

ПУБЛИЧНАЯ ОФЕРТА

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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

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 № 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 – Оферта) предлагает организациям и органам власти, соответствующим требованиям, указанным в Оферте, именуемым в дальнейшем «**Заказчик**», заключить соглашение на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью регистрации их в ГИС 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 (далее – Соглашение). Оферта в соответствии с пунктом 2 статьи 437 Гражданского кодекса Российской Федерации (далее – ГК РФ) является официальным предложением АО «ЦБТ» о заключении Соглашения. В случае полного и безоговорочного принятия изложенных ниже условий, Заказчик посредством акцепта Оферты путем совершения последовательных конклюдентных действий, указанных в п. 3.1 Соглашения, заключает настоящее Соглашение, в результате чего Заказчик и Исполнитель становятся Сторонами Соглашения.

1. Термины и определения

Термины, определения и сокращения, используемые в настоящем Соглашении, имеют следующее значения:

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Вектор Единой биометрической системы (далее – Вектор ГИС ЕБС) – персональные данные, полученные в результате математического преобразования биометрических персональных данных Клиента, содержащихся в Единой биометрической системе, которое произведено с использованием информационных технологий и технических средств, соответствующих требованиям Закона № 572-ФЗ.

ЕСИА – Федеральная государственная информационная система «Единая

система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

Заказчик – государственный орган, орган местного самоуправления, Центральный банк Российской Федерации, организация финансового рынка, иная организация, индивидуальный предприниматель, нотариус.

Защищенный канал – защищенный шифрованием канал связи с использованием СКЗИ класса КСЗ, используемый при осуществлении доступа к информационной инфраструктуре Исполнителя. Организация доступа к такому каналу, а также интеграция с ним Информационных систем Заказчика являются обязанностью Заказчика и не входят в обязательства Исполнителя по настоящему Соглашению.

Информационная система Заказчика (далее – ИС Заказчика) – система Заказчика, подключенная к ГИС ЕБС в соответствии с Регламентом.

Личный кабинет Единой биометрической системы (далее – ЛК ГИС ЕБС) – авторизованная часть Сайта Исполнителя, которая позволяет Заказчику взаимодействовать с Исполнителем в рамках Соглашения.

Личный кабинет ЕСИА (далее – ЛК ЕСИА) – это авторизованная часть единого портала Госуслуги по адресу в сети Интернет <https://esia.gosuslugi.ru/>, которая позволяет Заказчику получить доступ к ЛК ГИС ЕБС в рамках оказания Услуг.

Отчетный период – период, в течение которого оказывались Услуги, равный календарному кварталу.

Облачное типовое решение по информационной безопасности (далее также ОТИБ) – сервис электронной подписи биометрических персональных данных для взаимодействия с ГИС ЕБС.

Программное обеспечение (ПО) – интеграционное программное обеспечение Исполнителя, размещаемое (устанавливаемое) на территории Заказчика и осуществляющее предоставление интеграционных интерфейсов для информационной системы Заказчика при оказании Услуги.

Регистрация – присвоение Исполнителем номера Соглашения и фиксация даты его заключения с занесением указанных данных в информационные системы Исполнителя, а также присвоение и направление Заказчику такой Регистрационной информации, осуществляемое Исполнителем по результатам подтверждения соответствия Заказчика требованиям Оферты.

Процесс размещения сведений – размещение в Единой биометрической системе биометрических персональных данных физического лица в соответствии с Законом № 572-ФЗ.

Реестр размещений – совокупность информации о суммарном количестве размещений биометрических персональных данных физического лица в Единой биометрической системе в течение Отчетного периода.

Регистрационная информация – ключ доступа и/или иная аналогичная информация, с использованием которой Заказчик может начать пользоваться Услугами на условиях настоящего Соглашения.

Регламент по подключению к Облачному типовому решению по информационной безопасности (далее – Регламент) – документ, являющийся неотъемлемой частью Соглашения, размещенный на Сайте Исполнителя в разделе «Доступные материалы» во вкладках «ТИБ, ОТИБ, КриптоSDK, TLS», в соответствии с которым осуществляется взаимодействие Сторон по настоящему Соглашению.

Сайт Исполнителя – <https://ebs.ru/>.

СМЭВ – Единая система межведомственного электронного взаимодействия.

СКЗИ – средство криптографической защиты информации.

Тариф – размер платы за Услуги, определяемый исходя из информации, содержащейся в Реестре размещений за соответствующий Отчетный период. Тариф опубликован на Сайте Исполнителя <https://ebs.ru/documents/>.

Услуги – обеспечение Процесса размещения, включая осуществление контроля целостности и подтверждение подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц на технологическом участке обработки биометрических персональных данных физических лиц с целью их размещения 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, включающие в себя:

- настройку криптографического оборудования Заказчика в целях формирования Заказчиком Защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3 (в соответствии с Приложением № 6);
- техническое обслуживание Защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3 (в соответствии с Приложением № 5);
- предоставление доступа к криптографическому шлюзу в целях формирования Заказчиком Защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3;
- криптографическую аутентификацию Заказчика при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КС3.

