**II. ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**1.** **Предмет муниципального контракта**: оказание услуг по сопровождению электронных подписей.

**2.** **Требования к предоставляемым услугам:**

2.1. Место предоставления услуг: 628260, ул. 40 лет Победы, д. 11, г.Югорск, Ханты-Мансийский автономный округ-Югра, Тюменская область.

2.2. Наименование услуг: услуги Удостоверяющего центра по созданию ключей, изготовлению, выдаче сертификатов ключей проверки электронных подписей и сопровождению выданных сертификатов ключей проверки электронных подписей с использованием Заказчиком Корпоративного центра регистрации.

2.3. Условные обозначения и сокращения:

Таблица 1. Термины и определения

| Термин / Сокращение | Определение |
| --- | --- |
| ИС | Информационная система |
| Исполнитель | Организация, оказывающая услуги по изготовлению сертификатов ключей проверки электронных подписей и сопровождению выданных сертификатов ключей проверки электронных подписей |
| Корпоративный центр регистрации (далее – КЦР)  | Сервис для реализации взаимодействия Заказчика с УЦ в процессе выдачи СКПЭП |
| Криптопровайдер | Независимый модуль, позволяющий осуществлять криптографические операции в операционных системах |
| Пользователь | Потребитель услуг по созданию и выдаче СКПЭП |
| Сертификат ключа проверки электронной подписи (далее – Сертификат, СКПЭП)  | Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи |
| СКЗИ | Средство криптографической защиты информации – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности |
| ТЗ |  Техническое задание |
| УЦ | Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом №63-ФЗ «Об электронной подписи |
| ФСБ | Федеральная служба безопасности |
| ЭП | Электронная подпись |

2.4. Состав услуг.

Перечень услуг включает:

- предоставление лицензионного программного обеспечения, необходимого для получения и использования СКПЭП;

- предоставление доступа Заказчика к КЦР;

- оказание технической и методической поддержки пользователей по вопросам использования программного обеспечения и сопровождения полученных СКПЭП сроком на 12 мес., с момента выдачи СКПЭП;

- услуги Удостоверяющего центра, представленные в п. 4.4.

**3. Этапы, сроки и объёмы оказания услуг**

3.1. Этапы и сроки оказания услуг:

1. Первый этап - подготовка и настройка ИС Заказчика для работы с КЦР.

Состав работ по данному этапу включает:

­ выдача сертификатов, генерация ключей ЭП и ключей проверки ЭП для сотрудников Заказчика, выделенных для работы в КЦР (далее – администратор КЦР);

­ разворачивание и подключение КЦР на ресурсах Заказчика к УЦ Исполнителя;

­ настройка АРМ администратора КЦР.

2. Второй этап - Выдача сертификатов электронной подписи по мере подачи заявления на выдачу сертификата сотрудниками Заказчика.

В рамках этого этапа будут проводиться работы по созданию ключей, изготовлению и выдаче сертификатов ключей проверки электронных подписей в количестве 67 СКПЭП для сотрудников Заказчика.

3. Третий этап - Сопровождение СКПЭП сроком на 12 мес., с момента выдачи СКПЭП.

В рамках этого этапа будут проводиться работы по оказанию технической и методической поддержки уполномоченных лиц по вопросам использования программного обеспечения для получения СКПЭП и сопровождения полученных СКПЭП.

3.2. Объёмы оказания услуг:

Таблица 2. Объёмы оказания услуг

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование услуг | Характеристика предоставляемых услуг | Ед.изм. | Кол-во |
| 1 | Право на использование программы для ЭВМ «АС «Кабинет УЦ» | Право на использование программы для ЭВМ «АС «Кабинет УЦ» при выпуске одного квалифицированного сертификата для работы во внешних информационных системах | шт | 67 |
| 2 | Расширение права использования программы | Расширение права использования программы для портала СМЭВ | шт | 67 |
| 3 | Оказание услуг по изготовлению сертификата администратора | Оказание услуг по изготовлению сертификата администратора программы для ЭВМ «АС «Кабинет УЦ» | шт | 2 |

 **4. Основные требования к оказываемым слугам**

4.1. Требования к СКПЭП и ЭП.

