

«Утверждаю»
Генеральный директор
ООО «Электронный экспресс»



« 12 » апреля 20 21 г.



**Регламент оказания услуг
юридически значимого
электронного документооборота
(Регламент ЮЗД)**

**Порядок реализации функций аккредитованного
удостоверяющего центра и реализация его обязанностей**

Москва, 2021 г.

Содержание

ОБЩИЕ ПОЛОЖЕНИЯ	5
1.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	5
2.СТАТУС РЕГЛАМЕНТА.....	9
3.ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ	10
4. УСЛУГИ ЮЗД.....	10
4.1. Перечень услуг ЮЗД, предоставляемых Обществом	10
4.2.Вознаграждение за услуги ЮЗД.	10
ГЛАВА 1. РЕГЛАМЕНТ ОКАЗАНИЯ УСЛУГ ПО СДАЧЕ ОТЧЕТНОСТИ.....	11
ГЛАВА 2. РЕГЛАМЕНТ ОКАЗАНИЯ УСЛУГ ПО ЭЛЕКТРОННОМУ ДОКУМЕНТООБОРОТУ	12
ГЛАВА 3. ПОРЯДОК РЕАЛИЗАЦИИ ФУНКЦИЙ АККРЕДИТОВАННОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ИСПОЛНЕНИЯ ЕГО ОБЯЗАННОСТЕЙ.	14
1. Общие положения.	14
1.1. Предмет регулирования Порядка.	14
1.2. Публикация Порядка.....	14
1.3. Область применения Порядка.....	14
1.4. Срок действия Порядка	14
1.5. Контактная информация.....	14
1.6. Платность услуг.....	15
2. Перечень реализуемых Удостоверяющим центром функций	16
2.1. Назначение УЦ.....	16
2.2. Услуги УЦ.....	16
2.3. Структура УЦ	17
2.3.1. Административная служба УЦ.....	17
2.3.2. Служба регистрации УЦ	17
2.3.3. Служба безопасности УЦ.....	17
2.3.4. Техническая служба УЦ	18
2.4. Пользователи УЦ	18
2.5. Разрешение споров	19
2.6. Ответственность сторон.....	19
2.7. Прекращение деятельности.....	19
2.8. Порядок утверждения и внесения изменений в Регламент	20
3. Права и обязанности Удостоверяющего центра и Клиентов (пользователей УЦ).....	20
3.1. Права УЦ	20
3.2. Права Клиентов	21
3.2.1. Права лиц, не зарегистрированных в УЦ	21
3.2.2. Права лиц, зарегистрированных в УЦ	21
3.2.3. Права лиц, которые проходят процедуру регистрации в УЦ.....	22
3.3. Обязанности УЦ.....	22
3.3.1. Обязанности аккредитованного удостоверяющего центра.....	22
3.3.2. Синхронизация времени	24
3.3.3. Регистрация пользователей УЦ	24
3.3.4. Изготовление ключей ЭП и ключей проверки ЭП пользователей УЦ	24
3.3.5. Изготовление квалифицированных сертификатов ключей проверки ЭП	25
3.3.6. Аннулирование квалифицированных сертификатов ключей проверки ЭП	25
3.3.7. Уведомления	25
3.3.7.1. Уведомление о факте изготовлении квалифицированного сертификата ключа проверки ЭП	25
3.3.7.2. Уведомление о факте аннулирования сертификата ключа проверки ЭП.....	26
3.3.8. Реестр квалифицированных сертификатов ключа проверки ЭП	27
3.3.9. Восстановление работоспособности УЦ после сбоев	27
3.3.10. Прочие обязанности	27
3.4. Обязанности Клиентов.....	27
3.4.1. Обязанности лиц, не зарегистрированных в УЦ	27
3.4.2. Обязанности лиц, зарегистрированных в УЦ	28
3.4.3. Обязанности лиц, которые проходят процедуру регистрации в УЦ.....	28
4. Политика конфиденциальности	28
4.1. Типы конфиденциальной информации	28
4.2. Типы информации, не являющейся конфиденциальной.....	29
4.3. Исключительные полномочия официальных лиц	29

5. Перечень реализуемых Удостоверяющим центром функций. Процедуры и механизмы.	29
5.1. Перечень реализуемых Удостоверяющим центром функций.	29
5.2. Порядок и сроки выполнения действий для предоставления услуг Удостоверяющим центром	31
5.3. Процедура регистрации пользователей УЦ.....	31
5.3.1. Заявление на регистрацию.....	31
5.3.2. Идентификация Пользователя УЦ	32
5.4. Создание ключей электронных подписей и ключей проверки электронных подписей.....	32
5.5. Сроки действия ключей электронной подписи УЦ	34
5.6. Смена ключей ЭП Удостоверяющего центра.....	34
5.6.1. Плановая смена ключей ЭП Удостоверяющего центра	34
5.6.2. Внеплановая смена ключей ЭП Удостоверяющего центра.....	35
5.6.3. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца квалифицированного сертификата.	35
5.6.4. Создание и выдача квалифицированных сертификатов.....	36
5.6.5. Порядок создания квалифицированного сертификата	38
5.6.6. Порядок выдачи квалифицированного сертификата	38
5.6.7. Срок создания и выдачи квалифицированного сертификата	39
5.7. Процедура подтверждения действительности электронной подписи УЦ в квалифицированном сертификате ключа проверки ЭП	39
5.8. Процедура подтверждения действительности электронной подписи, использованной для подписания электронных документов	40
5.9. Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата.....	41
5.9.1. Основания прекращения действия или аннулирования квалифицированного сертификата.	41
5.9.2. Случаи аннулирования сертификата ключа проверки электронной подписи Удостоверяющим центром	41
5.9.3. Аннулирование квалифицированного сертификата	41
5.10. Порядок ведения реестра квалифицированных сертификатов	43
5.10.1. Структура реестра квалифицированных сертификатов	44
5.10.2. Внесение сведений в реестр квалифицированных сертификатов	45
5.10.3. Предоставление сведений из реестра квалифицированных сертификатов.....	46
5.11. Порядок технического обслуживания реестра квалифицированных сертификатов	46
5.12. Порядок исполнения обязанностей Удостоверяющего центра	47
5.13. Срок хранения сертификата ключа проверки ЭП.....	48
5.14. Процедура предоставления КСКПЭП	48
5.15. Механизм доказательства обладания ключом ЭП, соответствующим ключу проверки ЭП	49
5.16. Порядок проведения разбора конфликтной ситуации, связанной с применением электронной подписи в электронном документе	49
6. Дополнительные положения	51
6.1. Идентифицирующие данные Уполномоченного лица УЦ	51
6.2. Требования к средствам электронной подписи, используемым в составе Удостоверяющего центра и требования к средствам электронной подписи пользователей УЦ.....	51
6.3. Сроки действия ключей ЭП и квалифицированных сертификатов ключей проверки ЭП пользователей УЦ	52
6.4. Меры защиты ключей ЭП	52
6.5. Информация из квалифицированного сертификата ключа проверки ЭП на бумажном носителе или в электронном виде.....	53
6.6. Архивное хранение документированной информации	53
6.6.1. Хранение сертификатов ключей электронной подписи в электронном виде.....	53
6.6.2. Состав архивируемых документов	53
6.6.3. Источник комплектования архивного фонда.....	53
6.6.4. Архивохранилище	53
6.6.5. Срок архивного хранения.....	54
6.6.6. Уничтожение архивных документов	54
7. Структуры сертификатов и списков отозванных сертификатов	54
7.1. Структура квалифицированного сертификата	54
7.2. Структура списка отозванных сертификатов, изготавливаемого УЦ в электронной форме.....	59
7.2.1. Расширения списка отозванных сертификатов.	59
8. Программные и технические средства обеспечения деятельности УЦ	59