УПД – универсальный передаточный документ, который объединяет в себе счет-фактуру и первичный документ по Услугам в Отчетном периоде.

Электронная почта Заказчика – адрес электронной почты Заказчика, указываемый им в Форме.

2. Предмет Соглашения

2.1. В рамках настоящего Соглашения Исполнитель обязуется оказать Заказчику Услуги, а Заказчик обязуется принять Услуги, а также выполнить иные обязательства, предусмотренные Соглашением. 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.

2.2. Разработка сервисов взаимодействия ИС Заказчика с ГИС ЕБС и иного программного обеспечения для подключения ИС Заказчика к ГИС ЕБС, работы по

подключению и интеграции ИС Заказчика с ЕСИА и/или СМЭВ, приобретение дополнительного программного обеспечения для обеспечения взаимодействия ИС Заказчика с ГИС ЕБС не входят в состав Услуг и не относятся к предмету настоящего Соглашения. Указанные в настоящем пункте Соглашения условия оказания Услуг обеспечиваются Заказчиком самостоятельно и за собственный счет.

2.3. В целях обеспечения возможности оказания Услуг Исполнитель предоставляет Заказчику права использования ПО на условиях простой (неисключительной) лицензии в следующем объеме:

- территория использования ПО – Российская Федерация;
- срок использования соответствует сроку действия настоящего Соглашения;
- отсутствие обязанности предоставления Исполнителю отчетов об использовании ПО;
- запрет сублицензирования (предоставление прав использования ПО третьим лицам);
- запрет внесения в ПО изменений, сокращений и дополнений.

Способы использования ПО:

- право на воспроизведение ПО (право на установку без ограничений по количеству, составу оборудования, в памяти которого может быть воспроизведено ПО и без ограничений мест его установки) путем установки, копирования, запуска (без ограничений по количеству запусков) для использования по функциональному назначению;
- право на адаптацию, настройку (конфигурирование) и интеграцию;
- право на копирование ПО целиком или в части для целей восстановления после отказа системы или для целей архивации, а также в иных случаях, прямо предусмотренных.

Лицензионное вознаграждение за использования ПО Заказчиком включено в стоимость Услуг по Соглашению (учтено при формировании Тарифа).

2.4. ПО, 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.

2.5. Исполнитель вправе в одностороннем порядке, но в строгом соответствии с п. 4.5 данного Соглашения, изменять условия Соглашения путем опубликования на Сайте Исполнителя нового текста Оферты, в том числе путем внесения изменений в действующую редакцию Оферты (далее – Обновлённая Оферта). Изменения вступают в силу на 6 (шестой) рабочий день с даты размещения текста Обновленной Оферты на Сайте Исполнителя. Заказчик обязуется самостоятельно ознакомиться с текстом Обновленной Оферты и соблюдать ее условия с даты вступления в силу. Аналогичным образом Исполнитель вправе внести изменения в Регламент (далее – Обновленный Регламент).

Изменение условий Соглашения и (или) Регламента в целях приведения в соответствие с требованиями законодательства, регулирующего соответствующие отношения, возникающие по Соглашению, в том числе при осуществлении размещения биометрических персональных данных физических лиц с использованием ГИС ЕБС, вступают в силу одновременно с вступлением в силу соответствующих положений нормативно-правовых актов.

2.6. 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.

2.6.1. Заказчик дает Исполнителю свое безоговорочное предварительное согласие на соответствующую передачу прав и обязанностей Исполнителя по Соглашению, указанную в п.2.6.Соглашения, любому третьему лицу.

2.6.2. Исполнитель обязуется незамедлительно (не позднее дня, следующего за днем передачи, указанной в п. 2.6. Соглашения) уведомить Заказчика о такой передаче своих прав и обязанностей по Соглашению третьему лицу путем опубликования информации на Сайте Исполнителя (далее – уведомление) с указанием в уведомлении даты передачи и сведений о новом Исполнителе по Соглашению, необходимых для надлежащего исполнения Соглашения со стороны

Заказчика. Заказчик обязуется самостоятельно ознакомиться с таким уведомлением.

2.7. Стороны признают способ уведомления, указанный в п. 2.6.2 Соглашения, надлежащим, а момент (день) публикации/размещения уведомления моментом (днем) получения Заказчиком соответствующего и надлежащего уведомления. Заказчик считается уведомленным о передаче прав и обязанностей новому Исполнителю с момента (дня) публикации/размещения Заказчиком уведомления (п. 2.6.2. Соглашения).

2.8. Заказчик подтверждает и гарантирует, что криптооборудование, используемое на стороне Заказчика для подключения к информационной инфраструктуре Исполнителя, выбранное согласно Приложению № 2 и указанное в Приложении № 3, 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.

2.9. Настройка криптографического оборудования Заказчика в целях формирования Заказчиком Защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КСЗ выполняется Исполнителем в соответствии с перечнем работ по настройке криптографического оборудования (Приложение № 4). Параметры и условия технического подключения – в соответствии с Приложением № 6.

2.10. Техническое обслуживание Защищенного канала Заказчика при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КСЗ выполняется Исполнителем в соответствии с перечнем оказываемых услуг по техническому обслуживанию Защищенного канала (Приложение № 5).

