ЦУС с автоматической синхронизацией с основным ЦУС;
* резервные ЦУС должны иметь возможность получать инкрементальное обновление базы данных с основного ЦУС;
* возможность ручной синхронизации между основным и резервным ЦУС.
* возможность дистанционного подключения по ssh для проведения диагностики и получения следующей информации:
* ресурсы сетевого устройства (загруженность процессора, свободный объем ОЗУ, объем жесткого диска);
* содержимое ARP-кэша;
* результаты выполнения команд ping и traceroute;
* информация о сетевом трафике выбранного интерфейса;
* таблица соединений УБ;
* технологический отчет для службы поддержки.
* оповещение центра управления сетью о своей активности и о событиях, требующих оперативного вмешательства в режиме реального времени;
* регистрация следующих событий, связанных с работой и управлением УБ:
* загрузка, перезагрузка, выключение;
* вход (выход) администратора в систему (из системы);
* результат фильтрации входящих/исходящих пакетов;
* попытки несанкционированного доступа;
* любые нештатные ситуации, происходящие при работе УБ;
* при регистрации события должны фиксироваться:
* дата и время регистрируемого события;
* адрес источника и адрес получателя (при фильтрации), включая порты протоколов IP, TCP, UDP;
* результат попытки осуществления регистрируемого события – успешная или неуспешная (или результат фильтрации); автоматический контроль целостности программного обеспечения УБ при перезагрузке системы;
* должна быть обеспечена отказоустойчивая работа при непрерывном круглосуточном функционировании системы;
* Программное обеспечение УБ должно представлять собой функционально замкнутую среду, не допускающую возможности внедрения вредоносного программного обеспечения;
* Программное обеспечение УБ не должно требовать установки дополнительных средств антивирусной безопасности.
	+ 1. **Требования к системе обнаружения вторжений (IPS) комплекса № 1 и № 2:**
* наличие группировки сигнатур атак по общим признакам в программе управления;
* система управления УБ обеспечивает возможность создания и модификации собственных сигнатур атак;
* возможность обработки фрагментированного сетевого трафика;
* возможность включения IPS инспекции для отдельных правил межсетевого экрана;
* сигнатурные и эвристические методы обнаружения вторжений;
* поддерживаемые методы обнаружения атак включают:
	+ обнаружение скрытых каналов утечки (туннели в сетевых протоколах);
	+ поиск инъекций SQL и shell-кодов в HTTP-трафике;
* поддерживаемые протоколы:
	+ сетевого уровня: ICMPv4, IPv4;
	+ транспортного уровня: TCP, UDP, SCTP;
	+ канального уровня: PPPoE, PPP;
	+ прикладного уровня: FTP, HTTP, SMB, SSH, SMTP;
	+ сеансового уровня: SSL, DCE/RPC;
* возможность работы с несколькими сетевыми интерфейсами;
* максимальная пропускная способность L2 IPS в режиме работы УБ “Детектор Атак” должна составлять 2 200 Мбит/с для комплекса № 1 и 900 Мбит/с для комплекса № 2;
* Возможность создания исключений для отдельной сигнатуры базы решающих правил на основе:
	+ порта источника;
	+ порта получателя;
	+ ip-адреса, диапазона адресов получателя;
	+ ip-адреса, диапазона адресов источника;
* УБ обеспечивает работу двух режимов обновления базы сигнатур:
	+ вручную администратором;
	+ автоматически по расписанию;
* поддержка импорта пользовательских сигнатур из файла;
* УБ взаимодействует с единой системой аудита событий информационной безопасности;
* УБ обеспечивает уведомления администратора системы о событиях двумя доступными методами:
	+ уведомление на консоль администратора;
	+ отправка письма по электронной почте.
		1. **Требования к контролю приложений (DPI) комплекса № 1 и № 2:**
* расширенный контроль приложений - поддержка более 4000 приложений и сервисов;
* возможность централизованного обновления баз приложений без остановки работы УБ.
	+ 1. **Требование к GeoIP комплекса № 1 и № 2:**
* возможность использования сетевого объекта типа «Страна» в правилах фильтрации;
* возможность создавать группы сетевых объектов типа «Страна»;
* возможность централизованного обновления базы объектов типа «Страна» с сервера обновлений.
	+ 1. **Требование к потоковому антивирусу комплекса № 1 и № 2:**
* возможность анализа трафика по хэшам на наличие вредоносных файлов;
* возможность ограничивать размер файлов, передаваемых антивирусу на проверку;
* сканирование исходящих веб-запросов или вложений веб-почты, перед отправкой их на файловые серверы;
* сканирование входящих клиентских запросов на наличие вредоносного содержимого;
* возможность фильтровать тип проверяемого контента с использованием встроенных MIME-типов данных или указанием расширения файлов;
* возможность обновления базы хэшей вредоносных файлов;
* возможность блокировки доступа к вредоносным сайтам из базы Kaspersky Feed.
	+ 1. **Требования к категориям URL комплекса № 1 и № 2:**
* обеспечивать фильтрацию доступа пользователей на основе категорий веб-сайтов;
* возможность обновления базы категорий веб-сайтов с сервера обновлений;
* возможность объединения категорий веб-сайтов в группы.
	+ 1. **Требования к сертификации комплекса № 1 и № 2:**
* платформа должна входить в реестр телекоммуникационного оборудования российского производства (ТОРП);
* должен соответствовать «Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) по 4 уровню доверия;
* должен соответствовать «Требованиям к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ»;
* должен соответствовать «Требованиям к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ»;
* должно подтверждаться действующими сертификатами ФСТЭК России.
	+ 1. **Требования к технической поддержке комплекса**

На все поставляемые комплексы должна распространятся техническая поддержка производителя, включающая:

