**ПУБЛИЧНАЯ ОФЕРТА**

**О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика.**

|  |  |
| --- | --- |
| г. Москва | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

**Акционерное общество «Центр Биометрических Технологий»** (далее – **АО «ЦБТ»**) – оператор единой биометрической системы – государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных», которая содержит биометрические персональные данные физических лиц, векторы единой биометрической системы и иную предусмотренную в соответствии с частью 16 статьи 4 Федерального закона от 29.12.2022 N 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее – Закон № 572-ФЗ) информацию, которая используется в целях осуществления идентификации, аутентификации с использованием биометрических персональных данных физических лиц, а также в иных правоотношениях в случаях, установленных законодательством Российской Федерации, (далее – Единая биометрическая система либо ГИС ЕБС), именуемое в дальнейшем «Исполнитель» в лице Генерального директора Поволоцкого Владислава Юрьевича, действующего на основании Устава, настоящей публичной офертой (далее – Публичная оферта) предлагает организациям, осуществляющим размещение биометрических данных в Единой биометрической системе, именуемым в дальнейшем «Заказчик», совместно именуемым – «Стороны», а каждая по отдельности – «Сторона», заключить соглашение на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика. Данный документ в соответствии с пунктом 2 статьи 437 Гражданского Кодекса Российской Федерации (ГК РФ) является официальным предложением (Публичной офертой) АО «ЦБТ» о заключении Соглашения. В случае полного и безоговорочного принятия изложенных ниже условий, Заказчик посредством акцепта настоящей Публичной оферты путем совершения последовательных конклюдентных действий, указанных в п. 3.1 Соглашения, заключает настоящее Соглашение.

**СОГЛАШЕНИЕ**

**Термины и определения**

**ЕБС** – Государственная информационная система «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных», которая содержит биометрические персональные данные физических лиц, векторы единой биометрической системы и иную предусмотренную в соответствии с частью 16 статьи 4 Федерального закона №572-ФЗ информацию, которая используется в целях осуществления идентификации, аутентификации с использованием биометрических персональных данных физических лиц, а также в иных правоотношениях в случаях, установленных законодательством Российской Федерации, и оператором которой является определенная Правительством Российской Федерации организация.

**Информационная система (ИС) Заказчика** – информационная система Заказчика, осуществляющая сбор и обработку биометрических данных физических лиц.

**Отчетный период** – календарный квартал, в котором оказывались соответствующие Услуги. Исполнитель вправе увеличить продолжительность отдельного Отчетного периода в одностороннем порядке в соответствии с условиями Соглашения, но не более, чем на один календарный квартал.

**Положительное заключение** – подтверждение возможности оказания Услуг, предоставляемое технической поддержкой Исполнителя по итогам проверки возможности наличия технической возможности оказания Услуг.

**Программное обеспечение (ПО) –** интеграционное программное обеспечение, размещаемое на территории Заказчика и осуществляющее предоставление интеграционных интерфейсов для информационных систем Заказчика при оказании Услуги.

**Регистрация биометрических образцов** – совокупность транзакций, для которых подтверждена целостность и подлинность в ходе оказания Услуги, между Заказчиком и Исполнителем, результатом которой является регистрация биометрического образца в Единой биометрической системе.

**Регистрационная информация** – техническая информация, необходимая для осуществления сетевого взаимодействия между инфраструктурой Исполнителя и Заказчика (параметры сети, данные сертификата усиленной квалифицированной электронной подписи).

**Реестр регистраций** – совокупность информации о суммарном количестве Регистраций биометрических образцов за отчетный период.

**СМЭВ** - Единая система межведомственного электронного взаимодействия.

**СКЗИ** – средство криптографической защиты информации

**Сервис взаимодействия Заказчика** – набор сервисов, разрабатываемых Заказчиком, необходимый для взаимодействия Информационной системы Заказчика с сервисом по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя реализуемой СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика.

**Услуги** – действия по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя реализуемой СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика. Программное обеспечение, используемое для оказания Услуг, разработано на основе системного проекта, согласованного с ФСБ России, имеет положительное заключение ФСБ России о соответствии программно-аппаратного комплекса Исполнителя требованиям системного проекта и включают комплект эксплуатационной документации, утвержденный и (или) согласованный ФСБ России.