СКПЭП должны:

* соответствовать требованиям Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» в части требований к СКПЭП;
* соответствовать приказу ФСБ России №795 от 27 декабря 2011 года «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
* соответствовать криптографическим алгоритмам, определённым стандартами ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012;
* быть выпущены УЦ, аккредитованным Минкомсвязью России в соответствии с требованиями Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи»;

4.1.1. Требования к единой структуре сертификата ключа проверки электронной подписи.

Общие требования:

СКПЭП представляет собой электронный документ с электронной подписью уполномоченного лица удостоверяющего центра.

Структура и содержание СКПЭП определяются:

* Федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
* приказом ФСБ России № 795 от 27.12.2011 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
* международными рекомендациями RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».

СКПЭП должен содержать:

* обязательные поля СКПЭП;
* расширения СКПЭП.

4.1.2. Требования к составу и содержанию обязательных полей СКПЭП для физического лица.

В состав обязательных полей СКПЭП входят следующие поля:

* поле «Версия» (поле «Версия» (version) должна быть не ниже 3);
* поле «Серийный номер» (поле «Серийный номер» (serialNumber) должно содержать серийный номер СКПЭП, уникальный в пределах серийных номеров всех сертификатов, выданных УЦ, издавшего СКПЭП);
* поле «Издатель сертификата» (поле «Издатель сертификата» (issuer) идентифицирует аккредитованный УЦ, создавший и выдавший данный квалифицированный сертификат);
* поле «Срок действия сертификата» (должно содержать дату начала и дату истечения срока действия СКПЭП в формате UTC);
* поле «Владелец сертификата» (поле «Владелец сертификата» (Subject) содержит следующие компоненты имени и формируется следующим образом:
* обязательный компонент «Общее имя» (CN, CommonName), содержащий имя, фамилию и отчество физического лица;

Формат компоненты «Общее имя» (Common Name):

Длина текста не более 64 символов.

ФИО должно быть указано полностью так, как оно указано в документе, удостоверяющем личность владельца (например, паспорт).

Длина текста не более 64 символов.

* компонента «Город» (компонента «Город» (L, Locality), содержащий название населённого пункта, в котором проживает владелец сертификата. Длина текста не более 64 символов);
* компонента «Страна» (компонента «Страна» (С), содержащая название страны, в которой проживает владелец сертификата);
* компонента «Адрес электронный почты» (компонента «Адрес электронной почты» (E, EMail), содержащая адрес электронной почты владельца сертификата ключа подписи. Длина текста не более 64 символов);
* компонента «Идентификационный номер налогоплательщика владельца СКПЭП, INN» (компонента «Идентификационный номер налогоплательщика владельца СКПЭП, INN» (OID: 1.2.643.3.131.1.1). Текст длиной 12 цифр, содержащий ИНН владельца СКПЭП (10-значный код дополняется до 12-значного путём подстановки впереди текстового значения двух нулей));
* компонента «Страховой номер индивидуального лицевого счета владельца СКПЭП сертификата, СНИЛС» (компонента «Страховой номер индивидуального лицевого счета владельца СКПЭП сертификата, СНИЛС» (OID:1.2.643.100.3) страховой номер индивидуального лицевого счета владельца сертификата – физического лица, содержащий уникальный идентификатор владельца сертификата ключа подписи);
* поле «Открытый ключ» (поле «Открытый ключ» должно содержать название и алгоритм формирования открытого ключа. (Для формирования открытого ключа в соответствии с государственными стандартами Российской Федерации – ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.2.3));

Параметры и значение открытого ключа уполномоченного лица УЦ.

* поле «Доступ к информации о центрах сертификации» (должно содержать адреса распространения корневых сертификатов Удостоверяющего Центра);
* поле «Алгоритм подписи» (поле «Алгоритм подписи» должно содержать значение подписи ГОСТ Р 34.11/34.10-2012);
* поле «Средства электронной подписи и УЦ издателя» (поле «Средства электронной подписи и УЦ издателя» должно содержать наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным законом №63-ФЗ от 6 апреля 2011 г. «Об электронной подписи»).

4.1.3. Требования к составу и содержанию обязательных полей СКПЭП для юридического лица.