8.1. Программный комплекс обеспечения реализации целевых функций УЦ.....	59
8.2. Технические средства обеспечения работы ПКУЦ.....	61
8.3. Программные и программно-аппаратные средства защиты информации.....	61
8.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций УЦ.....	62
8.5. Перечень данных программного комплекса обеспечения реализации целевых функций УЦ, подлежащих резервному копированию.....	62
8.6. Порядок технического обслуживания средств обеспечения деятельности УЦ.....	62
8.6.1. Техническое обслуживание вычислительной техники и периферийного оборудования.....	63
8.6.2. Техническое обслуживание общесистемного и специализированного программного обеспечения.....	65
9. Роли обслуживающего персонала средств обеспечения деятельности УЦ.....	68
10. Обеспечение безопасности.....	70
10.1. Инженерно-технические меры защиты информации.....	70
10.1.1. Размещение технических средств УЦ.....	70
10.1.2. Физический доступ в помещения.....	70
10.1.3. Электроснабжение и кондиционирование воздуха.....	70
10.1.4. Подверженность воздействию влаги.....	71
10.1.5. Предупреждение и защита от возгорания.....	71
10.1.6. Хранение документированной информации.....	71
10.1.7. Уничтожение документированной информации.....	71
10.2. Программно-аппаратные меры защиты информации.....	71
10.2.1. Организация доступа к техническим средствам УЦ.....	71
10.2.2. Организация доступа к программным средствам УЦ.....	71
10.2.2.1. Общий перечень объектов доступа УЦ.....	72
10.2.2.2. Перечень объектов доступа, предоставляемых сотрудникам УЦ.....	72
10.2.2.3. Перечень объектов доступа, предоставляемых аутентифицированным пользователям УЦ при осуществлении сетевого взаимодействия с программными средствами УЦ.....	73
10.2.3. Контроль целостности программного обеспечения.....	74
10.2.4. Контроль целостности технических средств.....	74
10.2.5. Защита внешних сетевых соединений.....	74
10.2.5.1. Перечень информации, подлежащей защите.....	75
10.3. Организационные меры защиты информации.....	75
10.3.1. Предъявляемые требования к персоналу УЦ.....	75
10.3.2. Профессиональная переподготовка и повышение квалификации персонала.....	75
10.3.3. Организация сменной работы.....	75
10.3.4. Организация доступа персонала к документам и документации.....	75
10.3.5. Охрана здания и помещений.....	76
10.4. Юридические меры защиты информации.....	76
11. Взаимодействие Удостоверяющего центра с федеральными органами исполнительной власти в сфере использования электронной подписи.....	76
СПИСОК ЛИТЕРАТУРЫ.....	77
Приложение № 1.....	78
Приложение № 2 а.....	79
Приложение № 2 б.....	80
Приложение № 3 а.....	81
Приложение № 4.....	82
Приложение № 5.....	83
Приложение № 6 а.....	84
Приложение № 6 б.....	85
Приложение № 7 а.....	86
Приложение № 7 б.....	87
Приложение № 8 а.....	88
Приложение № 8 б.....	90
Приложение № 9.....	91
Приложение № 10.....	92
Приложение № 11.....	93
Приложение № 12.....	94
Приложение № 13.....	95

ОБЩИЕ ПОЛОЖЕНИЯ

ООО «Электронный экспресс» (Далее – Общество) зарегистрировано на территории Российской Федерации в городе Москве. Свидетельство о регистрации серия 77 № 010428831, выдано 15.05.2009 Межрайонной инспекцией ФНС № 46 по г.Москве.

Общество осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1. Лицензии ФСБ ЛСЗ № 0010530 Рег.№ 13681Н от 03 июля 2014г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"
2. Лицензии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций №121650 от 06 августа 2014г. на оказание телематических услуг связи.
3. Свидетельства Минкомсвязи России об аккредитации удостоверяющего центра № 745 от 06.09.2017. Аккредитация предоставлена на срок до 06 сентября 2022 года включительно на основании Приказа Минкомсвязи России № 472 от 06 сентября 2017 года «Об аккредитации удостоверяющих центров».

Реквизиты Общества:

ООО «Электронный экспресс»:

Юридический адрес: 119991, г. Москва, Ленинские горы, д.1, стр. 77

Фактический адрес: 119991, г. Москва, Ленинские горы, д.1, стр. 77

Контактные телефоны, факс, адрес электронной почты:

тел.: 8 (800) 333-88-88; e-mail: uc@garant.ru, www.garantexpress.ru

1.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Таблица 1. Список терминов

Термин	Определение
Общество	ООО «Электронный экспресс», оказывающее услуги по обеспечению юридически значимого документооборота (далее услуги ЮЗД), включающие в себя услуги по сдаче отчетности, услуги аккредитованного удостоверяющего центра
Клиент	Юридическое или физическое лицо, заключившее с Обществом Клиентский договор.
Сайт Общества	Сайт в сети Интернет (www.garantexpress.ru), на котором Общество размещает информацию об услугах ЮЗД, в том числе информацию об изменениях в тексте настоящего Регламента, действующих Ценовых предложениях и иную информацию

Ценовые предложения	Информация о стоимости лицензий и услуг ЮЗД, определяемых Обществом.
Пользователь Удостоверяющего центра (Пользователь УЦ)	Физическое лицо — уполномоченный представитель Клиента.
Владелец сертификата ключа проверки электронной подписи	Лицо, которому в установленном Федеральным законом (N 63-ФЗ) порядке выдан сертификат ключа проверки электронной подписи.
Демилитаризованная зона	Технология обеспечения защиты информационного периметра сети предприятия, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети, называемом демилитаризованной зоной (ДМЗ). Компьютеры в ДМЗ ограничены в доступе к основным сегментам сети предприятия с помощью межсетевого экрана (МЭ) с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в ДМЗ.
Маркер временного доступа	секретный пароль (десятизначное символьное значение), предоставляющее Пользователю УЦ возможность создания ключа электронной подписи и запроса на КСКПЭП.
Межсетевой экран	Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.
Сертификат ключа проверки электронной подписи	Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат)	Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
Копия сертификата ключа проверки электронной подписи	документ на бумажном носителе, содержащий информацию из сертификата ключа проверки электронной подписи
Реестр Удостоверяющего центра	набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию: • реестр поступивших заявлений на регистрацию и изготовление сертификата ключа подписи; • реестр поступивших заявлений на аннулирование (отзыв) сертификата ключа подписи; • реестр поступивших заявлений на приостановление/возобновление действия сертификата ключа подписи; • реестр доверенностей на получение услуг Удостоверяющего центра; • реестр Согласий на обработку персональных