1. ПРЕДМЕТ СОГЛАШЕНИЯ
	1. Исполнитель обязуется оказывать Заказчику Услуги, а Заказчик обязуется принять и оплатить эти Услуги. Услуги включают:
		1. настройка криптографического оборудования Заказчика в целях формирования Заказчиком защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3;
		2. техническое обслуживание защищенного канала Заказчика при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3;
		3. настройка криптографического шлюза на стороне Исполнителя в целях формирования защищенного канала с криптографическим шлюзом Заказчика при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3;
		4. криптографическую аутентификацию Заказчика при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3;
		5. криптографическую аутентификацию уполномоченных сотрудников Заказчика с применением средств УКЭП класса не ниже КС2, а также криптографическое подтверждение подлинности и целостности электронного сообщения, содержащего биометрические персональные данные физического лица класса КС3;
		6. осуществление обеспечения контроля целостности и подтверждение подлинности электронных сообщений, содержащих биометрические персональные данные, путем их подписания УКЭП Исполнителя, реализуемой СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2).
	2. Заказчик обязуется принять от Исполнителя и оплатить оказанные услуги в порядке и на условиях, определенных настоящим Соглашением.
	3. Исполнитель вправе в одностороннем порядке изменять условия Соглашения путем опубликования на сайте https://ebs.ru/ нового текста Публичной оферты или внесения изменений в действующую редакцию Публичной оферты. Изменения вступают в силу не менее через 5 (пять) рабочих дней с момента размещения измененного текста Публичной оферты на сайте Исполнителя. Заказчик обязуется самостоятельно ознакомиться с новыми редакциями и соблюдать условия новых редакций Публичной оферты.
	4. Исполнитель вправе в любой момент в одностороннем порядке передать свои права и обязанности по Соглашению (осуществить передачу договора по смыслу ст. 392.3 ГК РФ) третьему лицу (третьим лицам) полностью или частично.
	5. Заказчик дает Исполнителю свое безоговорочное предварительное согласие на соответствующую передачу прав и обязанностей Исполнителя по Соглашению, указанную в п. 1.4. Соглашения, любому третьему лицу.
	6. Разработка сервисов взаимодействия Информационной системы Заказчика с сервисом по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя реализуемой СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика и иного программного обеспечения для подключения Информационной системы Заказчика к инфраструктуре Исполнителя, работы по подключению и интеграции Информационной системы Заказчика с инфраструктурой Исполнителя, приобретение дополнительного программного обеспечения для обеспечения взаимодействия Информационной системы Заказчика с инфраструктурой Исполнителя не относятся к предмету настоящего Соглашения.
	7. Оказание Услуги осуществляется через предварительно сформированный Заказчиком и защищенный шифрованием канал с использованием СКЗИ класса КС3 при осуществлении доступа к информационной инфраструктуре Исполнителя. Организация доступа к предварительно сформированному каналу, а также интеграция с ним Информационных систем Заказчика являются обязанностью Заказчика и не входит в обязанности Исполнителя по настоящему Соглашению.
	8. Заказчик подтверждает и гарантирует, что криптооборудование, используемое на стороне Заказчика для подключения к информационной инфраструктуре Исполнителя, выбранное согласно Приложению № 2 к данной Оферте и указанное в Приложении № 3 к данной Оферте, не является контрафактным и контрабандным, свободно от прав третьих лиц, под арестом не состоит, в таможенной очистке не нуждается, соответствует всем необходимым техническим и качественным характеристикам и требованиям действующего законодательства Российской Федерации.
	9. Настройка криптографического оборудования Заказчика в целях формирования Заказчиком защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3 выполняется Исполнителем в соответствии со Спецификацией (Приложение № 4 к данной Оферте).
	10. Техническое обслуживание защищенного канала Заказчика при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3 выполняется Исполнителем в соответствии со Спецификацией (Приложение № 5 к данной Оферте).
2. ОБЯЗАННОСТИ И ПРАВА СТОРОН
	1. Права и обязанности Исполнителя:
		1. Исполнитель обязуется оказывать Заказчику Услуги в соответствии с условиями настоящего Соглашения.
		2. Услуги оказываются с соблюдением условий системного проекта, согласованного с ФСБ России, имеющего положительное заключение ФСБ России о соответствии программно-аппаратного комплекса Исполнителя требованиям по безопасности информации.
		3. Исполнитель обязуется в течение срока, указанного в п. 12.1, оказывать Услуги на условиях, предусмотренных настоящим Соглашением.
		4. Услуги оказываются Исполнителем удаленно, с использованием вычислительных и иных средств связи. Место оказания услуги – 115035, г. Москва, вн.тер.г. муниципальный округ Замоскворечье, Овчинниковская набережная, д. 18/1, стр. 2.
	2. Права и обязанности Заказчика:
		1. Заказчик обязуется выполнить все предписанные действия, указанные в документации к Услуге, размещенной на портале ebs.ru, до подачи обращения в службу технической поддержки Исполнителя. Если такие действия не приведут к устранению неисправности, то Заказчик незамедлительно уведомляет Исполнителя о наличии такой неисправности, по адресу электронной почты otib@ebs.ru.
		2. Заказчик обязуется создать необходимые условия для оказания Услуг Исполнителем, включая все работы по подключению и интеграции Информационной системы Заказчика, необходимые для оказания Услуг, приобретение дополнительного аппаратного и программного обеспечения, необходимого для оказания Услуги.
	3. Заказчик обязуется информировать Исполнителя (с приложением копий подтверждающих документов и соответствующих пояснений) обо всех изменениях, касающихся почтового адреса, адреса места нахождения, формы собственности, банковских реквизитов, изменения организационно-правовой формы, реорганизации, присоединении и т.д., путем направления указанной информации на электронную почту business@ebs.ru не позднее 3 (трех) рабочих дней с даты наступления таких изменений. В случае если Заказчик не уведомил Исполнителя об изменениях, указанных в настоящем пункте Соглашения, Исполнитель вправе применить к Заказчику меры ответственности за просрочку в соответствии с разделом 8 Соглашения, а также потребовать возмещения убытков.
	4. В рамках исполнения Соглашения Стороны могут обмениваться следующими первичными документами – УПД – посредством электронного документооборота с использованием только квалифицированной электронной подписи через операторов электронного документооборота. В момент осуществления фактических действий по обмену электронными документами Заказчик присоединяется к соглашению об электронном документообороте, размещенном по адресу https://ebs.ru/documents/.
3. АКЦЕПТ ОФЕРТЫ И ДАТА НАЧАЛА ОКАЗАНИЯ УСЛУГИ
	1. Подтверждением согласия с условиями настоящего Соглашения и акцептом настоящей Публичной оферты является осуществление Заказчиком на сайте https://ebs.ru/ следующих последовательных действий:
		1. заполнение формы в соответствии с Приложением № 1;
		2. направление заполненной формы (Приложение № 1) посредством нажатия на кнопку «Подписать и отправить»;
		3. предоставление положительного заключения технической поддержки Исполнителя о работоспособности защищенного канала Заказчика для осуществления доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3 в целях дальнейшей возможности оказания Услуг Исполнителем путем направления Исполнителем такого заключения на электронную почту, указанную в форме Приложения № 1.
	2. Исполнитель в течение 5 (пяти) рабочих дней после акцептирования настоящей Публичной оферты Заказчиком, направляет на электронную почту Заказчика, указанную в заполненной в соответствии с Приложением № 1 форме, Регистрационную информацию для подключения ИС Заказчика к сервису оказания Услуги. На предоставленную Регистрационную информацию распространяется режим конфиденциальности, предусмотренный разделом 10 настоящего Соглашения.
	3. Датой начала оказания Услуги считается дата направления Регистрационной информации в соответствии п.3.2 настоящего Соглашения.
	4. В результате совершения акцепта Заказчик и Исполнитель становятся Сторонами настоящего Соглашения.
4. ЦЕНА ОКАЗЫВАЕМЫХ УСЛУГ
	1. Заказчик оплачивает Услуги в рамках настоящего Соглашения в сроки и в порядке, установленные в настоящем Соглашении.
	2. Отчетным периодом для оказания Услуг является календарный квартал.
	3. Плата за Услуги облагается НДС в соответствии с законодательством Российской Федерации.
	4. Плата за Услуги устанавливается в зависимости от количества Регистраций биометрических образцов, произведенных Заказчиком за отчетный период:
		* От 0 до 150 Регистраций биометрических персональных данных – плата за Услуги составляет 240 000 (двести сорок тысяч) рублей 00 копеек, в том числе НДС 20 % в размере 40 000 (сорок тысяч) рублей 00 копеек.
		* От 151 до 900 Регистраций биометрических образцов – плата за Услуги составляет 492 000 (четыреста девяносто две тысячи) рублей 00 копеек, в том числе НДС 20 % в размере 82 000 (восемьдесят две тысячи) рублей 00 копеек.
		* Более 900 Регистраций биометрических образцов – плата за Услуги составляет 660 000 (шестьсот шестьдесят тысяч) рублей 00 копеек, в том числе НДС 20 % в размере 110 000 (сто десять тысяч) рублей 00 копеек.