В состав обязательных полей СКПЭП входят следующие поля:

* поле «Версия» (version) (должна быть не ниже 3);
* поле «Серийный номер» (serialNumber) (должно содержать серийный номер СКПЭП, уникальный в пределах серийных номеров всех сертификатов, выданных УЦ, издавшего СКПЭП);
* поле «Издатель сертификата» (issuer) (идентифицирует аккредитованный УЦ, создавший и выдавший данный квалифицированный сертификат);
* поле «Срок действия сертификата» (должно содержать дату начала и дату истечения срока действия СКПЭП в формате UTC);
* поле «Владелец сертификата» (Subject)

Содержит следующие компоненты имени и формируется следующим образом:

• обязательный компонент «Общее имя» (CN, CommonName), содержащий наименование юридического лица

Формат компоненты «Общее имя» (Common Name) (Длина текста не более 64 символов):

• компонент «Фамилия» (Surname), содержащий фамилию физического лица, и компонент «приобретенное имя» (GivenName), содержащий имя и отчество физического лица (ФИО должно быть указано полностью так, как оно указано в документе, удостоверяющем личность владельца (например, паспорт));

* компонента «Должность» (T, Title) (содержит должность владельца СКПЭП для юридических лиц. Длина текста не более 64 символов);
* компонента «Организация» (O, Organization) (содержит название юридического лица. Длина текста не более 64 символов);
* компонента «Город» (L, Locality) (содержит название населённого пункта, в котором расположена организация владельца сертификата. Длина текста не более 64 символов);
* компонента «Страна» (С) (содержит название страны, в которой расположена организация владельца сертификата);
* компонента «Адрес электронный почты» (E, EMail) (содержит адрес электронной почты владельца сертификата ключа подписи. Длина текста не более 64 символов);
* компонента «Основной государственный регистрационный номер владельца СКПЭП – юридического лица, OGRN» - (OID: 1.2.643.100.1) Текст длиной 13 цифр, содержащий ОГРН юридического лица;
* компонента «Идентификационный номер налогоплательщика владельца СКПЭП, INN» - (OID: 1.2.643.3.131.1.1). Текст длиной 12 цифр, содержащий ИНН владельца СКПЭП (10-тизначный код дополняется до 12-тизначного путём подстановки впереди текстового значения двух нулей);
* компонента «Страховой номер индивидуального лицевого счета владельца СКПЭП сертификата, СНИЛС» - (OID: 1.2.643.100.3) страховой номер индивидуального лицевого счета владельца сертификата – физического лица, содержащий уникальный идентификатор владельца сертификата ключа подписи, действующего от имени юридического лица;
* поле «Открытый ключ» - должно содержать: название и алгоритм формирования открытого ключа. (Для формирования открытого ключа в соответствии с государственными стандартами Российской Федерации – ГОСТ Р 34.11/34.10-2012 (OID 1.2.643.7.1.1.2.3);

Параметры и значение открытого ключа уполномоченного лица УЦ:

* поле «Доступ к информации о центрах сертификации» - должно содержать адреса распространения корневых сертификатов Удостоверяющего Центра;
* поле «Алгоритм подписи» - должно содержать значение подписи ГОСТ Р 34.11/34.10-2012;
* поле «Средства электронной подписи и УЦ издателя» - должно содержать наименования средств ЭП и средств аккредитованного УЦ, которые использованы для создания ключа ЭП, КПЭП, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.1.4. Требования к составу и содержанию расширений СКПЭП.

В состав расширений СКПЭП входят следующие расширения:

* расширение «Использование ключа» - расширение «Использование ключа» (обязательное поле) содержит набор областей использования ключа: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных;
* расширение «Улучшенный ключ» - содержит набор областей использования ключа. Набор областей должен включать следующие области:
* Проверка подлинности клиента (1.3.6.1.5.5.7.3.2);
* Защищённая электронная почта (1.3.6.1.5.5.7.3.4);
* Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6);
* расширение «Идентификатор ключа субъекта» - содержит идентификатор ключа владельца СКПЭП;
* расширение «Идентификатор ключа центра сертификатов» - содержит идентификатор ключа уполномоченного лица УЦ;
* расширение «Политики сертификата» - включает сведения о классе средств ЭП владельца СКПЭП;
* расширение «Точки распространения списков отзыва» - содержит URL-адрес точек распространения списков отозванных сертификатов по протоколу «http».

4.2. Требования к информационной системе КЦР.