	данных; • реестр изготовленных сертификатов ключей проверки электронной подписи; • реестр изготовленных Списков отозванных сертификатов; • служебная информация Удостоверяющего центра; • других документов, определенных настоящим Регламентом.
Средства электронной подписи	Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.
Список отозванных сертификатов	Электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые были аннулированы до окончания срока их действия или действие которых было приостановлено.
Удостоверяющий центр	Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом (N 63-ФЗ).
Уполномоченное лицо УЦ	сотрудник Общества, наделенный Обществом полномочиями по заверению Сертификатов ключей проверки электронной подписи и Списков отозванных сертификатов.
Центр Регистрации (ЦР)	подразделение Общества или партнерская организация, заключившая партнерский Договор с Обществом, осуществляющее регистрацию Пользователей УЦ, сбор и проверку необходимых документов
Уполномоченное лицо ЦР	сотрудник Центра Регистрации, уполномоченный осуществлять функции по регистрации Пользователей в Удостоверяющем центре.
Услуга сопровождение квалифицированного сертификата ключа проверки электронной подписи	услуга, в рамках которой осуществляется перевыпуск КСКПЭП во всех случаях за исключением: • изменение владельца сертификата; • изменение юридического лица, на который оформлен сертификат, в том числе преобразование юридического лица (слияние, поглощение и т.п.);
Электронная подпись	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Электронный документ	Документ, информация в котором представлена в электронной форме, способной быть обработанной

	средствами вычислительной техники
Электронный идентификатор	Последовательность символов, являющаяся составной частью простой электронной подписи Клиента. В качестве Электронного идентификатора используется номер мобильного телефона Клиента.
Простая электронная подпись Клиента	Сочетание Электронного идентификатора и сгенерированных Обществом уникальных кодов, направляемых Клиенту на указанный номер мобильного телефона
Признание простой электронной подписи аналогом собственноручной подписи	Клиент соглашается применять простую электронную подпись в качестве аналога собственноручной подписи для целей дополнительной идентификации и аутентификации.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Устойчивые русскоязычные сокращения, используемые в этом документе, описаны в таблице ниже.

Таблица 2. Список сокращений

Сокращение	Значение
АРМ	Автоматизированное рабочее место
ДМЗ	Демилитаризованная зона
КСКПЭП	Квалифицированный сертификат ключа проверки электронной подписи
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СУБД	Системы управления базами данных
УЦ	Удостоверяющий центр
ЦР	Центр регистрации
ЭДО	Электронный документооборот
ЭП	Электронная подпись
ЮЗД	Юридически значимый документооборот

Используемые иностранные сокращения, как правило, англоязычные, приведены в таблице ниже.

Таблица 3. Список иностранных сокращений

Сокращение	Значение	Перевод
AIA	Authority Info Access	Доступ к информации о Центре сертификации
CRL	Certificate Revocation List	Список отозванных сертификатов, СОС
CDP	CRL Distribution Point	Пункт распространения CRL

CRM	Customer Relationship Management System	Система, предназначенная для автоматизации работы при подключении клиентов к системе юридически значимого электронного документооборота (ЮЗД) и дальнейшем их обслуживании.
DN	Distinguished Name	Отличительное имя
IETF	Internet Engineering Task Force	Специальная комиссия интернет разработок
ITU	International Telecommunication Union	Международный союз электросвязи, МСЭ
ITU-T	Telecommunication Standardization Sector (ITU's)	Сектор стандартизации электросвязи (в МСЭ), МСЭ-Т
LDAP	Lightweight Directory Access Protocol	Облегчённый протокол доступа к Справочнику
PKI	Public Key Infrastructure	Инфраструктура ключей проверки ЭП
PKCS	Public Key Cryptography Standarts	стандарты криптографии с открытым ключом, разработанные компанией RSA Security; Удостоверяющий центр осуществляет свою работу в соответствии со следующими стандартами PKCS: • PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений; Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные; • PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.
RDN	Relative Distinguished Name	Относительное отличительное имя

2. СТАТУС РЕГЛАМЕНТА

2.1. Настоящий Регламент ЮЗД (далее – Регламент) определяет условия, на которых Общество оказывает юридическим и физическим лицам услуги ЮЗД.

2.2. Настоящий Регламент является Приложением № 1 к Клиентскому договору.

2.3. Подписание Клиентом Клиентского договора означает, что Клиент с условиями Регламента ознакомлен, принимает их и обязуется выполнять в полном объеме.

2.4. Предусмотренные настоящим Регламентом услуги оказываются при условии их оплаты Клиентом и наличия у Клиента программного обеспечения, совместимого с программно-аппаратными средствами Общества.

2.5. Услуги ЮЗД оказываются в соответствии с заявкой Клиента. В процессе обслуживания по заявке Клиента может осуществляться изменение настройки параметров электронного документооборота и изменение состава услуг. При выполнении перенастройки параметров ЮЗД и изменении состава услуг осуществляется перерасчет.

2.6. Не чаще чем 2 (Два) раза в месяц в период первых 5 (Пяти) календарных дней месяца

Общество имеет право приостановить оказание услуг на срок не более 1 (Одних) суток для проведения профилактических работ. При этом Общество публикует на сайте Общества соответствующее объявление с указанием даты проведения профилактических работ, не позднее чем за 7 (Семь) календарных дней до указанной даты.

3. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

3.1. Общество утверждает Регламент Приказом Генерального директора Общества, заверяет печатью и подписью Генерального директора Общества, хранит в офисе Общества. Действующий Регламент Общества Общество публикует на сайте.

3.2. Общество имеет право в одностороннем порядке вносить изменения и/или дополнения в настоящий Регламент.

3.2.1. Изменения и/или дополнения, вносимые Обществом в настоящий Регламент в связи с изменением законодательного и нормативного регулирования, вступают в силу одновременно с вступлением в силу изменений в указанных актах.

3.2.2. Изменения и/или дополнения, вносимые Обществом в настоящий Регламент, вступают в силу после опубликования на сайте Общества, с даты, указанной Обществом.

3.3. Клиент не реже одного раза в неделю самостоятельно или через уполномоченных лиц обращается на сайт Общества с целью ознакомления с действующей редакцией Регламента.

3.5. В случае несогласия Клиента с действующей редакцией Регламента Клиентский договор может быть расторгнут по инициативе Клиента.