* + - доступность услуги технической поддержки 24х7: портал самообслуживания, Е-mail;
		- самостоятельная регистрация и контроль обращений через портал самообслуживания производителя;
		- работа над инцидентами в режиме 8х5 (рабочие дни МСК 10:00-18:00);
		- консультирование по установке и использованию продукта;
		- информирование о доступных обновлениях по запросу;
		- доступ к пакетам обновлений продукта;
		- доступ к Базе знаний (известные ошибки и типовые решения);
		- доступ на форум по продукту;
		- прием предложений по улучшению продукта;
		- срок действия технической поддержки 1 (один) год с даты поставке комплекса.
		1. **Требования к поставке комплекса**

Поставляемые комплексы должны быть новыми (не бывшими в употреблении, не проходившими ремонт, в том числе восстановление, замену составных частей, восстановление потребительских свойств), собраны из новых комплектующих, должны быть серийными или состоять из серийно выпускаемых компонентов, не должны иметь дефектов, связанных с конструкцией, материалами или работой по их изготовлению, либо проявляющихся в результате действия или упущения производителя и/или Поставщика, при соблюдении Заказчиком правил эксплуатации поставляемых комплексов.

Все комплексы должны поставляться в заводской упаковке, обеспечивающей безопасность транспортировки комплекса и сохранность его качества в течение гарантийного срока хранения.

* + 1. **Требования к гарантии на комплекс**

Гарантийный срок на все поставляемые комплексы должен составлять 1 (один) год с даты поставке комплексов.

В течение всего срока предоставления гарантии:

Поставщик гарантирует соответствие показателей качества комплекса его паспортным данным, бесперебойную работу, надежность функционирования, сохранение требуемых свойств и пригодности комплекса к использованию.

Поставщик гарантирует, что Изготовитель безвозмездно устраняет дефекты комплекса при условии соблюдения потребителем правил и условий хранения, транспортировки, монтажа, установки и эксплуатации.

Срок нахождения изделия в сервисном центре для проведения ремонтных работ может составлять не более 15 (пятнадцати) рабочих дней без учета времени доставки и при наличии комплектующих.

Поставщик гарантирует соответствие показателей качества и надежности функционирования комплекса описанию объекта закупки, сохранение его требуемых свойств.

В рамках пакета услуг гарантийного обслуживания Поставщик гарантирует, что Изготовитель принимает претензии, как от авторизованных партнеров – поставщиков изделий, так и от заказчиков – конечных пользователей. Пользователь с претензиями и запросами на услуги гарантийного обслуживания может обращаться как к своему поставщику, который передает заявку на рассмотрение и обработку изготовителю, так и напрямую к Изготовителю.

Выполнение гарантийных обязательств должно осуществляться сервисными центрами, авторизованными производителями поставляемого комплекса.

На весь период гарантийного срока эксплуатации все необходимые работы по транспортировке комплекса до сервисных центров осуществляется силами Поставщика и за его счёт.

* + 1. **Требования к установке и настройке комплекса**

Комплекс должен быть установлен и настроен в инфраструктуре Заказчика.

Поставщик выполняет работы по установке, настройке комплекса в количестве указанном в пункте 2.1. настоящего технического задания. Поставщик должен обеспечить стабильную работу комплекса с имеющимся у Заказчика программным и аппаратным обеспечением, средствами маршрутизации сети, а также произвести по согласованию с Заказчиком установку и настройку политик безопасности на комплексе.

Адреса установки:

* г. Уфа, ул. Степана Злобина, д. 31/4;
* г. Уфа, ул. Ухтомского, д. 26/1;
* г. Уфа, ул. Софьи Перовской, д.13/2;
* г. Уфа, ул. Красина, д. 21/1;
* г. Уфа, ул. Комсомольская, 2;
	1. **Поставка интеллектуального межсетевого экрана уровня приложений. Установка и настройка.**

Интеллектуальный межсетевой экран уровня приложений (далее - ИМЭ), должен быть выполнен в виде законченного аппаратно-программного комплекса, с предварительно установленным программным обеспечением и встроенной операционной системой Linux.

Количество поставляемых ИМЭ - 1 (одна) шт.

# ИМЭ должен осуществлять:

* защиту от основных видов атак на веб-приложения из перечня OWASP Top 10;
* защиту от логических атак на приложения, в том числе от атак на механизмы аутентификации и контроля сессий и атак на бизнес-логику;
* эффективную защиту от ложных срабатываний при выявлении аномалий;
* поддержку распределенных, масштабируемых конфигураций с выделенными узлами анализа и узлами управления;
* централизованное управление всеми узлами ИМЭ.
	+ 1. **Требования к аппаратной части ИМЭ:**
* исполнение: для установки в монтажную стойку, высота не более 1U;
* наличие крепежного комплекта для установки в монтажный шкаф 19'';
* не менее двух процессоров Intel Xeon E5-2680v4;
* не менее 8х16Гб оперативной памяти;
* не менее 1 (одного) сетевого интерфейса в конфигурации:
* 10/100/1000BASE-T Gigabit Ethernet, с разъемами RJ45 UTP;
* 1 х модуль NCS2-IXM407 (4 порта 10 ГБ SPF);
* не менее 1 (одного) дискового накопителя SATA, объемом не менее 480 Гб;
* не менее 2 (двух) портов USB 2.0;
* не менее 1 (одного) видео порта VGA;
* не менее 1 (одного) последовательного (COM) порта с разъёмом RJ45;
* не менее 1 (одного) встроенного считывателя Touch Memory;
* не менее 2 (двух) персональных идентификатора Touch Memory iButton DS1992L;
* потребляемая мощность не более 300 Вт;
* не менее 2 (двух) блоков питания с поддержкой функции горячей замены (hot swap);
* шнур питания европейского стандарта длиной не менее 1 метра.