3. Акцепт оферты

3.1. Акцепт производится Заказчиком в соответствии с условиями настоящего раздела Соглашения. Услуги оказываются при условии соответствия Заказчика

требованиям Оферты и законодательства РФ. Подтверждением согласия с условиями настоящего Соглашения и акцептом Оферты является осуществление Заказчиком следующих последовательных действий:

3.1.1. Для Заказчика, имеющего доступ в авторизованную зону Сайта Исполнителя посредством ЛК ГИС ЕБС, с использованием учетных данных ЛК ЕСИА:

3.1.1.1. заполнение форм в соответствии с Приложением № 1 (далее – Формы) в ЛК ГИС ЕБС;

3.1.1.2. направление заполненных Форм посредством нажатия на кнопку «Акцептовать» в ЛК ГИС ЕБС с приложением сканированных копий подтверждающих документов, как это указано в Приложении № 1, с одновременным направлением на электронный адрес Исполнителя – business@ebs.ru – письмом по электронной почте сканированных копий документов, подписанных уполномоченным представителем Заказчика, с приложением документального обоснования наличия таких полномочий, с электронной почты Заказчика. Дата такой отправки, которая является датой акцепта Заказчиком Оферты, определяется автоматически в ЛК ГИС ЕБС. Исполнитель проверяет предоставленные Заказчиком сведения в Формах на соответствие Закона № 572-ФЗ в течение 10 (десяти) рабочих дней с даты акцепта настоящей Оферты Заказчиком (дата и действие, указанные в п. 3.1.1.2. Соглашения), проводит Регистрацию в случае, если представленная в Формах и подтверждающих документах информация соответствует требованиям Оферты и направляет на электронную почту Заказчика Регистрационную информацию для подключения ИС Заказчика к ГИС ЕБС, а также указывает дату регистрации. На предоставленную Регистрационную информацию распространяется режим конфиденциальности, предусмотренный разделом 7 настоящего Соглашения. В случае, если представленная в Формах и подтверждающих документах информация не соответствует требованиям Соглашения, Исполнитель направляет Заказчику на электронную почту Заказчика мотивированный отказ от регистрации Оферты. Заказчик обязан поправить информацию в Формах и направить ее повторно в соответствии с п. 3.1.1. Соглашения. Иные регламентные сроки и процедуры в рамках Соглашения указаны в том числе в Регламенте.

3.1.2. Для Заказчика, не имеющего доступ в авторизованную зону Сайта Исполнителя посредством ЛК ГИС ЕБС, с использованием учетных данных ЛК ЕСИА:

3.1.2.1. заполнение Форм и выбора Услуг(и);

3.1.2.2. направление сканированных копий Форм и подтверждающих документов, как это указано в Приложении № 1, подписанных уполномоченным представителем Заказчика с приложением документального обоснования наличия таких полномочий на электронный адрес Исполнителя – business@ebs.ru – письмом по электронной почте (далее – Письмо) с электронной почты Заказчика. Дата отправки Письма является датой акцепта Заказчиком Оферты и фиксируется Исполнителем. Исполнитель проверяет предоставленные Заказчиком сведения в Формах и подтверждающих документах на соответствие Закона № 572-ФЗ в течение 10 (десяти) рабочих дней с даты получения Письма (дата и действие, указанные в п. 3.1.2.2. Соглашения), проводит Регистрацию в случае, если представленная в Формах и подтверждающих документах информация соответствует требованиям Оферты и направляет на электронную почту Заказчика Регистрационную информацию для подключения ИС Заказчика к ГИС ЕБС, а также указывает дату Регистрации. На предоставленную Регистрационную информацию распространяется режим конфиденциальности, предусмотренный разделом 7 настоящего Соглашения. В случае, если представленная в Формах и подтверждающих документах информация не соответствует требованиям Соглашения, Исполнитель направляет на электронную почту Заказчика мотивированный отказ от регистрации Оферты. Заказчик обязан поправить информацию в Формах и направить ее повторно в соответствии с п. 3.1.2. Соглашения. Иные регламентные сроки и процедуры в рамках Соглашения указаны в том числе в Регламенте.

3.2. Датой начала оказания Услуги при акцепте Оферты считается:

3.2.1 дата регистрации Оферты (для п. 3.1.1. и п. 3.1.2.). Регистрация возможна только после выполнения Заказчиком требований Регламента.

3.3. В результате акцепта (п. 3.1. Соглашения) Заказчик и Исполнитель становятся Сторонами настоящего Соглашения.

4. Стоимость услуг и порядок расчетов

- 4.1. Исполнитель вправе взимать с Заказчика плату за оказание Услуг.
- 4.2. Размер оплаты Услуг за Отчетный период зависит от применяемого Заказчиком Тарифа.
- 4.3. Оплата Услуг, оказанных Заказчику, производится в течение 10 (десяти) календарных дней с даты приемки Заказчиком оказанных Услуг в соответствии с разделом 6 настоящего Соглашения.
- 4.4. Информация о размере и порядке определения стоимости Услуг с разбивкой по действующим Тарифам размещена на сайте Исполнителя в разделе «Документы», вкладка «Тарифы, оферты, соглашения».
- 4.5. В случае изменения условий о формировании стоимости Услуг (изменении Тарифа) по Соглашению, Исполнитель обязуется известить об этом Заказчика в соответствии с п. 2.5. Соглашения (путем размещения соответствующей информации на Сайте Исполнителя).