4. УСЛУГИ ЮЗД

4.1. Перечень услуг ЮЗД, предоставляемых Обществом

- Оказание услуг по сдаче отчетности (см. Главу 1 настоящего Регламента);
- Оказание услуг по электронному документообороту (см. Главу 2 настоящего Регламента);
- Оказание услуг аккредитованного удостоверяющего центра (см. Главу 3 настоящего Регламента).

Услуги ЮЗД не включают услуги по установке, наладке ИПК «ГАРАНТ Электронный экспресс» и «КриптоПро» и любое сервисное обслуживание, связанное с выездом специалиста.

4.2. Вознаграждение за услуги ЮЗД.

Деятельность по оказанию услуг ЮЗД осуществляется на платной основе.

Стоимость услуг ЮЗД определяется «Ценовыми предложениями», действующими на момент оказания услуг по Клиентскому договору и размещенными на сайте Общества.

Оплата осуществляется в российских рублях по безналичному расчету путем перечисления денежных средств на расчетный счет или иным способом, предусмотренным законодательством Российской Федерации.

ГЛАВА 1. РЕГЛАМЕНТ ОКАЗАНИЯ УСЛУГ ПО СДАЧЕ ОТЧЕТНОСТИ

1. Общество предоставляет услуги по сдаче отчетности, в том числе между Клиентами и органами государственной власти, внебюджетными фондами и иными организациями.

2. Услуги по сдаче отчетности включают в себя:

- регистрацию параметров электронного документооборота Клиента для обмена с адресатом на программных средствах Общества;
- обеспечение рассылки регистрационных данных Клиента адресатам в соответствии с нормативными правовыми и иными актами, регламентирующими указанную процедуру;
- предоставление возможности использования ресурсов Общества для обмена электронными документами с соответствующим адресатом, в том числе с использованием сертифицированных средств криптографической защиты информации;
- ведение учета и регистрацию фактов обмена электронными документами (мониторинг обмена);
- обеспечение рассылки сформированных Обществом электронных документов-подтверждений, фиксирующих дату поступления на сервер Общества электронных документов, в т.ч. определенных нормативными правовыми и иными актами, регулирующими порядок электронного документооборота;
- предоставление Клиенту консультаций по «горячей линии».

3. Возможность получения услуг по сдаче отчетности предоставляется Клиенту при наличии доступа к уникальной учетной записи.

4. Услуги по сдаче отчетности предоставляются в соответствии с заявкой Клиента.

5. Общество вправе отклонить заявку Клиента в случаях:

- выявления в ней неточностей и заведомо неверных данных;
- отсутствия необходимых документов.

При этом Общество оповещает Клиента об отклонении заявки с использованием общепринятых средств связи (телефон, факсимильная связь, электронная почта) и при необходимости направляет Клиенту уведомление с указанием причин отказа в письменном виде.

6. Общество не несет ответственность:

- за содержание и достоверность информации, передаваемой между Клиентом и адресатом;
- за отсутствие у адресата возможностей по приему и обработке информации в утвержденном формате;
- за последствия компрометации Клиентом используемых ключей, иных нарушений Клиентом Правил использования средств криптографической защиты информации;
- за неготовность Клиента к обмену электронными документами, обусловленную несвоевременной заявкой и (или) оплатой услуг, несвоевременным получением ключевой информации, а также несоблюдением Клиентом условий оказания услуг, определенных в настоящем Регламенте, действующих Ценовых предложениях;
- за приостановку (временное прекращение) оказания услуг Клиенту в случае

- неполучения и несвоевременной оплаты Клиентом счета, или, если Клиент своевременно не известил Общество об изменении адреса электронной почты, факса, почтового адреса и других контактных данных;
- за действия других участников электронного документооборота по обработке регистрационных данных Клиента, а также в случае иных обстоятельств, не зависящих от Общества.

ГЛАВА 2. РЕГЛАМЕНТ ОКАЗАНИЯ УСЛУГ ПО ЭЛЕКТРОННОМУ ДОКУМЕНТООБОРОТУ

1. Общество предоставляет услуги по электронному документообороту (ЭДО), между Контрагентами – пользователями системы ЭДО «Экспресс Документ».

2. Предоставляемые Обществом услуги по электронному документообороту в рамках системы ЭДО «Экспресс Документ» включают в себя:

- регистрацию параметров электронного документооборота Клиента для обмена с контрагентами;
- обеспечение обмена регистрационными данными между Клиентом и контрагентами в соответствии с нормативными правовыми и иными актами, регламентирующими указанную процедуру;
- предоставление возможности обмена электронными документами (актами, накладными, счетами-фактурами) с контрагентами, с использованием сертифицированных средств криптографической защиты информации;
- ведение учета и регистрацию фактов обмена электронными документами (мониторинг обмена);
- обеспечение рассылки сформированных Обществом электронных документов-подтверждений, фиксирующих дату поступления на сервер Общества электронных документов, в т.ч. определенных нормативными правовыми и иными актами, регулирующими порядок электронного документооборота;
- предоставление Клиенту консультаций по «горячей линии».

3. Клиенты - пользователи системы ЭДО при осуществлении информационного обмена в рамках системы ЭДО «Экспресс Документ» принимают к сведению электронные документы, подписанные квалифицированной ЭП.

4. Время создания, получения и отправления всех электронных документов в системе ЭДО «Экспресс Документ» фиксируется по времени сервера, на котором функционирует система. Общество несет ответственность за обеспечение информационной защиты системы управления временем сервера.

5. Клиенты - пользователи системы ЭДО принимают, что в случае наличия требований к формату и содержанию электронного документа, в Системе ЭДО используются электронные документы установленного формата.

6. Для организации электронного документооборота в рамках системы ЭДО «Экспресс Документ» Клиент должен установить необходимые аппаратные средства, лицензионное клиентское программное и информационное обеспечение и получить КСКПЭП в Удостоверяющем Центре ООО «Электронный экспресс» или в другом доверенном удостоверяющем центре.

7. Всем Клиентам, получившим КСКПЭП в УЦ ООО «Электронный экспресс» (см. раздел 5.4. («Создание ключей электронных подписей и ключей проверки электронных подписей»), Главы 3), автоматически предоставляется бесплатная услуга по обмену электронными документами в рамках системы ЭДО «Экспресс Документ». При этом, автоматическая регистрация КСКПЭП в системе ЭДО «Экспресс Документ» осуществляется в течение 1 часа с момента их выпуска.

ГЛАВА 3. ПОРЯДОК РЕАЛИЗАЦИИ ФУНКЦИЙ АККРЕДИТОВАННОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА И ИСПОЛНЕНИЯ ЕГО ОБЯЗАННОСТЕЙ.

1. Общие положения.

1.1. Предмет регулирования Порядка.