4.5 Основанием для выставления УПД является Реестр Регистраций, направляемый Исполнителем Заказчику по электронной почте, указанной Заказчиком в форме предоставления информации, заполненной в соответствии с Приложением № 1, не позднее 5 (пяти) рабочих дней, следующих за отчетным периодом.

1. ПРЕДОСТАВЛЕНИЕ ПРОГРАММНЫХ СРЕДСТВ
	1. В рамках оказания Услуги на условиях неисключительных прав осуществляется предоставление Программного обеспечения для размещения на территории Заказчика и использования при оказании Услуги.
	2. ПО предоставляется для использования на территории Российской Федерации на срок действия настоящего Соглашения.
	3. Заказчик вправе воспроизводить ПО только в неизменном виде.
	4. Исполнитель гарантирует работу ПО на протяжении всего периода оказания Услуги.
2. ПОРЯДОК РАСЧЕТОВ
	1. Заказчик оплачивает услуги ежеквартально, в сроки и в порядке, указанные в настоящем Соглашении.
	2. Оплата производится в российских рублях.
	3. Не позднее 5 (пяти) рабочих дней после направления Реестра Регистрации Исполнитель выставляет УПД. УПД выставляется Исполнителем в соответствии с Законодательством РФ.
	4. Оплата производится Заказчиком в течение 30 календарных дней с даты получения оригинала счета.
	5. Днем оплаты и исполнения Заказчиком своих обязательств по оплате является день зачисления денежных средств на расчетный счет Исполнителя, указанный в статье 18 настоящего Соглашения.
	6. Не реже одного раза в год, а также по мере необходимости, Стороны осуществляют сверку расчетов с оформлением двустороннего акта сверки расчетов. Акт сверки расчетов составляется заинтересованной Стороной в двух экземплярах, каждый из которых должен быть подписан уполномоченным представителем этой Стороны и скреплен ее печатью. Сторона-инициатор направляет в адрес Стороны-получателя два оригинала акта сверки расчетов почтовой связью заказным или ценным письмом с уведомлением о вручении, курьерской службой или иным согласованным Сторонами способом. В течение 10 (десяти) рабочих дней со дня получения акта сверки расчетов Сторона-получатель должна подписать, заверить печатью, направить один экземпляр акта сверки расчетов в адрес Стороны-инициатора, или направить Стороне-инициатору свои письменные мотивированные возражения по поводу достоверности содержащейся в акте сверки расчетов информации. Если в течение 10 (десяти) рабочих дней со дня получения акта сверки расчетов Сторона-получатель не направит в адрес Стороны-инициатора подписанный акт сверки расчетов или письменные мотивированные возражения по поводу достоверности, содержащейся в нем информации, акт сверки расчетов считается признанным Стороной-получателем в редакции Стороны-инициатора.
3. ПОРЯДОК СДАЧИ-ПРИЕМКИ УСЛУГ
	1. Не позднее 5 (пяти) рабочих дней с даты направления Реестра Регистраций, Исполнитель в подтверждение сдачи оказанных Услуг оформляет и отправляет по почте / курьерской службой / нарочным способом / посредствам электронного документооборота Заказчику подписанные со своей стороны два экземпляра УПД.
	2. Заказчик обязуется принять оказанные Услуги и подписать УПД в течение 5 (пяти) рабочих дней с даты его получения от Исполнителя или направить письменный мотивированный отказ от подписания УПД в тот же срок.
	3. В случае получения Исполнителем мотивированного отказа, Стороны согласовывают уменьшение стоимости оказанных Услуг не позднее чем через 3 (три) рабочих дня с даты получения Исполнителем мотивированного отказа от Заказчика.
	4. В случае непредставления Заказчиком подписанного УПД или мотивированного отказа в срок, установленный в п.7.2 настоящего Соглашения, Услуги признаются оказанными в полном объеме и в срок, УПД считается подписанным Сторонами.
	5. Подписанный Сторонами УПД удостоверяет факт принятия Заказчиком оказания Услуг в полном объеме и является основанием для оплаты Исполнителю оказанных Услуг по настоящему Соглашению.
4. ОТВЕТСТВЕННОСТЬ СТОРОН
	1. При нарушении обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации и настоящей Публичной офертой.
	2. За просрочку исполнения обязательств, предусмотренных настоящим Соглашением, Стороны выплачивают по письменному требованию пострадавшей Стороны неустойку в размере 1/365 (1/366 - если год високосный) ключевой ставки Центрального банка Российской Федерации от стоимости (с учетом НДС) не оказанных услуг (для Исполнителя) либо от неоплаченной в срок суммы (для Заказчика) за каждый день просрочки. Общая сумма пени не должна превышать 10% (десяти процентов) от стоимости не оказанных услуг (для Исполнителя) либо от неоплаченной в срок суммы (для Заказчика).
	3. Выплата неустойки по настоящей Публичной оферте осуществляется только на основании предъявленной письменной претензии.
	4. Уплата неустойки осуществляется в срок не позднее 10 (десяти) рабочих дней со дня получения соответствующего письменного требования.
	5. Оплата неустойки осуществляется по безналичному расчету в российских рублях путем перечисления денежных средств на расчетный счет Стороны, выставившей претензию. Обязанность по уплате неустойки считается исполненной со дня поступления денежных средств на расчетный счет Стороны, которой выплачивается неустойка.
	6. Уплата неустойки и возмещение убытков в случае неисполнения или ненадлежащего исполнения обязательств по настоящему Соглашению не освобождает Стороны от исполнения их обязательств по настоящему Соглашению.
	7. Заказчик несет полную ответственность за сбор биометрических образцов (биометрических персональных данных) и дальнейшую их передачу Исполнителю в соответствии с действующим Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ.
	8. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению, если докажут, что их неисполнение или ненадлежащее исполнение произошло вследствие действия обстоятельств непреодолимой силы или по вине другой Стороны.
	9. Окончание срока действия настоящего Соглашения не освобождает Стороны от ответственности за ранее допущенные нарушения в ходе исполнения Соглашения, если они не были устранены до момента окончания действия настоящего Соглашения.
5. СУБИСПОЛНИТЕЛИ
	1. Исполнитель имеет право привлекать к исполнению настоящего Соглашения субисполнителей без согласования с Заказчиком.
	2. Передача выполнения части исполнения своих обязательств субисполнителю не освобождает Исполнителя от обязательств и ответственности перед Заказчиком в рамках настоящего Соглашения. Исполнитель принимает на себя ответственность за ненадлежащее исполнение субисполнителем обязательств по настоящему Соглашению.
6. УСЛОВИЯ КОНФИДЕНЦИАЛЬНОСТИ
	1. Настоящим Стороны договорились, что конфиденциальной информацией являются любые сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах, предоставленные в любой форме, включая информацию, предоставленную устно, а также любая иная информация, обозначенная в качестве конфиденциальной информации или на которую имеется ссылка как на конфиденциальную информацию (далее по тексту - Конфиденциальная информация).
	2. Передающая Сторона - сторона, которой может быть как Исполнитель, так и Заказчик, передающая на условиях настоящего Соглашения Конфиденциальную информацию.
	3. Получающая Сторона - сторона, которой может быть как Исполнитель, так и Заказчик, получающая от Передающей Стороны на условиях настоящего Соглашения Конфиденциальную информацию.
	4. Представители - директора, должностные лица, сотрудники, юристы, бухгалтеры, аудиторы, финансовые консультанты, аффилированные лица Стороны, которые уполномочены раскрывать и/или получать Конфиденциальную информацию.
	5. Третьи лица - иные лица, не относящиеся к Сторонам и их Представителям.
	6. Разглашение Конфиденциальной информации – действие или бездействие Получающей Стороны, в результате которого Конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной Третьим лицам без согласия Передающей Стороны.
	7. Конфиденциальная информация не включает в себя информацию, которая (1) является общедоступной, либо (2) была доступна Получающей Стороне не на конфиденциальной основе до раскрытия этой информации Передающей Стороной, либо (3) становится доступна Получающей Стороне не на конфиденциальной основе из какого-либо источника помимо Передающей Стороны, при условии, что Получающей Стороне известно, что этому источнику не запрещено раскрывать такую информацию договорным или иным юридическим обязательством перед Передающей Стороной.
	8. Настоящие условия распространяются на Конфиденциальную информацию, передаваемую Передающей Стороной Получающей Стороне в связи с исполнением Соглашения, а также Конфиденциальную информацию, которая иным образом станет известной Получающей Стороне в связи с исполнением Соглашения (в указанном случае Передающая Сторона уведомляет Получающую Сторону о том, что такая информация является Конфиденциальной информацией).
	9. Передача Конфиденциальной информации осуществляется на бумажных и иных материальных носителях, содержащих отметку о конфиденциальности (грифы «Конфиденциальная информация», «Конфиденциально»).