5. Права и обязанности Сторон

- 5.1. Заказчик обязан обеспечить взаимодействие ИС Заказчика с ОТИБ согласно требованиям, указанным в Регламенте.
- 5.2. На момент заключения Соглашения Заказчик гарантирует готовность взаимодействия ИС Заказчика с ГИС ЕБС и Программного обеспечения для подключения ИС Заказчика к ГИС ЕБС. 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.
- 5.3. Заказчик обязуется выполнить все предписанные действия, указанные в документации к Услуге, размещенной на портале <https://ebs.ru/documents/tibkriptosdktls/>, 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.
- 5.4. 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. Оказание Услуг осуществляется через информационно-телекоммуникационную сеть «Интернет» (далее – сеть Интернет). Организация доступа к сети Интернет обеспечивается Заказчиком самостоятельно и за собственный счет и не входит в обязанности Исполнителя по настоящему Соглашению.

5.5. 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.

5.6. Исполнитель оказывает Услуги при наличии технической возможности.

5.7. Исполнитель обязан немедленно известить Заказчика и до получения от него указаний приостановить исполнение обязательств по настоящему Соглашению при обнаружении не зависящих от Исполнителя обстоятельств, угрожающих качеству результатов исполнения обязательств по настоящему Соглашению либо создающих препятствия по их исполнению в установленный срок.

5.8. Исполнитель вправе привлекать в целях должного выполнения настоящего Соглашения третьих лиц без согласования с Заказчиком/уведомления Заказчика, принимая на себя перед Заказчиком ответственность за их действия как за свои собственные.

5.9. Исполнитель имеет право приостановить оказание Услуг в срок приостановления оказания Услуг – до момента устранения Заказчиком оснований

такого приостановления.

О приостановке оказания Услуг Исполнитель направляет соответствующее сообщение на электронную почту Заказчика. При этом в случае, если приостановление Услуг длится более 6 (шести) месяцев с даты направления соответствующего сообщения Исполнителем, Исполнитель вправе расторгнуть Соглашение в одностороннем внесудебном порядке путем направления соответствующего уведомления Заказчику. Соглашение считается расторгнутым с даты вручения такого уведомления Заказчику.

5.10. Заказчик обязан представить Исполнителю сведения об уполномоченных лицах, ответственных за исполнение настоящего Соглашения, их номерах телефонов в Форме (Приложение № 1). В случае внесения изменений в перечень ответственных лиц, Заказчик обязан своевременно ставить об этом в известность Исполнителя. Сведения, указанные в настоящем пункте, предоставляются Заказчиком в виде соответствующего сообщения на адрес электронной почты Исполнителя – business@ebs.ru.

5.11. В течение 5 (пяти) рабочих дней со дня Регистрации Исполнитель обязан направить Заказчику по электронной почте, указанной в Форме:

- образцы подписей лиц, которые будут подписывать выставляемые в адрес Заказчика УПД;
- документы, подтверждающие полномочия лиц, которые будут подписывать УПД (заверенные надлежащим образом приказы, распоряжения, доверенности, копии банковских карточек или иные аналогичные документы) в случае, если право их подписи предоставлено иным лицам, кроме руководителя и главного бухгалтера.

5.12. 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.

5.13. 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/>.

5.14. Исполнитель имеет право периодически проводить работы по техническому обслуживанию. Данные работы называются плановыми работами и могут привести к перерывам в оказании Услуг и не считаются нарушением обязательств по оказанию Услуг.

5.15. Исполнитель информирует Заказчика о возможных перерывах в оказании Услуги при проведении плановых работ минимум за 24 (двадцать четыре) часа отправкой уведомления на электронную почту Заказчика.

5.16. Заказчик обязан осуществить действия по обеспечению безопасности собственного доступа в сеть Интернет.

5.17. В рамках исполнения Соглашения Заказчик присоединяется к Антикоррупционной политике Исполнителя, размещенной по адресу <https://ebs.ru/documents/>.

5.18. Исполнитель вправе разместить на Сайте Исполнителя перечень наименований Заказчиков, с которыми заключено Соглашение.

6. Приемка Услуг

6.1. Заказчики вправе направить запрос Исполнителю в отношении объема Услуг в Отчетном периоде на адрес электронной почты Исполнителя – business@ebs.ru – для предоставления Реестра размещений (далее – Реестр). Исполнитель обязан предоставить такой Реестр в течение 5 (пяти) календарных дней. Услуги в Отчетном периоде для указанных Заказчиков считаются оказанными в полном объеме, в срок и принятыми Заказчиком на пятый рабочий день с даты

окончания Отчетного периода, при этом обмен документами Сторонами не предусмотрен.

6.2. Не позднее 5 (пяти) рабочих дней с даты окончания Отчетного периода Исполнитель оформляет и отправляет Заказчику УПД, подписанный со своей стороны (посредством ЭДО/по почте/курьерской службой/нарочным Заказчику, п. 12.4. Соглашения). В УПД указывается стоимость оказанных Услуг в Отчетном периоде.