Настоящий Порядок определяет условия предоставления услуг УЦ ООО «Электронный экспресс» (далее по тексту — «УЦ»), включая права, обязанности и ответственность УЦ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы УЦ

1.2. Публикация Порядка

Настоящий Порядок распространяется:

- в электронной форме
 - по протоколу HTTPS из репозитория Владельца УЦ по адресу URL:
https://www.garantexpress.ru/services/electronic_signature/certification_center/
 - по электронной почте uc@garant.ru (sales_ee@garant.ru)
- в бумажной форме через Почту России: 117246, г.Москва, Научный проезд, 19, ООО «Электронный экспресс» (119991, г.Москва, Ленинские горы, д.1, стр.77, комн. 19, этаж 3)

Копии Порядка, предназначенные для распространения в электронной форме по протоколу HTTPS, состоят из двух файлов, один из которых содержит электронный образ Порядка в формате RTF, а другой — электронную подпись Руководителя Общества на файл электронного образа Порядка. Файл, содержащий электронную подпись Руководителя УЦ, имеет формат PKCS#7 Signed в кодировке Base64 и не содержит самих данных, т.е. является отсоединённой (detached) подписью.

1.3. Область применения Порядка

Настоящий Порядок предназначен служить соглашением, налагающим обязанности по всем вовлечённым сторонам, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

1.4. Срок действия Порядка

Настоящий Порядок вступает в силу со дня его публикации.

Срок действия Порядка — 6 лет.

Если УЦ официально не уведомит своих пользователей о прекращении действия Порядка, то Порядок автоматически пролонгируется на следующий срок.

Официальное уведомление о прекращении действия Порядка осуществляется способами, определёнными в разделе публикации Порядка:

- Копии уведомлений, предназначенные для распространения в электронной форме, распространяются с использованием протокола HTTPS.
- Копии уведомления, предназначенные для распространения в электронной форме через E-mail, защищены электронной подписью с использованием S/MIME.

1.5. Контактная информация

ООО «Электронный экспресс» (Далее – Общество) зарегистрировано на территории Российской Федерации в городе Москве. Свидетельство о регистрации серия 77 №

010428831, выдано 15.05.2009 Межрайонной инспекцией ФНС № 46 по г.Москве.

Общество осуществляет свою деятельность на территории Российской Федерации на основании следующего свидетельства и лицензий:

- Свидетельства Минкомсвязи России об аккредитации удостоверяющего центра № 745 от 06.09.2017. Аккредитация предоставлена на срок до 06 сентября 2022 года включительно на основании Приказа Минкомсвязи России № 472 от 06 сентября 2017 года «Об аккредитации удостоверяющих центров».

- Лицензии ФСБ ЛСЗ № 0010530 Рег.№ 13681Н от 03 июля 2014г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"

- Лицензии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций №121650 от 06 августа 2014г. на оказание телематических услуг связи.

Реквизиты Общества:

ООО «Электронный экспресс»:

Юридический адрес: 119991, г. Москва, Ленинские горы, д.1, стр. 77

Фактический адрес: 119991, г. Москва, Ленинские горы, д.1, стр. 77

Контактные телефоны, факс, адрес электронной почты:

тел.: 8 (800) 333-88-88; e-mail: uc@garant.ru, www.garantexpress.ru

Контактный телефон Административной службы УЦ	8 (800) 333-88-88
E-mail Административной службы УЦ	uc@garant.ru
Контактный телефон Службы регистрации УЦ	8 (800) 333-88-88
E-mail Службы регистрации УЦ	uc@garant.ru
Контактный телефон Службы безопасности УЦ	8 (800) 333-88-88
E-mail Службы безопасности УЦ	uc@garant.ru
Контактный телефон Технической службы УЦ	8 (800) 333-88-88

Время работы Удостоверяющего центра для приема клиентов:

09.00 — 18.00 по Московскому времени в рабочие дни.

Суббота, воскресенье и праздничные дни — выходные.

Информация из Реестров предоставляется круглосуточно.

Службы УЦ работают круглосуточно.

1.6. Платность услуг

Услуги Удостоверяющего центра оказываются на возмездной основе, за исключением предоставления информации из Реестра УЦ, в том числе информации об аннулированных

сертификатах.

Стоимость услуг Удостоверяющего центра приведена на сайте: http://www.garantexpress.ru/wp-content/uploads/2016/02/Cost_uslugi_new1.pdf и в Приложении № 13 настоящего Регламента.

Указанные данные о стоимости не являются публичной офертой.

Для заказа услуг Удостоверяющего центра и выставления счета необходимо обратиться по телефону 8 (800) 333-88-88, либо заказав обратный звонок на сайте <http://www.garantexpress.ru/>, либо прислав заявку по электронной почте на адрес ee_sales@garant.ru.

По согласованию с Клиентом будет определен состав услуг и выставлен счет, который необходимо оплатить в течение трех рабочих дней. После поступления средств на расчетный счет Общества, с клиентом свяжется ответственный сотрудник Общества и будет определена дата посещения офиса Центра Регистрации, а также предоставлена информация о комплекте необходимых для получения услуг документов.

В стоимость услуг входит перевыпуск КСКПЭП Пользователей УЦ в случае компрометации ключа электронной подписи Удостоверяющего центра.

В стоимость услуг входит предоставление участникам информационных систем в форме электронных документов копий КСКПЭП Пользователей УЦ, находящихся в Реестре изготовленных КСКПЭП, а также информации об их действии в виде Списков отозванных сертификатов.

В стоимость услуг входят аннулирование (отзыв) действия КСКПЭП Пользователя УЦ.

2. Перечень реализуемых Удостоверяющим центром функций

2.1. Назначение УЦ

УЦ предназначен для обеспечения участников информационных систем средствами и спецификациями для использования квалифицированных сертификатов ключей проверки электронной подписи (КСКПЭП) в целях обеспечения:

- применения электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- аутентификации участников информационных систем в процессе взаимодействия;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

2.2. Услуги УЦ

В процессе своей деятельности УЦ предоставляет Клиентам (Пользователям УЦ) следующие виды услуг:

- внесение в Реестр УЦ регистрационной информации о Клиентах;
- изготовление КСКПЭП Клиентов в электронной форме;
- изготовление копий КСКПЭП Клиентов на бумажных носителях;
- формирование ключей ЭП и ключей проверки ЭП по обращениям Клиентов с записью их на ключевой носитель;
- ведение Реестра изготовленных КСКПЭП Клиентов;
- предоставление КСКПЭП в электронной форме, находящихся в Реестре изготовленных

- КСКПЭП, по запросам Клиентов;
- аннулирование (отзыв) КСКПЭП по обращениям владельцев КСКПЭП, а также в случаях предусмотренных 63-ФЗ «Об электронной подписи»;
- предоставление Клиентам сведений об аннулированных КСКПЭП ;
- подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям Клиентов;
- подтверждение подлинности электронных подписей Уполномоченных лиц УЦ в изготовленных ими КСКПЭП по обращениям Клиентов;
- распространение средств электронной подписи по обращениям Клиентов

2.3. Структура УЦ

Структура УЦ включает в себя следующие организационные подразделения (службы):

- Административная служба УЦ;
- Служба регистрации УЦ;
- Служба безопасности УЦ;
- Техническая служба УЦ.