# Функциональные особенности ИМЭ:

* основные функции системы:
* защита от основных видов атак на веб-приложения из перечня OWASP Top 10;
* защита от логических атак на приложения, в том числе от атак на механизмы аутентификации и контроля сессий и атак на бизнес-логику.
* интерфейс управления:
* управление осуществляется по протоколу HTTP с использованием специализированного ВЕБ-интерфейса;
* в целях интеграции с другими решениями, управление может осуществляться также с использованием REST API;
* поддержка технологии асинхронного взаимодействия с системой управления (имитация «толстого клиента»);
* обеспечение возможности мониторинга и управления конфигурациями для нескольких защищаемых приложений из общего интерфейса;
* поддержка графического отображение и редактирование моделей нормального функционирования защищаемых приложений;
* веб-интерфейс обеспечивает версионность конфигурационных настроек системы: в т.ч. базовых конфигурационных настроек, настроек модулей анализа, моделей нормального функционирования приложений, правил принятия решений;
* интерфейс поддерживает механизмы аутентификации и авторизации пользователей. Ролевая модель должна предусматривать разграничение доступа для трех групп: администраторы (можно выполнять любые действия), аналитики (можно менять только настройки безопасности), операторы (только мониторинг и работа с событиями безопасности);
* действия пользователей веб-интерфейса, включая внесенные изменения, сохраняются во внутреннем журнале аудита системы.
* работа с использованием сигнатурного метода:
* наличие набора встроенных сигнатур в комплекте поставки;
* поддержка распространенного открытого формата веб-сигнатур ModSecurity;
* семантический анализ передаваемых данных;
* работа на основе позитивных моделей приложения:
* возможность гибкой настройки различных типов моделей для каждого из защищаемых приложений, в том числе:
* модели валидации протокола HTTP;
* модели синтаксического анализа запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с различными уровнями вложенности (в частности, XML, JSON, BASE64, GZIP);
* модели определения бизнес-действий в приложении, параметров бизнес-действий и их значений;
* модели пользователей, их идентификации, аутентификации и контроля сессий;
* наличие готовых моделей валидации протокола HTTP и синтаксического анализа запросов для типового веб-приложения в комплекте поставки;
* возможность разделения запросов к статическому и динамическому контенту на основе анализа заголовков и статистических моделей для минимизации времени обработки статического контента, а также экономии ресурсов, требуемых аналитику для разбора событий (запросы к статическим ресурсам не отображаются в консоли мониторинга);
* наличие алгоритма оценки отклонения числовых параметров действий веб-приложения от статистической нормы.
* обнаружение аномалий и значимых событий:
* возможность обнаружения аномалий или значимых данных как в HTTP-запросах, так и в HTTP-ответах;
* возможность обнаружения аномалий работы приложения на основе сопоставления значений параметров HTTP запросов/ответов с сигнатурами атак;
* возможность обнаружения аномалий или значимых данных в работе приложения на основе настроенных позитивных моделей приложения (совпадение с моделью или наоборот – отклонение от нее);
* обнаружение аномалий и значимых параметров непосредственно внутри вложенных данных, передаваемых по протоколу HTTP без ограничений на количество уровней вложенности;
* возможность обнаружения аномалий, свидетельствующих о возможных попытках атак, осуществляемых «методом грубой силы» (bruteforce);
* возможность обнаружения аномалий или значимых данных в процессе работы механизмов идентификации, аутентификации, авторизации пользователей и контроля пользовательских сессий;
* возможность обнаружения аномалий нарушения бизнес-логики приложения или контроля выполнения бизнес-логики путем использования соответствующей позитивной модели работы приложения.
* подавление ложных срабатываний:
* наличие механизма предварительного ("раннего") подавления ложных срабатываний, чтобы исключить возможность их влияния на сформированные правила принятия решений;
* наличие функции упрощенного ("быстрого") подавления ложных срабатываний оператором ИМЭ непосредственно при просмотре описания выявленной аномалии;
* возможность тонкой настройки подавления ложных срабатываний различных механизмов определения аномалий в привязке к отдельным параметрам запроса/ответа или бизнес-действиям.
* наличие автоматического алгоритма выявления сигнатурных правил с высоким уровнем ложных срабатываний.
* принятие решений
* наличие настраиваемого модуля принятия решений, позволяющего выделять значимые события информационной безопасности и принимать решения относительно дальнейших действий в отношении http-транзакций (запрос/ответ);
* управление правилами принятия решений на основе данных об источнике (ip-адрес, пользователь, id сессии) и цели httр-транзакции (приложение, бизнес-действие), а также обнаруженных в ней аномалиях или значимых данных;
* поддерживаются следующие возможные решения: блокировать http-транзакцию, пропустить http-транзакцию, пометить http-транзакцию, модифицировать ответ;
* управление правилами принятия решений (создание, удаление, перегруппировка) с помощью графического конфигуратора через интерфейс управления.
* мониторинг и аудит событий информационной безопасности
* должна выводиться обобщенная статистика по следующим параметрам: статусы HTTP ответа сервера, текущей пропускной способности (входящий/исходящий трафик), задержки обработки запросов приложением, уровня враждебности среды;
* сообщения об обнаруженных и/или заблокированных атаках на приложения должны выводиться в агрегированном виде, агрегация должна происходить по приложениям, типам обнаруженных аномалий и времени возникновения аномалий;
* для событий безопасности должна агрегироваться информация об источниках атак, в том числе по географическому распределению источников по странам, по номерам автономных систем;
* возможность автоматического оповещения пользователей системы о событиях безопасности с использованием электронной почты, гибкая настройка оповещений из ВЕБ-интерфейса;
* возможность автоматической генерации отчетов в формате PDF, содержащих статистику событий информационной безопасности за заданные промежутки времени, в том числе периодические отчеты с периодичностью «раз в сутки», «раз в неделю», «раз в месяц»;
* возможность передачи данных в режиме реального времени в систему мониторинга и корреляции событий информационной безопасности (SIEM).