6.3. Заказчик обязуется подписать УПД в течение 5 (пяти) рабочих дней с даты его получения от Исполнителя или направить письменный мотивированный отказ от его подписания в тот же срок.

6.4. В случае получения Исполнителем мотивированного отказа, Стороны согласовывают изменения в УПД не позднее чем через 5 (пять) рабочих дней с даты получения Исполнителем мотивированного отказа от Заказчика.

6.5. В случае непредставления Заказчиком подписанного УПД или мотивированного отказа в срок, установленный в п. 6.2 настоящего Соглашения, Услуги считаются оказанными в полном объеме, в срок и принятыми Заказчиком, УПД считается подписанным Сторонами на пятый рабочий день с даты получения УПД (дата отметки ЭДО либо дата, указанная п. 12.4. Соглашения).

6.6. Услуги в Отчетном периоде для указанных Заказчиков считаются оказанными в полном объеме, в срок и принятыми Заказчиком на пятый рабочий день с даты окончания Отчетного периода, при этом обмен документами Сторонами не предусмотрен.

6.7. Подписанный Сторонами УПД с учетом положений п. 6.4. и п. 6.5. Соглашения удостоверяет факт принятия Заказчиком оказанных Услуг в полном объеме.

7. Конфиденциальность

7.1. 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).

7.2. Передающая Сторона – сторона, которой может быть как Исполнитель, так и Заказчик, передающая на условиях настоящего Соглашения Конфиденциальную информацию.

7.3. Получающая Сторона – сторона, которой может быть как Исполнитель, так и Заказчик, получающая от Передающей Стороны на условиях настоящего Соглашения Конфиденциальную информацию.

7.4. Представители – директора, должностные лица, сотрудники, юристы, бухгалтеры, аудиторы, финансовые консультанты, аффилированные лица Стороны, которые уполномочены раскрывать и/или получать Конфиденциальную информацию.

7.5. Третьи лица – иные лица, не относящиеся к Сторонам и их Представителям.

7.6. 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.

7.7. 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.

7.8. 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).

7.9. 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.

7.10. 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.

7.11. Получающая Сторона соглашается, что Конфиденциальная информация будет использована исключительно в связи с исполнением Соглашения и что Получающая Сторона и ее Представители сохраняют 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.

7.12. 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.

7.13. 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.

7.14. 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.

7.15. 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.

7.16. 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.

7.17. 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.

7.18. 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.

7.19. Передающая Сторона настоящим гарантирует, что она обладает всеми правами в отношении Конфиденциальной информации, включая право передавать такую информацию Получающей Стороне на условиях настоящего Соглашения.

7.20. 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.

7.21. 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.

7.22. 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.

8. Ответственность Сторон

8.1. При нарушении обязательств по настоящему Соглашению Стороны несут ответственность согласно действующему законодательству Российской Федерации и настоящему Соглашению.

8.2. При нарушении Заказчиком обязательств по оплате Услуг, Исполнитель вправе потребовать от Заказчика выплаты неустойки в размере 0,1 % (ноль целых одна десятая процента) от неоплаченной в срок суммы за каждый день просрочки.

8.3. Выплата неустойки по настоящему Соглашению осуществляется только на основании письменной претензии (требования). Если письменная претензия одной Стороны не будет направлена в адрес другой Стороны, неустойка не начисляется и не уплачивается. Оплата неустойки производится не позднее 10 (десяти) календарных дней со дня поступления письменной претензии (требования), а также документов, подтверждающих требования, изложенные в претензии.

8.4. Сторона освобождается от уплаты неустойки, если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного настоящим Соглашением, произошло вследствие непреодолимой силы или по вине другой Стороны.

8.5. Исполнитель не несет ответственности за какие-либо убытки, возникшие не по вине Исполнителя вследствие ненадлежащего использования или невозможности воспользоваться Услугами.

8.6. В случае использования Заказчиком компьютерного и иного оборудования, каналов связи и (или) программ для ЭВМ, принадлежащих третьим лицам, при оказании Услуг Стороны соглашаются с тем, что Исполнитель не несёт ответственность за любые задержки, прерывания, прямой ущерб или упущенную выгоду, потери, происходящие из-за дефектов в любом электронном или механическом оборудовании и (или) программах для ЭВМ, либо вследствие иных объективных технологических причин, а также в результате действий или бездействий третьих лиц, проблем при передаче данных или соединении, перебоев в электропитании, произошедших не по вине Исполнителя.

8.7. Исполнитель при отсутствии его вины не несет ответственности перед Заказчиком за остановку производства, потерю данных, упущенную выгоду и любые другие косвенные потери и их последствия, в том числе возникшие в результате перерывов в оказании Услуг, вне зависимости от того мог или нет Исполнитель предвидеть возможность таких потерь в конкретной ситуации.

8.8. Исполнитель не несет ответственности за нарушение прав третьих лиц, возникших в результате действий Заказчика, совершенных с использованием Услуг.

8.9. Исполнитель не несет ответственность за принадлежность данных, предоставленных физическим лицом, Биометрическим персональным данным Клиента.