2.3.1. Административная служба УЦ

Административная служба УЦ предназначена для решения следующих задач:

- управление деятельностью УЦ;
- координация деятельности других Служб УЦ;
- взаимодействие с Клиентами в части разрешения вопросов, связанных с применением средств ЭП, ключей и квалифицированных сертификатов ключей проверки ЭП, изготавливаемых и/или распространяемых УЦ;
- взаимодействие с Клиентами в части разрешения вопросов, связанных с подтверждением электронной подписи Уполномоченного лица УЦ в КСКПЭП, изготовленных УЦ в электронной форме.

2.3.2. Служба регистрации УЦ

Служба регистрации УЦ предназначена для решения следующих задач:

- регистрация Клиентов;
- ведение Реестра зарегистрированных Клиентов;
- распространение средств электронной подписи и шифрования.

2.3.3. Служба безопасности УЦ

Служба безопасности УЦ предназначена для решения следующих задач:

- организация и выполнение мероприятий по защите ресурсов УЦ;
- изготовление и предоставление ключей по обращению Клиентов;
- изготовление и предоставление изготовленных КСКПЭП в электронной форме по обращению Клиентов;
- изготовление и предоставление копий КСКПЭП на бумажном носителе по обращению их владельцев;
- аннулирование (отзыв) КСКПЭП по обращениям владельцев сертификатов ключей проверки ЭП и в случаях, предусмотренных 63-ФЗ «Об электронной подписи»;
- предоставление Клиентам сведений об аннулированных КСКПЭП;

- предоставление копий сертификатов ключей проверки ЭП из Реестра квалифицированных сертификатов УЦ, по запросам Клиентов;
- техническое обеспечение процедуры подтверждения электронной подписи в документах, представленных в электронной форме, по обращениям Клиентов;
- техническое обеспечение процедуры подтверждения подлинности электронных подписей Уполномоченного лица УЦ в изготовленных сертификатах ключей проверки ЭП по обращениям Клиентов.

2.3.4. Техническая служба УЦ

Техническая служба УЦ предназначена для решения следующих задач:

- организация и выполнение мероприятий по эксплуатации программных и технических средств обеспечения деятельности УЦ;
- организация и выполнение мероприятий по техническому сопровождению распространяемых средств электронной подписи и шифрования.

2.4. Пользователи УЦ

Потребителями или пользователями услуг УЦ (далее по тексту — «Пользователи УЦ») называются лица, которые входят в одну из следующих групп:

- **Лица, не зарегистрированные в УЦ** — лица, не прошедшие процедуру регистрации в УЦ, использующие сертификаты других зарегистрированных Пользователей УЦ для каких-либо целей, например, для проверки электронных подписей;
- **Лица, зарегистрированные в УЦ** — лица, прошедшие полную процедуру регистрации в УЦ и являющиеся полноценными Пользователями УЦ;
- **Лица, которые проходят процедуру регистрации в УЦ** — лица, ещё не прошедшие полную процедуру регистрации в УЦ, но уже отправившие в УЦ запрос на регистрацию, который ещё не был одобрен оператором УЦ;

Проходить регистрацию в УЦ и стать зарегистрированным Пользователем УЦ может только физическое лицо.

Владельцем сертификата может быть только зарегистрированный Пользователь УЦ, физическое лицо.

Физическое лицо имеет право действовать от имени юридического лица без доверенности на основании уставных документов, что подтверждается записью в ЕГРЮЛ ФНС России.

Физическое лицо может представлять юридическое лицо при наличии доверенности, которая даёт данному физическому лицу право пользоваться услугами УЦ от имени юридического лица.

В тех случаях, когда КСКПЭП требуются для работы каких-либо устройств или программ, назначается ответственное лицо, которое регистрируется в УЦ и на имя которого УЦ изготавливает сертификаты.

Пользователем сертификата может быть любое лицо, устройство или программа.

Зарегистрированные Пользователи УЦ могут являться:

- владельцами ключей ЭП,
- владельцами КСКПЭП,
- пользователями КСКПЭП (владельцами которых являются другие пользователи).

Незарегистрированные пользователи могут являться:

- пользователями КСКПЭП (владельцами которых являются другие пользователи),
- пользователями, проходящими процедуру регистрации в УЦ

2.5. Разрешение споров

Сторонами в споре, в случае его возникновения, считаются Клиент и Общество, подписавшие Клиентский договор.

При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны должны руководствоваться действующим законодательством Российской Федерации.

Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в досудебном порядке.

Сторона, получившая от другой Стороны претензию, обязана в течение тридцати календарных дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

Все споры и разногласия между Сторонами, возникающие из Регламента или в связи с ним, в том числе касающиеся его действия, исполнения, изменения, прекращения или действительности, и по которым не было достигнуто соглашение, разрешаются в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

2.6. Ответственность сторон

Сторона, не исполнившая или ненадлежащим образом исполнившая свои обязательства по Регламенту, несет имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного другой Стороне. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Порядка своих обязательств.

Общество не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по Регламенту, а также возникшие в связи с этим убытки в случаях:

Если Общество обоснованно полагалось на сведения, указанные в заявлении Клиента;

Подделки, подлога либо иного искажения Клиентом либо третьими лицами информации, содержащейся в заявлении либо иных документах, предоставленных одной стороне от имени другой стороны.

Ответственность Сторон, не урегулированная положениями Клиентского договора и Регламента, регулируется законодательством Российской Федерации.

Общество не несёт ответственности за компрометацию маркера временного доступа и не возмещает ущерб, причиненный данными обстоятельствами.

2.7. Прекращение деятельности

Деятельность УЦ может быть прекращена в порядке, установленном законодательством Российской Федерации.

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

- 1) сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;
- 2) передать в уполномоченный федеральный орган в установленном порядке реестр

квалифицированных сертификатов;

3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

2.8. Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент составляется в письменной форме и заверяется собственноручной подписью Руководителя Общества и печатью Общества.

Изменения в Регламент вносятся путём составления дополнительного соглашения к Регламенту.

Изменению не подлежат положения настоящего Порядка, прямо или косвенно ущемляющие права пользователей услуг УЦ.

Утверждение и публикация дополнительных соглашений к Регламенту осуществляется в порядке, соответствующем порядку утверждения и публикации Регламента.

3. Права и обязанности Удостоверяющего центра и Клиентов (пользователей УЦ)

3.1. Права УЦ

УЦ имеет право:

3.1.1. Создавать сертификаты ключей проверки электронных подписей и выдавать такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 63-ФЗ «Об электронной подписи», на основании соглашения между удостоверяющим центром и заявителем.