Для организации приёма и обработки запросов на выдачу СКПЭП, Исполнитель должен произвести установку и настройку на ресурсах Заказчика информационной системы КЦР для подключения к УЦ Исполнителя.

Внедрение ИС КЦР целесообразно для Заказчика ввиду отсутствия необходимости поддерживать инфраструктуру УЦ, а также актуализировать её, в соответствии с требованиями законодательства.

ИС КЦР должна выполнять следующие функции:

1. предоставлять веб-интерфейс для выполнения операций по управлению жизненным циклом СКПЭП;

2. возможность входа в КЦР по СКПЭП;

3. Возможность просмотра списка запросов на СКПЭП, выданных СКПЭП;

4. Автоматическое заполнение реквизитов организации при формировании заявки на выдачу СКПЭП;

5. Возможность создания запроса на выдачу СКПЭП;

6. Возможность удаления запроса на СКПЭП;

7. Возможность редактирования данных при формировании запроса на выдачу СКПЭП, включаемых в СКПЭП

8. Возможность контроля соответствия требованиям и ограничениям:

8.1 Соответствие по формату полей;

8.2 Соответствие скан-копиям документов;

9. Возможность печати заявления на выдачу сертификата ЭП, бланка сертификата ЭП;

10. Возможность загрузки/просмотра скан-копий документов. Возможность ввода реквизитов скан-копий документов;

11. Возможность сканирования документов из ИС КЦР;

12. Возможность просмотра информации о выдаваемом сертификате ЭП;

13. Возможность просмотра истории изменений статусов обработки запроса на выдачу сертификата ЭП;

14. Возможность выгрузки списка сертификатов ЭП в формате Microsoft Excel;

15. Возможность уведомления пользователей и администраторов КЦР об изменениях статусов запроса на сертификат (по e-mail или СМС);

16. Предоставление Базы знаний, инструкций по работе в ИС КЦР. Уведомление об изменениях в ИС КЦР.

17. Доступ ИС КЦР к УЦ Исполнителя должен осуществляться по защищённому каналу, с шифрованием по алгоритму ГОСТ 28147-89.

Формирование и запись ключа электронной подписи и ключа проверки электронной подписи, а также установка изготовленного Исполнителем СКПЭП должны производиться уполномоченным лицом на собственном рабочем месте, с использованием ИС для уполномоченного лица, предоставляющей соответствующий функционал. Доступ уполномоченного лица к соответствующей ИС должен осуществляться по защищённому каналу. В результате уполномоченное лицо получит сертификат ключа проверки электронной подписи. Сертификат должен иметь ограниченный срок действия – 12 месяцев, считая от даты его выдачи.

ИС для уполномоченного лица должна выполнять следующие функции:

1. Идентификация пользователя при входе в ИС по номеру телефона, аутентификация – по одноразовому СМС-коду, отправляемому на номер телефона пользователя;

2. Возможность просмотра списка заявок на сертификат ЭП, выданных сертификатов ЭП для пользователя;

3. Возможность редактирования данных о пользователе, обратившемся за сертификатом ЭП;

4. Возможность загрузки/просмотра скан-копий документов (паспорт, СНИЛС, заявление на выдачу сертификата ЭП);

5. Возможность подписи заявления на выдачу ЭП действующим сертификатом ЭП пользователя;

6. Возможность создания запросов на управление жизненным циклом СКПЭП в электронном виде и отправка их в ИС КЦР;

7. Возможность возврата отправленной на проверку в УЦ Исполнителя формы запроса на выдачу сертификата ЭП;

8. Возможность проверки на соответствие требованиям используемых типов ключевых носителей;

9. Для создания запросов на выдачу СКПЭП сотрудники Заказчика используют веб-интерфейс ИС на собственном рабочем месте;

10. Возможность подтверждения генерации запроса на выдачу сертификата ЭП при помощи ввода одноразового СМС-кода;

11. Возможность установки выпущенного сертификата ЭП на ключевой носитель;

12. Возможность копирования контейнера с сертификатом ЭП на другой носитель.

4.3. Требования к сервису, реализующий функционал проверки и автоматической настройки рабочих станций Заказчика для работы с СКПЭП.