9. Обстоятельства непреодолимой силы

9.1. 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.

9.2. При наступлении обстоятельства непреодолимой силы Сторона, для которой создалась невозможность исполнения своих обязательств по Соглашению, должна в течение 10 (десяти) календарных дней письменно уведомить другую Сторону о таком обстоятельстве и причине его возникновения, а также предоставить документальное подтверждение действия обстоятельств непреодолимой силы, указанных в уведомлении, выданное компетентным государственным органом. Срок исполнения обязательств отодвигается соразмерно времени, в течение которого будут действовать обстоятельства непреодолимой силы.

9.3. Если указанные обстоятельства будут продолжаться более 3 (трех) месяцев, то каждая из Сторон имеет право отказаться от дальнейшего исполнения обязательств по настоящему Соглашению. В этом случае Стороны должны провести взаиморасчеты за фактически оказанные услуги.

10. Обработка персональных данных

10.1. Стороны гарантируют наличие законных оснований для осуществления передачи персональных данных, операторами которых они являются.

10.2. Сторона, получившая персональные данные от другой Стороны, не принимает на себя обязательства по информированию субъектов, чьи персональные данные ей переданы, о начале их обработки, полагая, что они проинформированы об этом Стороной, передавшей их персональные данные.

10.3. Стороны обязуются обеспечивать конфиденциальность и безопасность передаваемых друг другу персональных данных при их обработке, а также принимать необходимые организационные и технические меры, соответствующие требованиям ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

11. Порядок рассмотрения споров

11.1. Все споры и разногласия, которые могут возникнуть из-за настоящего Соглашения или в связи с ним, Стороны решают путем переговоров.

11.2. Претензионный порядок урегулирования споров будет применяться Сторонами в случаях, предусмотренных законом и настоящим Соглашением. Претензия в рамках Соглашения может быть направлена с использованием электронной почты, указанной Сторонами в заполненной в соответствии с Формой. Оригиналы направляются по почте/курьерской службой/нарочным с уведомлением о доставке. Датой доставки документов считается дата доставки электронного сообщения. Срок рассмотрения претензии 10 (десять) рабочих дней с момента ее доставки.

11.3. В случае, если споры и разногласия не урегулированы в соответствии с п. 11.2 настоящего Соглашения, каждая из Сторон вправе обратиться в Арбитражный суд г. Москвы с иском о разрешении спора.

12. Срок действия Соглашения, условия его расторжения

Иные условия Соглашения

12.1. Настоящее Соглашение вступает в силу с даты акцепта Оферты и действует бессрочно.

12.2. Соглашение может быть прекращено:

- по соглашению Сторон;
- по инициативе Исполнителя (односторонний отказ от исполнения Соглашения) в случае невыполнения Заказчиком требований, предусмотренных п. 2.8. либо п. 5.2. настоящего Соглашения. При этом Исполнитель обязан уведомить Заказчика о расторжении не менее чем за 10 (десять) календарных дней до предполагаемой даты прекращения Соглашения;
- по инициативе Заказчика (односторонний внесудебный отказ от исполнения Соглашения). При этом Заказчик обязан уведомить Исполнителя о расторжении не менее чем за 30 (тридцать) календарных дней до предполагаемой даты прекращения Соглашения;
- по инициативе Исполнителя по основаниям, не связанным с нарушением Соглашения (односторонний внесудебный отказ от исполнения Соглашения). 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.

12.3. При расторжении настоящего Соглашения по любым основаниям его положения будут применяться к отношениям Сторон вплоть до полного окончания взаимных расчётов и передачи необходимой документации.

12.4. В случае если документы, касающиеся настоящего Соглашения, отправляются почтовой связью, доказательством отправления этих документов является почтовое уведомление с указанием даты о вручении почтового отправления Стороне и отсчет срока идет с даты отметки о вручении на почтовом уведомлении. О доставке документов, отправленных почтовой связью, Сторона, их

получившая, не позднее следующего рабочего дня обязана уведомить Сторону, отправившую документы, путем направления соответствующего сообщения на адрес электронной почты, указанный Сторонами в настоящем Соглашении. УПД, любые уведомления, направляемые Сторонами в рамках настоящего Соглашения, могут быть отправлены курьерской службой, либо вручены уполномоченным представителем Стороны, отправляющей такое уведомление, уполномоченному представителю Стороны, принимающей такое уведомление, по акту приема-передачи документов. Датой уведомления считается дата его доставки, указанная в уведомлении о вручении или доставке либо дата, указанная в акте приема-передачи документов.