# Архитектурные особенности ИМЭ

* вариант поставки:
* программно-аппаратный комплекс с заданными характеристиками.
* встраивание в корпоративную инфраструктуру доставки приложений:
* поддержка централизованного управления узлами ИМЭ;
* поддержка конфигураций с установкой узла анализа и системы управления на одном физическом устройстве;
* поддержка распределенных, масштабируемых конфигураций с разделенными узлами анализа и управления;
* возможность работы в качестве типового модуля для Nginx (предоставление вердиктов), типового модуля для Suricata
* возможность работы узлов анализа и систем управления одновременно с несколькими защищаемыми приложениями;
* поддержка интеграции с корпоративной инфраструктурой доставки приложений: с внешними балансировщиками, SSL-концентраторами и т.п.
* возможность балансировки трафика и терминирования SSL непосредственно на узле анализатора ИМЭ.
* **режимы работы:**
* возможность работы узлов анализа в активном режиме с возможностью блокировки запросов/ответов (режим reverse proxy) с возможностью временного быстрого включения или выключения режима блокировки;
* возможность работы узлов анализа в пассивном режиме с возможностью мониторинга без влияния на анализируемый трафик;
* возможность работы узлов анализа в автономном режиме, при котором данные о транзакциях загружаются из лог-файла веб-сервера или по протоколу pcap;
* возможность работы узлов анализа в гибридном режиме, с поддержкой как активного, так и пассивного режимов на одном узле анализа для различных приложений.
* **отказоустойчивость:**
* возможность построения кластерных конфигураций active-active или active-passive для узлов анализа, active-passive с репликацией для системы управления;
* поддержка программного режима «bypass» и выполнения действия по умолчанию без проверки в случае локальных сбоев или резких скачков нагрузки.
* **интеграция с внешними системами:**
* возможность интеграции с другими системами с использованием механизмов syslog, SNMP, SQL, REST API.
	+ 1. **Требования к технической поддержке ИМЭ**

На поставляемый ИМЭ должна распространятся техническая поддержка производителя, включающая:

* + - доступность услуги технической поддержки 24х7: портал самообслуживания, Е-mail;
		- самостоятельная регистрация и контроль обращений через портал самообслуживания производителя;
		- работа над инцидентами в режиме 8х5 (рабочие дни МСК 10:00-18:00);
		- консультирование по установке и использованию продукта;
		- информирование о доступных обновлениях по запросу;
		- доступ к пакетам обновлений продукта;
		- доступ к Базе знаний (известные ошибки и типовые решения);
		- доступ на форум по продукту;
		- прием предложений по улучшению продукта;
		- срок действия технической поддержки 1 (один) год с даты поставке комплекса.
		1. **Требования к поставке ИМЭ**

Поставляемый ИМЭ должен быть новым (не бывшим в употреблении, не проходившим ремонт, в том числе восстановление, замену составных частей, восстановление потребительских свойств), собран из новых комплектующих, должен быть серийным или состоять из серийно выпускаемых компонентов, не должен иметь дефектов, связанных с конструкцией, материалами или работой по их изготовлению, либо проявляющихся в результате действия или упущения производителя и/или Поставщика, при соблюдении Заказчиком правил эксплуатации поставляемого ИМЭ.

ИМЭ должен поставляться в заводской упаковке, обеспечивающей безопасность транспортировки ИМЭ и сохранность его качества в течение гарантийного срока хранения.

* + 1. **Требования к гарантии на ИМЭ**

Гарантийный срок на ИМЭ должен составлять 1 (один) год с даты поставке ИМЭ.

В течение всего срока предоставления гарантии:

Поставщик гарантирует соответствие показателей качества ИМЭ его паспортным данным, бесперебойную работу, надежность функционирования, сохранение требуемых свойств и пригодности ИМЭ к использованию.

Поставщик гарантирует, что Изготовитель безвозмездно устраняет дефекты ИМЭ при условии соблюдения потребителем правил и условий хранения, транспортировки, монтажа, установки и эксплуатации.

Срок нахождения изделия в сервисном центре для проведения ремонтных работ может составлять не более 15 (пятнадцати) рабочих дней без учета времени доставки и при наличии комплектующих.

Поставщик гарантирует соответствие показателей качества и надежности функционирования ИМЭ описанию объекта закупки, сохранение его требуемых свойств.

В рамках пакета услуг гарантийного обслуживания Поставщик гарантирует, что Изготовитель принимает претензии, как от авторизованных партнеров – поставщиков изделий, так и от заказчиков – конечных пользователей. Пользователь с претензиями и запросами на услуги гарантийного обслуживания может обращаться как к своему поставщику, который передает заявку на рассмотрение и обработку изготовителю, так и напрямую к Изготовителю.

Выполнение гарантийных обязательств должно осуществляться сервисными центрами, авторизованными производителями поставляемого ИМЭ.

На весь период гарантийного срока эксплуатации все необходимые работы по транспортировке ИМЭ до сервисных центров осуществляется силами Поставщика и за его счёт.

* + 1. **Требования к установке и настройке ИМЭ**

ИМЭ должен быть установлен и настроен в инфраструктуре Заказчика.

Поставщик выполняет работы по установке, настройке ИМЭ в количестве указанном в пункте 2.2. настоящего технического задания. Поставщик должен обеспечить стабильную работу ИМЭ с имеющимся у Заказчика программным и аппаратным обеспечением, средствами маршрутизации сети, а также произвести по согласованию с Заказчиком установку и настройку политик безопасности на ИМЭ.

Адрес установки:

* Республика Башкортостан, г. Уфа, ул. Степана Злобина, д. 31/4;
1. **Предоставить и установить средства криптографической защиты информации для ViPNet сети № 11765**

|  |  |  |
| --- | --- | --- |
| **№** **п/п** | **Наименование** | **Количество** |
|  | ПО ViPNet Client for Windows 4.х (КС2)  | 70 |

Поставка эквивалента не допускается в связи с необходимостью обеспечения взаимодействия с программным обеспечением, используемым Заказчиком.

Исполнитель должен выполнить установку и настройку поставляемых средств криптографической защиты информации в рамках пункта 2.9. технического задания.