Стороны соглашаются с тем, что Конфиденциальная информация может быть передана Передающей Стороной Получающей Стороне с использованием каналов закрытой электронной почты (с использованием программного комплекса средств шифрования передаваемой информации по алгоритму ГОСТ) и указанием о том, что передаваемая информация является Конфиденциальной информацией.

В случае раскрытия Конфиденциальной информации в устном виде Стороны обязуются в течение 3 (трех) рабочих дней с момента устного раскрытия оформить передачу такой Конфиденциальной информации на бумажных и иных материальных носителях или с использованием каналов закрытой электронной почты в соответствии с настоящим пунктом Соглашения.

Передача Конфиденциальной информации способами, не предусмотренными настоящим пунктом Соглашения, запрещается.

* 1. Получающая Сторона вправе предоставлять доступ к полученной по настоящему Соглашению Конфиденциальной информации только тем Представителям Получающей Стороны, доступ которых к Конфиденциальной информации необходим в связи с Соглашением, и только в той части, в которой это необходимо. При этом Представители Получающей Стороны, получившие доступ к такой информации, должны быть уведомлены Получающей Стороной о конфиденциальности информации и условиях ее использования. Перечень Представителей Получающей Стороны, которым предоставлен доступ к Конфиденциальной информации, должен быть передан Получающей Стороной Передающей Стороне до предоставления им доступа к Конфиденциальной информации.
	2. Получающая Сторона соглашается, что Конфиденциальная информация будет использована исключительно в связи с исполнением Соглашения и что Получающая Сторона и ее Представители сохранят конфиденциальность такой информации и эта информация не будет раскрыта или передана Третьим лицам без предварительного письменного согласия Передающей Стороны. Получающая Сторона обязуется обеспечить защиту переданной Конфиденциальной информации на уровне не меньшем, чем осуществляется защита Конфиденциальной информации Получающей Стороны.

В случае передачи Получающей Стороной на основании письменного согласия Передающей Стороны Конфиденциальной информации Третьим лицам, Получающая Сторона обязана обеспечить, чтобы Третьи лица до получения доступа к Конфиденциальной информации приняли на себя обязательства по использованию и неразглашению такой информации на условиях, предусмотренных в настоящем Соглашении. Получающая Сторона должна заблаговременно предоставить Передающей Стороне копию соглашения о конфиденциальности, подписанного Получающей Стороной с Третьим лицом.

* 1. В случае получения мотивированного требования от органа государственной власти или органа местного самоуправления о предоставлении Конфиденциальной информации, в случаях, если это не запрещено действующим законодательством РФ, Получающая Сторона обязана уведомить соответствующий орган государственной власти или орган местного самоуправления о конфиденциальности такой информации и ее обладателе.

В случае получения от органа государственной власти или органа местного самоуправления мотивированного требования о предоставлении Конфиденциальной информации, Получающая Сторона обязана незамедлительно известить о таком требовании Передающую Сторону для того, чтобы Передающая Сторона имела возможность принять меры в порядке защиты, ограничения или предотвращения подобной передачи или раскрытия Конфиденциальной информации, насколько это допускается законом.

Получающая Сторона имеет право раскрыть органу государственной власти или органу местного самоуправления лишь ту часть полученной от Передающей Стороны Конфиденциальной информации, раскрытие которой требуется по закону.