13. Адреса и банковские реквизиты АО «ЦБТ»

ИНН 9705169387 КПП 770501001

р/с 40702810503800001245

Наименование банка:

ПАО Банк ВТБ г. Москва БИК 044525187

к/с 30101810700000000187

ОГРН 1227700243748

Место нахождения: 115035, город Москва, Овчинниковская набережная, д. 18/1,
стр. 2

Почтовый адрес: 115035, город Москва, Овчинниковская набережная, д. 18/1, стр. 2

АО «ЦБТ»

Генеральный директор АО «ЦБТ» В.Ю. Поволоцкий

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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 Услуге

Все поля обязательны к заполнению

I. Данные о лице, уполномоченном акцептировать Публичную оферту о заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащие биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения 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 (далее – Оферта)

1. Лицо, действующее от имени Заказчика при акцепте Оферты	
Ф.И.О.	
Должность	
Документальное обоснование полномочий	
2. Уполномоченное лицо Заказчика по Соглашению	
Ф.И.О.	
Должность	
Номер телефона	
3. Предоставление контактных данных ответственных лиц Заказчика	
Сотрудник, ответственный за подключение	
1	Ф.И.О.
2	Рабочий телефон
3	Мобильный телефон
4	Адрес электронной почты
Сетевой инженер, ответственный за подключение	
5	Ф.И.О.

6	Рабочий телефон		
7	Мобильный телефон		
8	Адрес электронной почты		
Лицо, ответственное за информационную безопасность			
9	Ф.И.О.		
10	Рабочий телефон		
11	Мобильный телефон		
12	Адрес электронной почты		
Объект подключения			
13	Адрес местонахождения		
14	Этаж		
15	Помещение		
16	Используемое криптооборудование		
17	Лицензионный номер		
18	Заводской номер		

II. Сведения о Заказчике

Полное наименование	
Сокращенное наименование	
ИНН	
КПП	
ОГРН/ОГРНИП	
Код ИФНС	
Телефон	
Адрес местонахождения (индекс, город, улица, дом)	
Адрес почтовый (индекс, город, улица, дом)	
Электронная почта Заказчика	

Перечень документов ²	Наименование и реквизиты документа, копия которого предоставляется Заказчиком	V
Устав/Учредительный договор		
Свидетельство ИНН		
Свидетельство ОГРН		
Выписка из ЕГРЮЛ		
Документ, подтверждающий полномочия подписанта Формы (если подписант не является единоличным исполнительным органом, кроме документа – основания (доверенности и т.д.), также предоставляются документы, подтверждающие полномочия единоличного исполнительного органа, уполномочившего такое лицо).		

С условиями Оферты ознакомлен и согласен. Верность указанных в Форме сведений подтверждаю.

Дата _____

Подпись/расшифровка подписи _____/_____

Приложение № 2

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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

Требования, обеспечиваемые при подключении Заказчика к информационной инфраструктуре Исполнителя с применением СКЗИ класса КСЗ

1. В целях формирования Заказчиком Защищенного канала при осуществлении доступа к информационной инфраструктуре Исполнителя с применением СКЗИ класса КСЗ используются следующие варианты типового криптографического оборудования «Код Безопасности» Заказчика:

- использование кластера АПКШ Континент 3.9 IPC-R800;
- использование одиночного АПКШ Континент 3.9 IPC-R800;
- использование кластера АПКШ Континент 3.9 IPC-R550;
- использование одиночного АПКШ Континент 3.9 IPC-R550;
- использование кластера АПКШ Континент 3.9 IPC-R300;
- использование одиночного АПКШ Континент 3.9 IPC-R300;
- использование кластера АПКШ Континент 3.9 IPC-R50;
- использование одиночного АПКШ Континент 3.9 IPC-R50.

2. В таблице 1 представлены рекомендации по выбору типа АПКШ Континент в зависимости от количества используемых Заказчиком сетевых узлов (автоматизированных рабочих мест (далее – 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-R550, IPC-R800
2	от 11 до 100	IPC-R300
3	от 1 до 10	IPC-R50

3. 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 КСЗ.

Таблица 2. Рекомендации по пропускной способности каналов связи

№ п/п	Необходимая производительность шифрования	Рекомендуемая номенклатура решений Код безопасности
1	до 2,5 Гбит/с	IPC-R800
2	до 1 Гбит/с	IPC-R550
3	до 500 Мбит/с	IPC-R300
4	до 350 Мбит/с	IPC-R50

4. 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.

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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

Требования к Оборудованию, предоставляемому Заказчиком для обеспечения возможности оказания Услуг

1. Оборудование должно представлять собой аппаратно-программный комплекс шифрования (АКПШ) с характеристиками не ниже, чем у АКПШ «Континент IPC-R50».

2. У Заказчика должно быть право на получение технической поддержки АКПШ на срок не менее одного года с даты начала его эксплуатации и с характеристиками, не ниже чем у продукта «Ключ активации сервиса прямой технической поддержки уровня «Расширенный» для АКПШ «Континент», 1 год, HSEC-SUPPORT-EXT».

3. Комплектность Оборудования и документов при передаче Исполнителю должна быть не менее чем:

- АКПШ с упаковкой производителя;
- CD диск/иной материальный носитель с документацией на АКПШ;
- паспорт на АКПШ;
- копия документа, подтверждающего право Заказчика на оказание ему технической поддержки, как указано в п. 2 выше (копии соответствующего сертификата/ключа активации и т.д.).

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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

Перечень работ по настройке криптографического оборудования

1. Выполняемые работы:

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

2. Настройка криптографического оборудования:

- Преднастройка Оборудования согласно согласованным с Заказчиком техническим параметрам подключения (Приложение № 6 к данной оферте).
- Подготовка конфигурационного и ключевого файлов для Оборудования марки «Континент» осуществляется на стороне Исполнителя в центре управления сети (ЦУС).
- Установка 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.