Для проверки и автоматической настройки рабочих станций Заказчика и их подготовки для работы с СКПЭП Исполнитель должен предоставить соответствующее программное обеспечение, которое позволяет выполнять на рабочей станции пользователя, следующие операции:

1. Проверка рабочей станции для работы с сертификатами электронной подписи и выдача предупреждающего уведомления, о необходимости установки требуемого ПО с последующим выбором действия по установке со стороны пользователя:

а. Настройка рабочей станции и браузера для работы с сертификатами электронной подписи, в том числе:

- исправление расположения временной папки ОС;

- отключение конфликтных служб ОС;

- отключение конфликтных надстроек браузера;

- отключение конфликтных программ в автозагрузке ОС;

- настройка зоны «Надёжные узлы» браузера;

- изменение режима кеширования страниц браузера;

- отключение режима совместимости для браузера Internet Explorer;

б. Установка необходимых компонент и запуск служб для работы с сертификатами электронной подписи, в том числе:

- установка Windows Installer;

- установка компонента CAPICOM;

- установка сертификатов УЦ;

- установка драйверов ключевых носителей;

- запуск службы «Автоматическое обновление» ОС;

- установка необходимого пакета обновлений ОС и браузера;

- запуск необходимых служб ОС;

- регистрация OID сертификатов для УЦ;

- установка сертификатов в хранилище «Личное» с ключевых носителей;

в. Возможность локальной загрузки на рабочую станцию необходимых компонентов для работы с сертификатами электронной подписи;

г. Возможность уменьшения объёма загружаемых файлов за счёт анализа локально размещённых на рабочей станции установочных файлов и установленных программ;

д. Возможность самостоятельного выбора пользователем необходимых для установки компонентов;

Сервис должен функционировать в:

- ОС: Windows XP/2003/Vista/2008/2008 R2/7/8/10/2012 (32 или 64 бит);

- Интернет браузер: Google Chrome, Opera, Mozilla Firefox, Яндекс.Браузер, Internet Explorer (не ниже версии 8.0).

4.4. Требования к услугам удостоверяющего центра.

В состав услуг УЦ, предоставляемых Исполнителем Заказчику, входит:

* изготовление СКПЭП;
* выдача СКПЭП с информацией об их действии, допустимых областях использования и иных ограничений, содержащихся в сертификате;
* ограничение срока действия СКПЭП – 12 мес.;
* возможность создания ключа ЭП и ключа проверки ЭП заявителем;
* аннулирование СКПЭП;
* ведение реестра выданных СКПЭП, обеспечение его актуальности и сохранности;
* проверка и обеспечение уникальности ключей проверки ЭП в реестре сертификатов;
* организацию и обеспечение исполнения требований к СКПЭП и ЭП согласно п. 4.1 ТЗ;
* предоставление службы штампов времени (служба TSP)

Cлужба TSP должна обеспечивать:

* удостоверение времени создания и/или подписания электронного документа;
* соответствие следующим стандартам: RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).
* предоставление службы онлайн проверки статуса сертификата (служба OCSP):

Cлужба OCSP должна обеспечивать:

* возможность проверки статуса СКПЭП в режиме реального времени;
* работу по протоколу RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP).

4.5. Требования к предоставлению услуг.

Предоставление услуг должно осуществляться в соответствии с Регламентом УЦ и условиями государственного контракта.

**5.** **Требования к качеству оказываемых Услуг**

5.1. Гарантия качества услуг.

Исполнитель обязан обеспечить гарантийное сопровождение выданных СКПЭП и ЭП сроком 1 год, с момента выдачи, в соответствии с требованиями ТЗ.

Гарантийное сопровождение СКПЭП и ЭП включает:

- ведение реестра выданных и аннулированных СКПЭП в соответствии с требованиями приказа Минкомсвязи России от 05.10.2011 №250 «Об утверждении Порядка формирования и ведения реестров квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров»;

- аннулирование СКПЭП;

- консультирование пользователей по вопросам, связанным с получением услуг и использованием средств ЭП. Требования к техническому сопровождению представлены в п. 5.2;

Исполнитель обеспечивает выполнение гарантийных обязательств с соблюдением временных характеристик, приведённых в Таблице 3.