* 1. Получающая Сторона несет ответственность за нарушение обязательств по соблюдению условий использования и обеспечения конфиденциальности полученной Конфиденциальной информации в соответствии с законодательством Российской Федерации и условиями настоящего Соглашения и обязана возместить Передающей Стороне убытки, возникшие у Передающей Стороны вследствие ненадлежащего исполнения Получающей Стороной условий настоящего раздела.
	2. Получающая Сторона несет ответственность в полном объеме за разглашение Конфиденциальной информации ее Представителями и Третьими лицами, получившими доступ к такой информации в соответствии с условиями, определенными в пунктах 7.10. и 7.11. настоящего Соглашения.
	3. При Разглашении Конфиденциальной информации, а также при наличии обстоятельств, способствующих Разглашению Конфиденциальной информации, Получающая Сторона обязана незамедлительно уведомить об этом Передающую Сторону, предоставить Передающей Стороне всю необходимую информацию о факте Разглашения или наличии угрозы Разглашения, причинах, приведших к этому, и мерах, предпринятых Получающей Стороной для предотвращения Разглашения и устранения возникших в связи с этим неблагоприятных последствий.
	4. Обязательства Получающей Стороны по сохранению конфиденциальности полученной от Передающей Стороны Конфиденциальной информации, определенные в настоящем разделе, сохраняют силу в течение 3 (трех) лет после истечения срока действия настоящего Соглашения.
	5. Получающая Сторона назначит и уведомит Передающую Сторону об уполномоченных Представителях, ответственных за контроль за соблюдением обязательств по настоящему разделу, не позднее 3 (трех) рабочих дней со дня заключения настоящего Соглашения. Об изменении уполномоченных Представителей Получающая Сторона обязана уведомить Передающую Сторону не позднее 5 (пяти) рабочих дней до момента такого изменения.
	6. Получающая Сторона признает, что ни Передающая Сторона, ни кто-либо из ее аффилированных лиц, а также никто из ее уполномоченных Представителей не дает никаких заверений или гарантий относительно полноты Конфиденциальной информации или ее использования Получающей Стороной.
	7. Передающая Сторона настоящим гарантирует, что она обладает всеми правами в отношении Конфиденциальной информации, включая право передавать такую информацию Получающей Стороне на условиях настоящего Соглашения.
	8. Передающая Сторона вправе потребовать от Получающей Стороны вернуть ей материальные носители Конфиденциальной информации, направив Получающей Стороне уведомление о возврате в письменной форме. В течение 10 (десяти) рабочих дней после получения такого уведомления Получающая Сторона обязана вернуть все оригиналы носителей Конфиденциальной информации и уничтожить все копии такой информации и ее воспроизведения в любой форме (включая компьютерные записи и файлы), находящиеся в распоряжении Получающей Стороны, а также в распоряжении лиц, которым такая информация была передана в соответствии с Соглашением.
	9. Передающая Сторона имеет право прекратить защиту конфиденциальности переданной по настоящему Соглашению Конфиденциальной информации, о чем в обязательном порядке должна письменно проинформировать Получающую Сторону в течение 10 (десяти) рабочих дней с момента принятия решения о прекращении защиты.
	10. Положения настоящего раздела имеют приоритетное значение по отношению к условиям Соглашения и любым другим соглашениям Сторон и включенным в них нормам о конфиденциальности, регулирующим те же и/или аналогичные отношения между ними.
1. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ
	1. К обстоятельствам непреодолимой силы Стороны согласились относить стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, связанных с исполнением настоящего Соглашения юридических лиц, военные действия и иные непредвиденные обстоятельства, создающие препятствия или иным образом мешающие выполнению Сторонами обязательств по настоящему Соглашению.
	2. При наступлении обстоятельства непреодолимой силы Сторона, для которой создалась невозможность исполнения своих обязательств по Соглашению, должна в течение 3 (трех) календарных дней письменно уведомить другую Сторону о таком обстоятельстве и причине его возникновения. Срок исполнения обязательств отодвигается соразмерно времени, в течение которого будут действовать обстоятельства непреодолимой силы.
	3. Если указанные обстоятельства будут продолжаться более 2 (двух) месяцев, то каждая из Сторон имеет право отказаться от дальнейшего исполнения обязательств по Соглашению. В этом случае Стороны должны провести взаиморасчеты за фактически выполненные работы, оказанные услуги.
2. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ
	1. Настоящее Соглашение вступает в силу с даты акцепта Публичной оферты Заказчиком и действует бессрочно.
3. ОФИЦИАЛЬНЫЙ ЯЗЫК
	1. Вся относящаяся к настоящему Соглашению переписка и другая документация, которой обмениваются Стороны в ходе исполнения обязательств по Соглашению, должны быть составлены и подписаны на русском языке. При справочном предоставлении информации, в том числе технической, на иностранных языках к ней должен прилагаться перевод, который при наличии расхождений между ним и справочной информацией будет иметь преимущественную юридическую силу, при условии ответственности представившей данные документы Стороны за аутентичность перевода.
4. РАЗРЕШЕНИЕ СПОРОВ
	1. Все споры и разногласия, которые могут возникнуть из-за настоящего Соглашения или в связи с ним, будут разрешаться, прежде всего, путем переговоров между Сторонами.
	2. Претензионный порядок урегулирования споров будет применяться Сторонами в случаях, предусмотренных законом. Претензия в рамках Соглашения может быть направлена с использованием факса и/или электронной почты, указанной Сторонами в заполненной в соответствии с Приложением №1 форме. Оригиналы направляются по почте / курьерской службой / нарочным с уведомлением о доставке. Датой доставки документов считается дата доставки факса / электронного сообщения. Срок рассмотрения претензии 10 (десять) рабочих дней с момента ее доставки.
	3. В случае если споры и разногласия не урегулированы в соответствии с п.14.2 настоящего Соглашения, каждая из Сторон вправе обратиться в Арбитражный суд г. Москвы с иском о разрешении спора.
5. РАСТОРЖЕНИЕ СОГЛАШЕНИЯ
	1. Соглашение может быть прекращено:
* по соглашению Сторон;
* по инициативе Заказчика. При этом Заказчик обязан уведомить Исполнителя о расторжении не менее чем за 30 (тридцать) календарных дней до предполагаемой даты прекращения Соглашения, а также произвести оплату всех причитающихся Исполнителю сумм в рамках настоящего Соглашения;
* по инициативе Исполнителя. При этом Исполнитель обязан уведомить Заказчика об отказе от исполнения Соглашения не менее чем за 30 (тридцать) календарных дней до предполагаемой даты прекращения Соглашения;
* по иным основаниям, предусмотренным настоящим Соглашением и действующим законодательством.
	1. При расторжении настоящего Соглашения по любым основаниям его положения будут применяться к отношениям Сторон вплоть до полного окончания взаимных расчётов и передачи необходимой документации.
1. НАЛОГИ И ПОШЛИНЫ
	1. Исполнитель самостоятельно оплачивает все налоги, пошлины, лицензионные сборы и другие обязательные платежи, связанные с исполнением Соглашения.
2. АНТИКОРРУПЦИОННАЯ ДОГОВОРНАЯ ОГОВОРКА
	1. Заказчику известно о том, что Исполнитель ведет антикоррупционную политику и развивает не допускающую коррупционных проявлений культуру. Заказчик настоящим подтверждает, что он полностью разделяет нетерпимость к любым коррупционным проявлениям и в своей деятельности, в том числе в рамках исполнения настоящего Публичной оферты, предпринимает меры для их исключения в соответствии с действующим законодательством.
3. АДРЕСА И РЕКВИЗИТЫ АО «ЦБТ»

|  |
| --- |
| **АО «ЦБТ»**ИНН 9705169387; КПП 770501001ОГРН 1227700243748; ОКПО 73636434Местонахождение: Российская Федерация, 115035, г. Москва, вн.тер.г. муниципальный округ Замоскворечье, Овчинниковская набережная, д. 18/1, стр. 2. Почтовый адрес: 115035, г. Москва, вн.тер.г. муниципальный округ Замоскворечье, Овчинниковская набережная, д. 18/1, стр. 2.Банковские реквизиты:р/с 40702810503800001245,в ПАО «Банк ВТБ»,к/с 30101810700000000187, БИК 044525187 |
| АО «ЦБТ»Генеральный директор Поволоцкий Владислав Юрьевич |