Поставляемые программные средства криптографической защиты настраиваются Исполнителем в соответствии с параметрами защищённой сети ViPNet с номером 11765, действующей в МУП УИС.

Адрес установки:

* Республика Башкортостан, г. Уфа, ул. Степана Злобина, д. 31/4.
1. **Предоставить сертификат активации сервиса совместной технической поддержки программного обеспечения и программно-аппаратного комплекса ViPNet сети № 11765 на срок 12 месяцев, уровень – Расширенный**

|  |  |  |
| --- | --- | --- |
| **№** **п/п** | **Наименование** | **Количество** |
| 1 | ПО ViPNet Administrator 4.х (КС2)  | 1 |
| 2 | ПАК ViPNet Coordinator HW 1000 4.x | 2 |
| 3 | ПАК ViPNet Coordinator HW 1000 C 4.x | 2 |
| 4 | ПАК ViPNet Coordinator HW100 C 4.x (+unlim)  | 7 |
| 5 | ПО ViPNet Client for Windows 4.х (КС2)  | 111 |

Поставка эквивалента не допускается в связи с необходимостью обеспечения взаимодействия с программным обеспечением, используемым Заказчиком.

Сертификат активации должен содержать следующую информацию: перечень продуктов ViPNet на которые сертификат распространяется, включая наименование продукта, количество лицензий/оборудования, номер сети.

Сертификат активации сервиса совместной технической поддержки предоставляет возможность получать в течение действия срока сертификата (12 месяцев):

* Прием запросов через web-форму с сайта Производителя;
* Приём обращений и консультирование по электронной почте в рабочие дни с 9:00 до 18:00 МСК;
* Приём обращений и консультирование по телефону горячей линии в рабочие дни с 9:00 до 18:00 МСК;
* Рекомендации по процессу установки продукта в объеме эксплуатационной документации;
* Рекомендации по настройке продукта в объеме эксплуатационной документации;
* Исполнитель предоставляет обновление (hotfix), устраняющее дефекты, выявленные в продукте;
* Исполнитель предоставляет обновление (hotfix), а также все изменения, производимые в рамках минорной (MINOR) версии продукта (service pack);
* Исполнитель предоставляет новые версии (изменение мажорной (MAJOR) версии, поколения) продукта без взимания дополнительной платы (для ПАК – только программные компоненты);
* Восстановление работоспособности (ремонт) вышедшего из строя оборудования (аппаратной платформы ПАК) из состава Продуктов Пользователя в соответствии с гарантийными обязательствами ОАО «ИнфоТеКС». Доставка не входит в стоимость.
1. **Предоставить ключ активации сервиса совместной технической поддержки уровня «Стандартный» для СЗИ Secret Net Studio**

|  |  |  |
| --- | --- | --- |
| **№** **п/п** | **Наименование** | **Количество**  |
| 1 | Ключ активации сервиса совместной технической поддержки уровня «Стандартный» для СЗИ Secret Net Studio сроком 12 месяцев | 364 |

Поставка эквивалента не допускается в связи с необходимостью обеспечения взаимодействия с программным обеспечением, используемым Заказчиком.

Ключ активации должен содержать следующую информацию: уровень обслуживания, срок действия услуги, ключ активации технической поддержки, количество экземпляров продукта для поддержки.

Срок действия поставляемого ключа активации должен продлевать срок действия предыдущей технической поддержки на срок не менее 12 месяцев.

В соответствии с ключом активации сервиса совместной технической поддержки уровня «Стандартный» служба технической поддержки обеспечивает:

* доступность услуги технической поддержки 24х7: портал самообслуживания, e-mail;
* самостоятельную регистрацию и контроль обращений через портал самообслуживания;
* работу над инцидентами в режиме 8х5 (рабочие дни МСК 10:00–18:00);
* консультирование по установке и использованию продукта;
* информирование о доступных обновлениях продукта по запросу;
* доступ к пакетам обновлений продукта (при обеспечении непрерывности поддержки);
* доступ к базе знаний (известные ошибки и типовые решения);
* прием предложений по улучшению продукта.

Срок действия сертификата ключа активации сервиса совместной технической поддержки уровня «Стандартный» для СЗИ Secret Net Studio: с 01 февраля 2023 по 31 января 2024 г. (необходимость обеспечения непрерывной технической поддержки).

1. **Предоставить право на получение технической поддержки «КИБ Серчинформ»**

|  |  |  |
| --- | --- | --- |
| **№** **п/п** | **Наименование** | **Количество** |
| 1 | Предоставить право на получение технической поддержки «КИБ Серчинформ», гарантийные обязательства в течение 1 года | 10 |

Поставка эквивалента не допускается в связи с необходимостью обеспечения взаимодействия с программным обеспечением, используемым Заказчиком.

Техническая поддержка осуществляется в рабочие дни с 09.00 до 18.00 МСК по телефону и e-mail.

В соответствии с правом на получение технической поддержки служба технической поддержки обеспечивает:

* помощь в установке продукта;
* консультирование по вопросам настройки программы;
* консультирование по вопросам эксплуатации клиентских приложений продукта;
* консультирование по вопросам анализа перехваченной информации;
* предоставление информации по новым версиям;
* консультирование по работе новых версий;
* постановка задач и планирование работы с инженером технической поддержки в случае возникновения проблем в работе продукта;
* помощь при возникновении проблем в работе продукта.
1. **Предоставить право на сопровождение по информационной безопасности (далее - Услуга)**