3.1.2. Предоставлять КСКПЭП в электронной форме, находящихся в Реестре УЦ, всем лицам, обратившимся в УЦ;

3.1.3. Не проводить регистрацию лиц, обратившихся по вопросу представления КСКПЭП в электронной форме, находящихся в Реестре УЦ;

3.1.4. Отказать в предоставлении услуг по регистрации пользователям УЦ, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;

3.1.5. Отказать в изготовлении ключей не зарегистрированным пользователям УЦ, подавшим заявление на изготовление ключей, без предоставления информации о причинах отказа;

3.1.6. Отказать в изготовлении КСКПЭП зарегистрированным пользователям УЦ, подавшим заявление на изготовление КСКПЭП, с указанием причин отказа;

3.1.7. Отказать в аннулировании (отзыве) сертификата ключа проверки ЭП владельцу сертификата, подавшему заявление на аннулирование (отзыв) сертификата, в случае если истёк установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате;

3.1.8. Аннулировать (отозвать) сертификат ключа проверки ЭП Клиента в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного сертификата ключа проверки ЭП и указанием обоснованных причин;

3.1.9. Отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом

электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

3.1.10. Отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи.

3.1.11. Наделить третьих лиц (далее - доверенные лица) полномочиями по вручению сертификатов ключей проверки электронных подписей от имени этого удостоверяющего центра.

3.2. Права Клиентов

В этом разделе описаны права Клиентов для каждой группы пользователей УЦ, перечисленной в разделе 2.4.

3.2.1. Права лиц, не зарегистрированных в УЦ

Эту группу Клиентов составляют лица, не прошедшие регистрацию в УЦ, использующие сертификаты других зарегистрированных пользователей УЦ для каких-либо целей, например, для проверки электронных подписей.

Лица, не зарегистрированные в УЦ, имеют следующие права:

- Получать в электронной форме списки отозванных сертификатов ключей проверки ЭП, изготовленные УЦ;
- Получать в электронной форме КСКПЭП Уполномоченных лиц УЦ;
- Получать в электронной форме КСКПЭП Клиентов, находящиеся в Реестре КСКПЭП УЦ;
- Применять КСКПЭП УЦ для проверки электронных подписей УЦ в КСКПЭП пользователей, изготовленных УЦ.
- Применять КСКПЭП Клиентов для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в КСКПЭП.
- Применять список отозванных сертификатов ключей проверки ЭП, изготовленный УЦ, для проверки статуса КСКПЭП.
- Обращаться в УЦ для внесения в Реестр УЦ регистрационной информации о пользователе;
- Обращаться в УЦ за подтверждением подлинности электронных подписей в электронных документах;
- Обращаться в УЦ за подтверждением подлинности электронных подписей Уполномоченных лиц УЦ в изготовленных УЦ КСКПЭП пользователей;
- Обращаться в УЦ с целью получения (приобретения) средств электронной подписи.

3.2.2. Права лиц, зарегистрированных в УЦ

Эту группу Клиентов составляют лица, прошедшие полную регистрацию в УЦ.

Лица, составляющие группу зарегистрированных пользователей УЦ, имеют все права группы незарегистрированных пользователей и, дополнительно к ним, следующие права:

- Формировать ключи ЭП и ключи проверки ЭП на своём рабочем месте с использованием средства ЭП и программных средств, предоставляемых УЦ;

- Обращаться в УЦ для изготовления КСКПЭП;
- Пользоваться предоставляемыми УЦ программными средствами для получения и установки на своё рабочее место изготовленных КСКПЭП;
- Обращаться в УЦ для аннулирования (отзыва) своих КСКПЭП в течение срока действия соответствующих ключей ЭП.

3.2.3. Права лиц, которые проходят процедуру регистрации в УЦ

Эту группу пользователей услуг УЦ составляют лица, не прошедшие полную регистрацию в УЦ, но уже отправившие запрос на регистрацию, который ещё не одобрен оператором УЦ.

Лица, составляющие группу подавших запрос на регистрацию в УЦ пользователей, имеют все права группы незарегистрированных пользователей и, дополнительно к ним, следующие права:

- Обращаться в УЦ за проверкой состояния отправленного ранее запроса на регистрацию.

3.3. Обязанности УЦ

3.3.1. Обязанности аккредитованного удостоверяющего центра УЦ обязан

3.3.1.1. Выдавать квалифицированный сертификат в соответствии с требованиями Статьи 18 63-ФЗ «Об электронной подписи»;

3.3.1.2. Выполнять требования к содержанию и форме квалифицированного сертификата ключа проверки электронной подписи в соответствии со Статьей 17 63-ФЗ «Об электронной подписи» и Приказа ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи";

3.3.1.3. Использовать для изготовления ключей ЭП УЦ и формирования электронных подписей только средства криптографической защиты информации (средства электронной подписи), входящие в состав выбранной комплектации «КриптоПро УЦ» согласно (ЖТЯИ.00078-01 30 01).

При использовании в соответствии с положениями формуляра (ЖТЯИ.00078-01 30 01), ПAK «КриптоПро УЦ 2.0» удовлетворяет «Требованиям к средствам удостоверяющего центра» ФСБ России:

- варианты исполнения 1, 4 и 5 - классу КС2 (используются СКЗИ/средства ЭП класса КС2);
- варианты исполнения 2 и 6 - классу КС3 (используются СКЗИ/средства ЭП класса КС3);
- вариант исполнения 3 - классу КС1 (используются СКЗИ/средства ЭП класса КС1).

3.3.1.4. Хранить следующую информацию в течение всего срока деятельности в форме, позволяющей проверить ее целостность и достоверность:

- 1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
- 2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;
- 3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать

по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

3.3.1.5. Для подписания от своего имени квалифицированных сертификатов использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

3.3.1.6. Не использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

3.3.1.7. Обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов аккредитованного удостоверяющего центра в любое время в течение всего срока деятельности удостоверяющего центра.

3.3.1.8. В случае принятия решения о прекращении своей деятельности сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности, передать в уполномоченный федеральный орган в установленном порядке реестр выданных квалифицированных сертификатов, передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению.

3.3.1.9. Выполнять требования настоящего Порядка реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее Порядок).

3.3.1.10. Не наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от своего имени.

3.3.1.11. Использовать ключи ЭП УЦ только для подписи издаваемых им сертификатов ключей проверки ЭП и списков отозванных сертификатов.

3.3.1.12. Принять меры по защите ключей ЭП УЦ в соответствии с положениями настоящего Порядка.

3.3.1.13. Осуществлять в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи.

3.3.1.14. Устанавливать сроки действия сертификатов ключей проверки электронных подписей;

3.3.1.15. Аннулировать выданные сертификаты ключей проверки электронных подписей, в случаях предусмотренных 63-ФЗ «Об электронной подписи»;

3.3.1.16. Выдать по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

3.3.1.17. Вести реестр выданных и аннулированных сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

3.3.1.18. Создавать по обращениям заявителей ключи электронных подписей и

ключи проверки электронных подписей;

3.3.1.19. Проверять уникальность ключей проверки электронных подписей в реестре сертификатов;

3.3.1.20. Осуществлять по обращениям участников электронного взаимодействия проверку электронных подписей;

3.3.1.21. Информировать в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

3.3.1.22. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

3.3.1.23. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;

3.3.1.24. Обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей;

3.3.1.25. Не указывать в создаваемом сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром;

3.3.1.26. Хранить информацию, внесенную в реестр сертификатов, в течение всего срока деятельности удостоверяющего центра.