3. Для передачи ключевой информации Заказчику Исполнитель может привлекать третью сторону, осуществляющую такую передачу надежным способом, исключающим несанкционированный доступ.

4. 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.

5. Сопровождение работ Исполнителем производится удаленно.

6. На объекте установки Заказчик создает необходимые условия для выполнения работ.

7. Место выполняемых работ – территория Заказчика: _____.

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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

Перечень оказываемых услуг по техническому обслуживанию Защищенного канала

1. Оказываемые услуги:

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

2. Дата начала оказания Услуг исчисляется со дня подписания Сторонами акта сдачи-приемки выполненных работ по настройке защищенного канала с использованием Оборудования, указанного в Приложении № 3 к данной Оферте.

3. Техническое обслуживание защищенного канала производится в соответствии с описанием, указанным в Приложении № 5.1 к данной Оферте.

4. Место размещения поддерживаемого Оборудования – территория Заказчика: _____.

Приложение № 5.1

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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

- 1.1. Предоставление услуг Заказчику осуществляется по Запросу Заказчика.
- 1.2. Запрос направляется в Центр технической поддержки Исполнителя по электронной почте otib@ebs.ru.
- 1.3. Запрос должен содержать следующие сведения:
 - номер Оферты;
 - координаты представителя Заказчика;
 - тип, серийный номер Оборудования, аппаратного обеспечения;
 - 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.

2. Описание услуг

2.1. Технический консалтинг

В рамках действия этой услуги Исполнителем обеспечивается:

2.1.1. Регистрация запросов от уполномоченных лиц технических служб Заказчика 24 часа в сутки, 365/366 дней в году, включая выходные и праздничные дни.

2.1.2. Работы по заявкам выполняются в рабочие часы (с 9:00 до 18:00 по московскому времени), в рабочие дни (согласно законодательству Российской Федерации).

2.1.3. Консультации при возникновении у специалистов Заказчика затруднений при использовании Оборудования. Помощь и технические консультации оказываются как при первичной инсталляции, так и при эксплуатации.

2.1.4. Поддержка ключевой и справочной информации в актуальном состоянии, просмотр журналов событий, проактивная работа по поддержанию в работоспособном состоянии Защищенного канала, обеспечиваемого Оборудованием.

2.1.5. Внесение необходимых изменений в конфигурацию криптооборудования в случае изменений со стороны Заказчика.

2.1.6. Предоставление Заказчику инструкций по проведению диагностики при подозрении на неисправность Оборудования.

2.1.7. Проведение работ по поиску и локализации причин возникновения некорректной работы Оборудования и/или аппаратного обеспечения.

2.1.8. Исполнение услуг до полного устранения проблемы или до момента, когда Стороны совместно вынесут решение о нецелесообразности дальнейшей работы над проблемой.

2.1.9. Услуги оказываются при помощи средств удаленного доступа.

3. 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 (24x7)
Временной режим регистрации запросов	круглосуточно (24x7)
Временной режим решения запросов критичного приоритета	круглосуточно (24x7)
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

3.1. 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.

3.1.1. 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

4. Запросы на обслуживание

Таблица 2. Параметры выполнения запросов на обслуживание

Вид запроса	Максимальное допустимое время обработки запроса в зависимости от приоритета, рабочих часов*			Согласование запроса	Форма подачи
	Критичный	Высокий	Стандартный		
Консультационные услуги	-	-	80 рабочих часов	Не требуется	Электронная почта
Стандартный запрос	8 астрономических часов	24 рабочих часа	40 рабочих часов	Не требуется	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.

4.1. 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

О заключении соглашения на оказание услуг по осуществлению контроля целостности и подтверждения подлинности электронных сообщений, содержащих биометрические персональные данные физических лиц, на технологическом участке обработки биометрических персональных данных физических лиц с целью размещения их в ГИС 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

Параметры и условия технического подключения

Подключение кластера или одиночного криптошлюза

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

1.1. 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.

1.2. Обеспечивает физическое размещение Оборудования Заказчика в зависимости от модели оборудования;

1.3. Обеспечивает подключение оборудования максимальной потребляемой мощностью 200 Вт (каждый) к сети гарантированного электропитания питания 220 В с помощью кабеля типа C13 – CEE7/7 (евровилка);

1.4. Обеспечивает возможность подключения к сетевому оборудованию Заказчика интерфейсов криптошлюзов с использованием интерфейсов Ethernet Base T 100/1000;

1.5. Обеспечивает связность на втором уровне модели OSI/ISO внутренних и отдельно внешних интерфейсов криптошлюзов, другими словами, размещение двух физических внутренних интерфейсов – в одном широкополосном сегменте, внешних – в другом;

1.6. Обеспечивает отсутствие логических препятствий для прохождения трафика по протоколу UDP, TCP и по портам 4431, 4444, 4445, 4446, 5100-5103, 4433, 7500, 10000-10031, 5101, 5106, 5107, 5557 между внешним адресом (ip ext) и адресами криптошлюзов сети ЕБС;

1.7. 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;

1.8. 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).