Таблица 3. Временные характеристики

| № п/п | Состав услуг | Время выполнения | Период предоставления услуг |
| --- | --- | --- | --- |
| 1 | Создание и выдача СКПЭП | Не более 1 рабочего дня с момента предоставления пользователем Заказчика необходимых документов | В режиме 5х8:с 09:00 до 18:00, в рабочие дни Заказчика |
| 2 | Ведение реестра выданных и аннулированных СКПЭП | Актуализация с периодичностью не менее, чем 1 раз в час | В режиме 24х7х365:Круглосуточно, без выходных дней. |
| 3 | Аннулирование СКПЭП | Не более 2-х часов с момента поступления необходимых сведений. | В режиме 5х8:с 09:00 до 18:00, в рабочие дни Заказчика. |

5.2. Требования к техническому сопровождению.

5.2.1. Общие положения:

1. Исполнитель в рамках технического сопровождения должен организовать горячую линию для обращений Заказчика;
2. Горячая линия Исполнителя должна обеспечивать Заказчику возможность оперативно получать консультации по вопросам использования, установки и настройки СКПЭП, выданных Исполнителем, в рамках областей их применения;
3. Горячая линия должна работать круглосуточно, без выходных дней, в режиме 24х7х365;
4. При необходимости и с согласия Заказчика консультации должны оказываться при помощи технологий удалённого доступа.

5.2.2. Требования к оказанию услуг по телефону:

1. Исполнитель должен обеспечить единую точку входа для телефонных обращений Заказчика. Номер телефона должен принадлежать пулу адресов ТфОП населённого пункта размещения Заказчика или префиксу 8-800;
2. Исполнитель должен обеспечивать уровень обслуживания не ниже 80/90 (ожидание ответа у 80% обращений абонентов составляет не более 90 секунд);
3. Исполнитель должен обеспечить соединение Заказчика с консультантом Исполнителя со следующими количественными характеристиками (с момента соединения с консультантом Исполнителя): консультант Исполнителя должен поднимать трубку звонящего телефона не позднее пятого звонка (не более чем через 10 секунд). Консультант Исполнителя должен представиться (фамилия, имя);
4. Каждое обращение Заказчика должно фиксироваться;
5. Должна производиться аудиозапись каждого обращения Заказчика;
6. В случае если проблему не удалось решить сразу, Заказчику должен сообщаться номер обращения, либо внутренний номер консультанта Исполнителя и сроки решения проблемы;
7. Заявки от Заказчика, требующие для решения привлечения дополнительных специалистов Исполнителя, должны переводиться на соответствующие отделы сразу после обращения. Информация о ходе решения должна быть сообщена Заказчику не позднее суток с момента его последнего обращения;
8. Консультант Исполнителя должен доводить решение проблемы Заказчика до логического завершения (Заказчик подтверждает решение проблемы).

5.2.3. Требования к оказанию услуг через веб-сайт (Онлайн-консультант):

1. Онлайн-консультант должен располагаться на сайте Исполнителя;
2. Каждый ответ от специалиста Исполнителя должен содержать ФИО консультанта;

5.2.4. Требования к оказанию услуг по почте:

* 1. Исполнитель должен обеспечить единую точку входа для обращений по электронной почте;
	2. Обработка почты должна вестись в режиме 24/7/365;
	3. Ответ Исполнителя должен отправляться не позднее 2-х часов с момента поступления письма Заказчика. Если решение требует привлечения дополнительных сотрудников Исполнителя, то в ответе должен быть указан номер обращения и сроки решения проблемы;
	4. Каждый ответ от специалиста Исполнителя должен содержать всю контактную информацию: ФИО, телефон, внутренний номер, должность.

Ответ на официальный письменный запрос Заказчика по почте должен предоставляться не позднее чем через 30 календарных дней с момента поступления обращения.

**6. Требования к Исполнителю**

1. Исполнитель должен иметь Лицензию Федеральной службы безопасности Российской Федерации на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя, при условии наличия в данной действующей лицензии следующих работ (видов деятельности), предусмотренных пунктами: 12, 15, 20, 21, 24, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, являющихся приложением к Положению, утверждённому Постановлением Правительства Российской Федерации от 16.04.2012 № 313;
2. Исполнитель должен иметь Свидетельство об аккредитации удостоверяющего центра, выданного Министерством связи и массовых коммуникаций Российской Федерации;
3. Исполнитель должен выполнять требования Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и иных нормативных документов по защите персональных данных и должен быть включён в реестр операторов, осуществляющих обработку персональных данных.

Согласовано:

Контрактная служба: О.В.Дергилев