**Приложение № 1**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Форма предоставления информации Заказчиком для доступа к Услугам**

Данные о лице, уполномоченном акцептировать настоящую Публичную оферту

|  |  |
| --- | --- |
| ФИО |  |
| Должность |  |
| Е-mail (электронный адрес) |  |

Все поля обязательны к заполнению

Данные о Заказчике

|  |  |
| --- | --- |
| Полное наименование  |  |
| Краткое наименование  |  |
| ИНН |  |
| КПП |  |
| ОГРН/ОГРНИП |  |
| Код [ИФНС](https://service.nalog.ru/addrno.do)  |  |
| Телефон |  |
| Адрес юридический (индекс, город, улица, дом) |  |
| Адрес почтовый (индекс, город, улица, дом) |  |

Все поля обязательны к заполнению

Дополнительные данные

|  |  |
| --- | --- |
|  |  |

С условиями Публичной оферты о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика, Заказчик ознакомлен и согласен.

**Приложение № 2**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Рекомендуемые требования, обеспечиваемые при подключении Заказчика к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3**

1. В целях формирования Заказчиком защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3, используются следующие варианты типового криптографического оборудования «Код Безопасности» Заказчика:
* использование кластера АПКШ Континент IPC-3000\*;
* использование одиночного АПКШ Континент IPC-3000\*;
* использование кластера АПКШ Континент IPC-1000/IPC-1000F;
* использование одиночного АПКШ Континент IPC-1000/IPC-1000F;
* использование кластера АПКШ Континент IPC-100;
* использование одиночного АПКШ Континент IPC-100;
* использование одиночного АПКШ Континент IPC-25;
* использование одиночного АПКШ Континент IPC-10.
1. В таблице 1 представлены рекомендации по выбору типа АПКШ Континент в зависимости от количества используемых Заказчиком сетевых узлов (АРМ, серверов, терминалов), обрабатывающих подлежащую защите информацию:

Таблица 1 - Рекомендуемое оборудование в зависимости от количества АРМ

|  |  |  |
| --- | --- | --- |
| № п/п | Количество серверов, АРМ и терминалов в защищаемом сегменте | Рекомендуемая номенклатура решений Код безопасности |
| 1 | более 100 | IPC-1000, IPC-1000F, IPC-3000 |
| 2 | от 11 до 100 | IPC-100 |
| 3 | от 1 до 10 | IPC-25, IPC-10 |

1. В таблице 2 представлены рекомендации по выбору типа АПКШ Континент в зависимости от необходимой пропускной способности защищенного канала при осуществлении Заказчиком доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3:

Таблица 2 - Рекомендации по пропускной способности каналов связи

|  |  |  |
| --- | --- | --- |
| № п/п | Необходимая производительность шифрования | Рекомендуемая номенклатура решений Код безопасности |
| 1 | до 2,7 Гбит/с | IPC-3000/IPC-1000 |
| 2 | до 950 Мбит/с | IPC-1000F |
| 3 | до 300 Мбит/с | IPC-100 |
| 4 | до 100 Мбит/с | IPC-25, IPC-10 |

1. Рекомендации по обеспечению резервного электроснабжения

При подключении АПКШ Континент к UPS последний обеспечивает работу компьютера только до тех пор, пока не разрядится батарея. После разряда батареи компьютер будет некорректно выключен, что может привести к потере данных. В то же время большинство современных UPS могут подключаться к компьютеру с помощью интерфейсного кабеля и посылать сигнал об истощении батареи. Полученный сигнал компьютер может использовать для корректного выключения.

**Приложение № 3**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Спецификация Оборудования Заказчика**

1. Оборудование:

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Описание** | **Кол-во** |
| 1 | АПКШ Континент | Производитель ООО «Код Безопасности». АПКШ Континент IPC-100 | 1 |
| 2 | Техническая поддержка | Ключ активации сервиса прямой технической поддержки уровня "Расширенный" для АПКШ "Континент", 1 год, HSEC-SUPPORT-EXT | 1 |

2. Комплектность принятого Оборудования от Заказчика:

* АПКШ Континент IPC-100, 1 шт.

2.1. Комплектность поставки:

* АПКШ Континент IPC-100
* CD диск с документацией
* паспорт Оборудования
* копии сертификатов
* упаковка

**Приложение № 4**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Спецификация на выполняемые работы по настройке криптографического оборудования**

1. Выполняемые работы:

Настройка криптографического оборудования Заказчика, указанного в Спецификации (Приложение № 3 к данной Оферте), в целях формирования Заказчиком защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3.

1. Настройка криптографического оборудования включает в себя:
* Преднастройку Оборудования согласно согласованным с Заказчиком техническим параметрам подключения:
	+ Подготовка конфигурационного и ключевого файлов для Оборудования марки «Континент» осуществляется на стороне Исполнителя в центре управления сети (ЦУС).
	+ Установку конфигурационного и ключевого файлов на оборудование марки «Континент» производят специалисты Заказчика, имеющие допуск к работе с СКЗИ, по инструкции, полученной от Исполнителя.
	+ На площадке размещения Оборудования Заказчика, необходимо присутствие специалистов Заказчика для выполнения необходимых действий.
	+ Передача ключей шифрования Заказчику осуществляется по защищенному каналу надежным способом, исключающим несанкционированный доступ.
* Консультация специалистов Заказчика по вопросам, связанным с техническими параметрами подключения;
* Настройка подключения;
* Тестирование Оборудования и защищенного канала:
	+ В случае готовности ресурсов Заказчика осуществляется проверка соединения посредством пинга ресурсов Единой биометрической системы (далее – ЕБС) с ресурсов Заказчика.
	+ В случае неготовности ресурсов Заказчика осуществляется проверка соединения посредством пинга криптошлюза ЕБС с криптошлюза Заказчика.
1. Срок выполнения работ: в течение 5 (пяти) рабочих дней с даты извещения Заказчиком Исполнителя о готовности площадки объекта и монтаже Оборудования Заказчика для проведения работ.
2. Сопровождение работ Исполнителем производится удаленно.
3. На объекте установки Заказчик создает необходимые условия для выполнения работ.
4. Место выполняемых работ – территория Заказчика: \_\_\_\_\_\_\_\_\_\_\_\_\_.