Услуга оказываются в течение 12 (двенадцати) месяцев с даты подписания универсального передаточного документа в объеме указанном в таблице:

| **№ п/п** | **Наименование услуг/этапа** | **Содержание/результаты этапа** | **Периодичность/****территория исполнения** |
| --- | --- | --- | --- |
|  | Разработка, контроль утверждения, актуализация, в случае изменения законодательства РФ, организационно-распорядительных документов (далее – ОРД) по безопасности информационных систем персональных данных (далее – ИСПДн). | Актуальный комплект документов ИСПДн;Акт по результатам контроля. | Не более 2 (двух) раз в 3 (три) месяца с начала действия договора, сопровождается выездом представителя Исполнителя на территорию Заказчика. |
|  | Сверка утвержденных документов с перечнем предоставленных ранее проектов документов. | Акт сверки.В случае отсутствия утвержденных документов передача их в электронном виде официальным письмом на имя начальника отдела безопасности. | Не более 2 (двух) раз в 3 (три) месяца с начала действия договора, сопровождается выездом представителя Исполнителя на территорию Заказчика. |
|  | Сопровождение аттестованных ИСПДн.Исполнитель проверяет в отношении ИСПДн следующее:* наличие и актуальность установленных средств защиты информации и средств криптографической защиты информации;
* соответствие настроек средств защиты информации и уровню защищенности и актуальным угрозам безопасности информации;
* наличие дистрибутивов и формуляров средств защиты информации и средств криптографической защиты информации;
* наличие и актуальность технической и аттестационной документации на аттестованные системы.
 | Заключение о соответствии или несоответствии:* оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных;
* акт оценки эффективности.
 | Не более 1 (одного) раза за период действия договора. |
|  | Формирование предложений по совершенствованию функционирования систем безопасности. | Предложение по совершенствованию функционирования систем безопасности, на основании частного технического задания. | Не более 3 (трех) раз за период действия договора, при внесении изменений в законодательство или при вводе в эксплуатацию новых ИСПДн. |
|  | Ознакомление работников Заказчика, непосредственно осуществляющих обработку персональных данных (далее – ПДн), с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн. | Очные инструктажи.Информационная рассылка.Заполнение и выдача:* журнала ознакомления работников с положениями законодательства РФ по ПДн;
* заключение о допуске к самостоятельной работе с средствами криптографической защиты информации (далее –СКЗИ).
 | Очные инструктажи проводятся не менее 1 (одного) раза в 3 (три) месяца с начала действия договора, сопровождаются выездом представителя Исполнителя на территорию Заказчика, заполнением журнала ознакомления работников с положениями законодательства РФ по ПДн (при тематике очного инструктажа о ПДн) и/или Заключение о допуске к самостоятельной работе с СКЗИ (при тематике очного инструктажа о правилах эксплуатации СКЗИ). |
|  | Проведение аудита соответствия на выполнение требований 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 (инструкция ФАПСИ №152 от 13 июня 2001г.). | Заключение по результатам аудита.Выдача рекомендаций по устранению выявленных недочетов.Оказание помощи в устранении недочетов. | Не более 4 (четырех) раз за период действия договора, сопровождается выездом представителя Исполнителя на территорию Заказчика. |
|  | Проведение аудита соответствия на выполнение требований положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (Постановление правительства № 678 от 15 сентября 2008г.). | Выдача заключения по результатам аудита.Выдача рекомендаций по устранению выявленных недочетов.Оказание помощи в устранении недочетов. | Не более 4 (четырех) раз за период действия договора, сопровождается выездом представителя Исполнителя на территорию Заказчика. |
|  | Сопровождение органа криптографической защиты Заказчика в части:поэкземплярного учета используемых СКЗИ, эксплуатационной и технической документации к ним. | Заполнения учетных журналов:* журнал поэкземплярного учета СКЗИ;
* журнал учета лицевых счетов пользователей СКЗИ.
 | По мере необходимости, за период действия договора, сопровождается выездом представителя Исполнителя на территорию Заказчика. |
|  | Консультирование ИТ-специалистов по общим вопросам информационной безопасности. | Консультирование в ходе выезда, по телефону или электронной почте. | Очное консультирование проводится не более 2 (двух) раз в 3 (три) месяца за период действия договора, сопровождается выездом представителя Исполнителя на территорию Заказчика.Консультирование с применением информационно-телекоммуникационных технологий и (или) телефонной связи проводится в рабочие дни с 9:00 до 18:00 по Уфимскому времени. |
|  | Реагирование на инциденты информационной безопасности ИСПДн/СКЗИ. | Участие в анализе причин инцидента и сборе данных.Выдача рекомендаций по предотвращению повторного возникновения инцидента ИБ.Проведение очного инструктажа с сотрудниками по теме инцидента. | Услуга оказывается при возникновении инцидента информационной безопасности.Услуга осуществляется на территории Исполнителя. |
|  | Анализ защищенности информационных систем. | Предоставление отчета об инструментальном анализе защищенности, содержащий перечень выявленных уязвимостей и описание угроз, возможных для реализации посредством эксплуатации выявленных уязвимостей. | Проводится не менее 1 (одного) раза в месяц с начала действия договора, с использованием средств анализа защищенности Заказчика и (или) Исполнителя, сопровождается выездом представителя Исполнителя на территорию Заказчика. |
|  | Техническое обслуживание используемых у Заказчика средств защиты информации и средств криптографической защиты информации, в том числе:* средств защиты от несанкционированного доступа;
* средств антивирусной защиты;
* средств предотвращения утечки информации (DLP-система);
* средств анализа защищенности;
* средств криптографической защиты информации.
 | Установка, настройка, обновление (дистрибутивы с новыми версиями или пакетами обновлений предоставляются Заказчиком) средств защиты информации и средств криптографической защиты информации.  | Услуга оказывается без ограничения по временис применением информационно-телекоммуникационных технологий или с выездом представителя Исполнителя на территорию Заказчика, предоставляется в рабочие дни с 9:00 до 18:00 по Уфимскому времени. |
|  | Участие в проверках контролирующих органов (ФСБ, ФСТЭК, Роскомнадзор). | Устранение замечаний в документах по информационной безопасности и настройках средств защиты информации и средств криптографической защиты информации. | По мере необходимости, за период действия договора, сопровождается выездом представителя Исполнителя на территорию Заказчика. В адрес Исполнителя не позднее 3 (трех) рабочих дней уведомить о предстоящей проверки.  |

Перечень ИСПДн:

* «1С: Управление сбытом тепловой энергии»;
* «1С: Зарплата и Управление персоналом»;
* «1С: Документооборот»;
* «CallCenter»;
* «Финансовая система».

Требования к порядку оказания услуги:

* Исполнитель должен обеспечить прием звонков по многоканальному номеру телефонной связи (номер телефона), по e-mail (адрес e-mail) в следующем режиме: с 09:00 до 18:00 часов по Уфимскому времени ежедневно (кроме субботы, воскресения и праздничных дней).
* При формировании и обработке Обращений Заказчика должны использоваться следующие приоритеты Обращений:
* высокий − в случае если вследствие ошибки/сбоя функционирования компонентов информационных систем выявлена недоступность или неправильная работа функций средств защиты информации, препятствующая работе нескольких пользователей с прикладным программным обеспечением; в случае обнаружения нарушений в работе средств защиты информации, следов проникновения в информационные системы злоумышленников, вредоносного программного обеспечения; необходимости удаления пользователей из информационных систем;
* средний − в случае если недоступность или неправильная работа компонентов информационных систем препятствует работе только одного Пользователя с прикладным программным обеспечением; в случае необходимости допуска новых сотрудников к работе в информационных системах;
* низкий − если ошибки, недостатки в работе информационных систем не препятствуют работе Пользователей, но снижают ее эффективность или затрудняют использование компонентов информационных систем; другие обращения.
* Исполнитель должен обеспечить регистрацию всех Обращений Заказчика, поступивших по специально выделенному e-mail и Help Desk. Программное обеспечение Help Desk предоставляется Исполнителем.
	1. **Требования к разработке частной модели угроз безопасности персональных данных при их обработке в ИСПДн**

Угрозы безопасности информации определяются Исполнителем по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

В качестве исходных данных для определения угроз безопасности информации Исполнитель должен использовать банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

При определении угроз безопасности информации Исполнитель должен учитывать структурно-функциональные характеристики ИСПДн, включающие структуру и состав ИСПДн, физические, логические, функциональные и технологические взаимосвязи между сегментами ИСПДн, с иными ИСПДн и информационно-телекоммуникационными сетями, режимы обработки информации в ИСПДн и в ее отдельных сегментах, а также иные характеристики ИСПДн, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации Исполнителем при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик ИСПДн, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание ИСПДн и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСПДн, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Перечень ИСПДн:

* «1С: Управление сбытом тепловой энергии»;
* «1С: Зарплата и Управление персоналом»;
* «1С: Документооборот»;
* «CallCenter»;
* «Финансовая система».
	1. Требования к разработке частного технического задания на создание системы обеспечения информационной безопасности

Разрабатываемый документ должен учитывать перечень актуальных угроз безопасности информации Модели угроз безопасности ПДн.

Техническое задание на создание системы защиты информации должно содержать:

* исходные данные, описывающие существующие у Заказчика ИСПДн, их характеристики и количество обрабатываемой информации;
* перечень применяемых программных средств и информационных технологий;
* перечень технических средств, их размещение относительно контролируемой зоны;
* информационные потоки;
* описание технологических процессов обработки данных по каждой информационной системе;
* определение требуемых уровней защищенности;
* общие требования, предъявляемые к системе защиты информации информационных систем;
* перечень необходимых мер защиты, которые должна реализовывать система защиты информации информационных систем;
* перечень предполагаемых к использованию средств защиты информации.
	1. **Требования к разработке технического проекта на создание системы обеспечения информационной безопасности**

Технический проект Исполнитель обязан разработать, с учетом частного технического задания, требования совместимости выбираемых проектных решений со средствами и системами защиты информации для управления информационной безопасностью МУП УИС.

В результате выполнения работ по данному этапу исполнитель обязан разработать следующие документы технического проекта на создание системы обеспечения информационной безопасности:

* ведомость технического проекта;
* описание комплекса технических средств;
* ведомость покупных изделий;
* пояснительная записка к техническому проекту, содержащая:
* общие описание системы обеспечения информационной безопасности;
* структурная и функциональная схема системы обеспечения информационной безопасности;
* схема функциональной структуры;
* спецификация оборудования и материалов;
* требования к местам размещения средств защиты информации и средств криптографической защиты информации, входящих в состав и обеспечивающих функционирование системы обеспечения информационной безопасности МУП УИС.
	1. **Срок оказания услуг и выполнение работ**

В течение 60 рабочих дней со дня подписания Договора. Период оказания услуг по сертификату: в течение 12 (двенадцати) календарных месяцев.

1. **Требования к оказываемым услугам и выполняемым работам**

Оказание услуг и выполнение работ по обеспечению информационной безопасности проводить в соответствии с требованиями действующих Законов, Положений, Инструкций, Методик, Стандартов, ГОСТ и других, действующих законодательных и нормативно-технических документов на соответствие требованиям безопасности информации:

* Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Указ Президента Российской Федерации от 06.03.97 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
* Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
* Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Приказ 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»;
* Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
* «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК РФ 15 февраля 2008 г.);
* Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
* Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
* «Методика оценки угроз безопасности информации» Утверждена ФСТЭК России от 5 февраля 2021 года;
* Банк данных угроз безопасности информации (bdu.fstec.ru).
1. **Места оказания услуг и выполнения работ**
* Управление - г. Уфа, ул. Степана Злобина, д. 31/4;
* АВС - г. Уфа, ул. Степана Злобина, д. 31/4а;
* АТЦ - г. Уфа, ул. Степана Злобина, 31/4;
* СВХР - г. Уфа, ул. Генерала Горбатова, 7/1;
* ЛМиС - г. Уфа, ул. Генерала Горбатова, 7/1;
* Служба сбыта - г. Уфа, ул. Комсомольская, д. 2;
* Демское управление - г. Уфа, ул. Ухтомского, д. 26/1;
* Кировское управление – г. Уфа, ул. Софьи Перовской, д.13/2;
* Ленинское управление - г. Уфа, ул. Красина, д. 21/1;
* Советское управление - г. Уфа, ул. Комсомольская, д. 18/1.
1. **Требования к гарантийному сопровождению и объему предоставления гарантий качества работ**

Исполнитель гарантирует качество выполнения услуг и работ. Исполнитель несет ответственность за недостатки, обнаруженные в пределах гарантийного сопровождения с момента подписания универсального передаточного документа (УПД) Заказчиком.