**Приложение № 5**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Спецификация на оказываемые услуги по техническому обслуживанию защищенного канала**

1. Оказываемые услуги:

Техническое обслуживание защищенного канала Заказчика при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3.

1. Дата начала оказания Услуг исчисляется со дня подписания Сторонами Акта сдачи-приемки выполненных работ по настройке защищенного канала с использованием Оборудования, указанного в Спецификации оборудования (Приложение № 3 к данной Оферте).
2. Техническое обслуживание защищенного канала производится в соответствии с описанием услуги, указанном в Приложении № 5.1 к данной Оферте.
3. Срок оказания услуг: 1 (один) год с даты начала оказания Услуг, указанной в пункте 2. настоящего Приложения.
4. Приемка-сдача услуг осуществляется Сторонами ежеквартально путем оформления и подписания УПД, в порядке, предусмотренном статьей 7 данной Оферты.
5. Место установки поддерживаемого Оборудования – территория Заказчика: \_\_\_\_\_\_\_\_\_\_\_\_\_.

**Приложение № 5.1**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Описание услуг по техническому обслуживанию защищенного канала, оказываемых Исполнителем, и условия их предоставления**

Настоящее Приложение о видах и условиях предоставления услуг является неотъемлемой частью Оферты. Все термины, написанные с заглавной буквы, определение которых ниже не приводится, употребляются в том же значении, которое было оговорено в Оферте. В случае возникновения расхождений между условиями настоящего Приложения и Оферты, условия по определению порядка оказания услуг настоящего Приложения имеют преимущественную силу.

|  |  |
| --- | --- |
| **Термин или сокращение** | **Определение** |
| **ЦТП** | Центр технической поддержки Исполнителя |
| **Запрос** | Оформленная в соответствии с определенным порядком заявка Заказчика на предоставление услуг |

1. **Порядок оформления Запроса**
	1. Предоставление услуг Заказчику осуществляется по Запросу Заказчика.
	2. Запрос направляется в Центр технической поддержки Исполнителя по электронной почте otib@ebs.ru.
	3. Запрос должен содержать следующие сведения:
2. номер Оферты;
3. координаты представителя Заказчика;
4. тип, серийный номер Оборудования, аппаратного обеспечения;
5. подробное описание неисправности.

1.4 При соответствующем оформлении Запроса Исполнитель регистрирует Запрос и в течение 1 (одного) рабочего часа, устанавливает приоритет Запроса, сообщает Заказчику номер Запроса по электронной почте или по телефону. После регистрации Запроса от Заказчика Запрос считается принятым, Исполнитель приступает к его выполнению в соответствии с оказываемыми видами услуг.

1. **Описание услуг**
	1. **Технический консалтинг**

В рамках действия этой услуги Исполнителем обеспечивается:

* + 1. Регистрация запросов от уполномоченных лиц технических служб Заказчика 24 часа в сутки, 365/366 дней в году, включая выходные и праздничные дни.
		2. Работы по заявкам выполняются в рабочие часы (с 9-00 до 18-00 по московскому времени), в рабочие дни (согласно законодательству Российской Федерации).
		3. Консультации при возникновении у специалистов Заказчика затруднений при использовании Оборудования. Помощь и технические консультации оказываются как при первичной инсталляции, так и при эксплуатации.
		4. Поддержка ключевой и справочной информации в актуальном состоянии, просмотр журналов событий, проактивная работа по поддержанию в работоспособном состоянии защищенного канала, обеспечиваемого Оборудованием.
		5. Внесение необходимых изменений в конфигурацию криптооборудования в случае изменений со стороны Заказчика.
		6. Предоставление Заказчику инструкций по проведению диагностики при подозрении на неисправность Оборудования.
		7. Проведение работ по поиску и локализации причин возникновения некорректной работы Оборудования и/или аппаратного обеспечения.
		8. Исполнение услуг до полного устранения проблемы или до момента, когда Стороны совместно вынесут решение о нецелесообразности дальнейшей работы над проблемой.
		9. Услуги оказываются при помощи средств удаленного доступа.
1. **Базовые параметры предоставления услуги технического обслуживания защищенного канала**

Базовые параметры предоставления услуги определяют уровень доступности услуги.

Таблица 1. Базовые параметры предоставления технического обслуживания криптооборудования

|  |  |
| --- | --- |
| **Временной режим доступности защищенной сети** | круглосуточно (24х7) |
| **Временной режим регистрации запросов** | круглосуточно (24х7) |
| **Временной режим решения запросов критичного приоритета** | круглосуточно (24х7) |
| **Временной режим решения и обработки запросов других степеней** | с 9:00 до 18:00 часов (Московское время) ежедневно по рабочим дням |
| **Временной интервал проведения регламентных работ на Оборудовании криптошлюзов** | Для проведения плановых работ выделяется технологическое окно с 19:00 до 08:00 следующего дня (местное время Заказчика) с уведомлением о проведении работ и риске недоступности за один рабочий день до начала работ. |
| **Минимальное время предупреждения о регламентных работах** | 1 рабочий день |
| **Минимальное время предупреждения о неотложных ремонтных работах**  | 2 астрономических часа |

* 1. **Параметры исполнения стандартных запросов**

В случае если Запрос требует согласования ответственными сотрудниками Заказчика или Исполнителя, время проведения такого согласования не учитывается в суммарном времени выполнения Запроса.

* + 1. Определение критичности запросов

|  |  |  |
| --- | --- | --- |
| **№** | **Критичность запроса** | **Описание** |
| 1 | Критичный | Полное прерывание работы кластера горячего резервирования продолжительностью более 15 минут.  |
| 2 | Высокий | Полное прерывание работы одиночного АПКШ продолжительностью более 15 минут, периодически возникающие прерывания в штатной работе криптошлюза / кластера горячего резервирования продолжительностью не более 15 минут, возникающие с периодичностью не более 1 раза в 1 час |
| 3 | Стандартный | Неработоспособность вспомогательных функций (неработоспособность отдельных услуг, модуля мониторинга хода исполнения услуг) криптошлюза/кластера горячего резервирования |

1. **Запросы на обслуживание**

Таблица 2. Параметры выполнения запросов на обслуживание

| Вид запроса | Максимальное допустимое время обработки запроса, в зависимости от приоритета, рабочих часов\* | Согласо-вание запроса | Форма подачи  |
| --- | --- | --- | --- |
| Критичный | Высокий | Стандартный |
| **Консультационные услуги**  | - | - | 80 рабочих часов | Не требуется | Телефонное обращениеЭлектронная почта |
| **Стандартный запрос** | 8 астроно-мических часов | 24 рабочих часа | 40 рабочих часов | Не требуется | Телефонное обращение Электронная почта |