Исполнитель обязан безвозмездно устранить недостатки в течение гарантийного сопровождения в согласованный с Заказчиком срок, в случаях если:

* Качество выполненных работ не соответствует требованиям данного Технического задания (описания объекта закупки) или требованиям законодательства, государственным нормам, правилам или стандартам;
* Работы выполнены Исполнителем с отступлениями от требований нормативных документов.

Действие гарантийного сопровождения продлевается эквивалентно времени, прошедшему со дня письменного уведомления Заказчика об обнаружении недостатков до письменного уведомления Исполнителя об их устранении.

Срок гарантийного сопровождения составляет 12 месяцев с подписания УПД**.**

1. **Требования к исполнителю**

1) действующая лицензия, выданная Федеральной службой по техническому и экспортному контролю в соответствии с Постановлением Правительства РФ от 03 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» на осуществление деятельности по технической защите конфиденциальной информации, с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:

* контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

**или**

* услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

**либо**

выписка из реестра лицензий, на осуществление деятельности по технической защите конфиденциальной информации, с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:

* контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

**или**

* услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
* услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

**и**

2) действующая лицензия, выданная Федеральной службой безопасности в соответствии с Постановлением Правительства РФ от 16 апреля 2012 года № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (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) с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:

* монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

**или**

* монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

**либо**

выписка из реестра лицензий, на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (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) с указанием выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности:

* монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

**или**

* монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;
* работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
* передача шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* передача защищенных с использованием шифровальных (криптографических) средств информационных систем;
* передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* передача средств изготовления ключевых документов;
* предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;
* изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

Приложение № 2 к извещению

**Форма котировочной заявки**

Дата, исх. номер

 в МУП УИС

*(наименование заказчика)*

**ЗАЯВКА НА УЧАСТИЕ В ЗАПРОСЕ КОТИРОВОК В ЭЛЕКТРОННОЙ ФОРМЕ**

1. Изучив извещение о проведении запроса котировок в электронной форме № номер извещения «Наименование закупки» на право заключения вышеупомянутого договора для нужд МУП УИС, а также применимые к данной закупке законодательство и нормативные правовые акты Российской Федерации, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(полное наименование участника)* в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(наименование должности, Ф.И.О. руководителя, уполномоченного лица для юридического лица)*, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_,сообщает о согласии участвовать в запросе котировок в электронной форме на условиях, установленных в извещении о проведении запроса котировок в электронной форме, и направляет настоящую заявку.

О факте признания Заказчика банкротом уведомлены, к заключению договора в случае победы готовы.

2. Настоящей заявкой мы выражаем своё согласие оказать услуги, выполнить работы в точном соответствии с условиями, указанными в извещении, техническом задании и проекте договора, по цене:

 рублей, НДС в том числе *или* не облагается на основании \_\_\_\_\_\_\_\_\_\_*.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №п\п | Наименование услуг, работ | Кол-во | Ед. изм. | Срок гарантии на услуги, работы (мес.) | Цена за единицу (руб.) | Сумма (руб.) |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| **Итого:** |  |

 *Значение в столбце 7 в каждой строке должно быть вычислено* ***исключительно путём умножения***

***значения в столбце 3 на значение в столбце 6****. Какое-либо округление не допускается.*

*Значение в строке «Итого» должно строго равняться предложенной цене договора.*

3. Мы подтверждаем, что качество оказываемых услуг (выполняемых работ) соответствует требованиям действующих ГОСТов и другой нормативно-технической документации, удостоверяется соответствующими документами на русском языке согласно требованиям действующего законодательства, подтверждающими качество и безопасность.

4. Мы подтверждаем отсутствие сведений об организации в реестре недобросовестных поставщиков.

5. Мы подтверждаем, что в отношении нас не проводится процедура ликвидации, арбитражным судом не принято решения о признании нас банкротом и об открытии в отношении нас конкурсного производства, наша деятельность не приостановлена в порядке, предусмотренном Кодексом РФ об административных правонарушениях.

6. Мы подтверждаем, что у нас не имеется просроченной задолженности по налогам, сборам и иным обязательным платежам в бюджеты любого уровня и государственные внебюджетные фонды.

Ф.И.О. (полностью) руководителя, директора (для юридических лиц) (с указанием должности):

Документ, на основании которого действует руководитель (директор), его реквизиты:

Реквизиты для договора (заменить на свои):

|  |
| --- |
| **Муниципальное унитарное предприятие «Уфимские инженерные сети» городского округа город Уфа Республики Башкортостан**Юридический адрес:450065, Республика Башкортостан, город Уфа,улица Дмитрия Донского, дом № 9Фактический, почтовый адрес:450080, Республика Башкортостан, город Уфа,улица Степана Злобина, дом № 31/4ИНН 0277121421КПП 027701001ОГРН 1120280015910ОКПО 38479844Р/с 40702810700250003612в филиале ПАО «Банк УралСиб» в г. Уфа БИК 048073770К/с 30101810600000000770Тел.: (347) 246-26-96uiszakupki@gmail.com |
| Исполнительный директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ М. Г. Петров |

-----------------------------------------------------------------------------

Сведения о контактном лице - непосредственном составителе заявки на участие:

Ф. И. О.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Электронная почта: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 *(должность, И. О. Фамилия) (подпись)*

М. П.