* Исполнитель обязуется соблюдать сроки решения запросов при своевременном предоставлении результатов первичной диагностики Заказчиком.
* Регистрация инцидентов критичного приоритета возможна при условии использования схемы с резервированием защищенного канала (кластер горячего резервирования).
* В случае использования одиночного криптошлюза вместо кластера горячего резервирования, максимально допустимое время отработки запроса удваивается.
* В случае использования криптошлюза с «холодным» резервированием время на организацию монтажа Заказчиком запасного Оборудования и предоставления удаленного доступа к нему не учитывается в общем времени исполнения Запроса.
	1. **Условия предоставления услуги и ограничения.**

В случае нарушения условий предоставления услуги и ограничений, перечисленных в таблице (Таблица 3. Условия предоставления услуги и ограничения), Исполнитель не несет ответственности за сроки выполнения Запросов, указанные в таблице (Таблица 2. Параметры выполнения Запросов на обслуживание) для всех Запросов, которые были зарегистрированы после нарушения указанных условий и ограничений.

Таблица 3. Условия предоставления услуги и ограничения

| **№ п/п** | **Условие/ограничение** | **Параметр** |
| --- | --- | --- |
| 1 | Максимальное количество Запросов (за календарный месяц) всех видов на один Защищенный канал передачи данных | *<=5* |
| 2 | Наличие действующего ключа технической поддержки производителя на используемое криптооборудование в течение всего времени оказания услуги | *= количеству криптошлюзов* |

**Приложение № 6**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Технические параметры подключения**

**Подключение кластера или одиночного криптошлюза**

1. Для организации подключения кластера горячего резервирования или одиночного криптошлюза Заказчик:

* 1. Обеспечивает выделение IP адресов в сети Заказчика, в соответствии с типовой схемой и таблицей:

|  |  |  |
| --- | --- | --- |
| **№** | **IP адрес/маска** | **Назначение** |
| 1 | ip/mask ext | Активный адрес внешних интерфейсов. Может быть как из частного, так и из публичного адресного пространства |
| 2 | ip/mask int | Активный адрес внутренних интерфейсов. Ip ext и ip int обязательно должны принадлежать разным подсетям. |
| 3 | ip gw ext | Адрес шлюза по умолчанию в сети, в которую включаются внешние интерфейсы. |
| 4 | ip fw | Публичный транслируемый адрес, через который осуществляется доступ к внешнему адресу (п. 1). Указывается в случае использования частных адресов на внешних интерфейсах. |
| 5 | ip gw int | Адрес шлюза для доступа к внутренним ресурсам Заказчика.Указывается в случае нахождения ресурсов Заказчика (п. 7) и внутренних интерфейсов (п. 2) в разных сетях. |
| 6 | ip res | Адрес ресурса Заказчика, либо адрес трансляции, с которого идут обращения через защищенный канал  |

* 1. Обеспечивает физическое размещение Оборудования Заказчика, в зависимости от модели оборудования:
* Для АПКШ «Континент» IPS-3000\IPS-1000\IPS-400 одно место размером 19 дюймов Rack 2U (для установки в стойку глубиной от 480 мм и более) 88 x 445 x 490 мм (ВхШxГ);
* Для АПКШ «Континент» IPS-100 одно место размером 19 дюймов Rack 1U (для установки в стойку глубиной от 480 мм и более) 45 х 437 x 417 мм (ВхШxГ);
* Для АПКШ «Континент» IPS-25 место размером 155х275х45 мм (ГxШxВ);
* Для АПКШ «Континент» IPS-10 место размером 33,4 х 216 x 134,2 мм (ВхШxГ).
	1. Обеспечивает подключение оборудования максимальной потребляемой мощностью 200 Вт (каждый) к сети гарантированного электропитания питания 220 В с помощью кабеля типа С13 – СЕЕ7/7 (евровилка);
	2. Обеспечивает возможность подключения к сетевому оборудованию Заказчика интерфейсов криптошлюзов с использованием интерфейсов Ethernet Base T 100/1000;
	3. Обеспечивает связность на втором уровне модели OSI/ISO внутренних и отдельно внешних интерфейсов криптошлюзов, другими словами, размещение двух физических внутренних интерфейсов - в одном широковещательном сегменте, внешних - в другом;
	4. Обеспечивает отсутствие логических препятствий для прохождения трафика по протоколу UDP, TCP и по портам 4431, 4444, 4445, 4446, 5100-5103, 4433, 7500, 10000-1031, 5101, 5106, 5107, 5557 между внешним адресом (ip ext) и адресами криптошлюзов сети ЕБС.
	5. При использовании частных адресов на внешних интерфейсах – обеспечивает статическую трансляцию адреса частного внешнего адреса (ip ext) в публичный адрес (ip fw) и трансляцию публичного адреса (ip fw) в частный внешний адрес (ip ext) по протоколам и портам согласно п.п. 1.6.
	6. Обеспечивает трансляцию адресов ресурсов Заказчика в один адрес (ip res), принадлежащий сети внутреннего адреса (ip int). В случае невозможности выделения адреса из сети внутреннего адреса - обеспечивает маршрутизацию в локальной сети Заказчика таким образом, чтобы трафик с адреса ресурсов Заказчика (ip res), отправляемый на серверы ЕБС, направлялся на внутренний адрес (ip int).

**Приложение № 7**

**к публичной оферте о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих собранные биометрические персональные данные физических лиц, на технологическом участке обработки собранных биометрических персональных данных физических лиц с целью регистрации их в ЕБС с использованием СМЭВ, путем их подписания УКЭП Исполнителя, реализуемых СКЗИ класса не ниже КВ (средствами электронной подписи класса не ниже КВ2) без размещения средств защиты информации и подписания на территории Заказчика**

**Контактные данные ответственных лиц Заказчика**

|  |  |  |  |
| --- | --- | --- | --- |
| **Контактные данные** | **Рабочий телефон** | **Мобильный телефон** | **Е-mail** |
| **Сотрудник, ответственный за подключение** |  |  |  |
| ФИО |  |
| **Сетевой инженер** |  |  |  |
| ФИО |  |
| **Лицо, ответственное за информационную безопасность** |  |  |  |
| ФИО |  |
| **Объект подключения** | **Адрес** | **Этаж** | **Помещение** |
|  |  |  |
| **Используемое** **криптооборудование** |  |  |  |
| **Лицензионный номер** |  |  |  |
| **Заводской номер** |  |  |  |