3.3.2. Синхронизация времени

УЦ организует работу своих Служб по Всемирному координированному времени (UTC) с учётом часового пояса места расположения УЦ.

УЦ обязан синхронизировать по времени все программные и технические средства обеспечения деятельности по назначению.

3.3.3. Регистрация пользователей УЦ

УЦ обеспечивает регистрацию Пользователей УЦ по заявлениям на регистрацию в соответствии с порядком регистрации, изложенным в настоящем Регламенте.

УЦ обязан обеспечить уникальность информации, используемой для идентификации и аутентификации Пользователей УЦ в УЦ.

УЦ обязан не разглашать (публиковать) регистрационную информацию пользователей УЦ, за исключением информации, заносимой в изготавливаемые сертификаты.

3.3.4. Изготовление ключей ЭП и ключей проверки ЭП пользователей УЦ

УЦ обязан изготовить ключ ЭП и ключ проверки ЭП зарегистрированному Пользователю УЦ по заявлению с использованием средств электронной подписи, сертифицированных в соответствии с действующим законодательством Российской Федерации.

УЦ обязан обеспечить сохранение в тайне изготовленного ключа ЭП.

УЦ обязан записать ключ на отчуждаемый носитель, в соответствии с требованиями

по эксплуатации программного и/или аппаратного средства, выполняющего процедуру генерации ключей.

УЦ обязан выполнять процедуру генерации ключей и запись ключей на отчуждаемый носитель только с использованием программного и/или аппаратного средства, сертифицированного в соответствии с законодательством Российской Федерации.

УЦ обязан обеспечить защиту ключевого носителя от копирования.

3.3.5. Изготовление квалифицированных сертификатов ключей проверки ЭП

УЦ обеспечивает изготовление КСКПЭП зарегистрированному Пользователю УЦ по заявлению, в соответствии с форматом и порядком идентификации владельца КСКПЭП, определённым в настоящем Регламенте.

Руководством общества назначено лицо, ответственное за создание и проверку ЭП в УЦ. Также назначено лицо, ответственное за аннулирование КСКПЭП.

УЦ обязан обеспечить уникальность регистрационных (серийных) номеров изготавливаемых КСКПЭП Пользователей УЦ.

УЦ обязан обеспечить уникальность значений ключей проверки ЭП в изготовленных КСКПЭП пользователей УЦ.

3.3.6. Аннулирование квалифицированных сертификатов ключей проверки ЭП

УЦ обязан аннулировать КСКПЭП:

- 1) по заявлению его владельца.
- 2) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- 3) установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- 4) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

УЦ обязан в течение 12 часов занести сведения об аннулированном сертификате в список отозванных сертификатов с указанием даты, времени, причины аннулирования.

3.3.7. Уведомления

3.3.7.1. Уведомление о факте изготовлении квалифицированного сертификата ключа проверки ЭП

УЦ обязан официально уведомить о факте изготовления сертификата ключа проверки ЭП его владельца.

Срок уведомления — не позднее 24 часов с момента изготовления сертификата ключа проверки ЭП.

Официальным уведомлением о факте изготовлении сертификата является отправка почтового сообщения по электронной почте с прикреплённым сертификатом ключа проверки ЭП с адреса отправителя uc@garant.ru.

Временем отправки почтового сообщения признается время отправки почтового сообщения с почтового сервера, осуществляющего отправки почтовых сообщений УЦ, и

включённое в заголовок почтового сообщения.

3.3.7.2. Уведомление о факте аннулирования сертификата ключа проверки ЭП

УЦ обязан официально уведомить о факте аннулирования сертификата ключа проверки ЭП его владельца.

Срок уведомления — не позднее 24 часов с момента занесения сведений об аннулированном сертификате в список отозванных сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка отозванных сертификатов, который содержит сведения об аннулированном сертификате, по адресам

http://ca.garant.ru/cdp/accredited/garant_ac3.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac3.crl

http://ca.garant.ru/cdp/accredited/garant_ac4.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac4.crl

http://ca.garant.ru/cdp/accredited/garant_ac5.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac5.crl

http://ca.garant.ru/cdp/accredited/garant_ac6.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac6.crl

http://ca.garant.ru/cdp/accredited/garant_ac7.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac7.crl

http://ca.garant.ru/cdp/accredited/garant_ac8.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac8.crl

http://ca.garant.ru/cdp/accredited/garant_ac9.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac9.crl

http://ca.garant.ru/cdp/accredited/garant_ac10.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac10.crl

http://ca.garant.ru/cdp/accredited/garant_ac11.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac11.crl

http://ca.garant.ru/cdp/accredited/garant_ac12.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac12.crl

http://ca.garant.ru/cdp/accredited/garant_ac13.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac13.crl

Временем аннулирования КСКПЭП признается время занесения сведений об аннулированном сертификате в список отозванных сертификатов, указанное в списке отозванных сертификатов.

Временем опубликования списка отозванных сертификатов признается время изготовления списка отозванных сертификатов, указанное в списке отозванных

сертификатов.

УЦ обязан включать полный адрес (URL) списка отозванных сертификатов из репозитория УЦ в издаваемые КСКПЭП пользователей УЦ.

3.3.8. Реестр квалифицированных сертификатов ключа проверки ЭП

УЦ обязан вести Реестр всех изготовленных КСКПЭП пользователей УЦ в течение установленного срока хранения.

Реестр сертификатов ключей проверки ЭП ведётся в электронном виде.

УЦ обязан осуществлять выдачу КСКПЭП в электронной форме по обращениям пользователей УЦ.

УЦ обязан публиковать выписки из Реестра, позволяющие определить действительность КСКПЭП пользователей УЦ.

Выписка из Реестра УЦ предоставляется в виде списка отозванных сертификатов в электронной форме и формате, определённом настоящим Регламентом.

3.3.9. Восстановление работоспособности УЦ после сбоев

В целях недопущения технических сбоев Удостоверяющий центр обязан обеспечить выполнение мероприятий, направленных на их предотвращение и оперативное восстановление работоспособности средств УЦ, руководствуясь «Порядком технического обслуживания средств обеспечения деятельности УЦ», изложенным в п. 9.6. настоящего Регламента. В случае возникновения технического сбоя Удостоверяющий центр должен обеспечить информирование участников информационных систем о статусе сертификатов не позднее 2-х часов с момента наступления сбоя (обеспечить публикацию списков отозванных сертификатов), а полное восстановление работоспособности УЦ - не позднее суток с момента наступления сбоя.

3.3.10. Прочие обязанности

УЦ обязан уведомлять владельца КСКПЭП о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования КСКПЭП.

3.4. Обязанности Клиентов

В этом разделе описаны обязанности Клиентов для каждой группы пользователей УЦ, перечисленной в разделе 2.4.

3.4.1. Обязанности лиц, не зарегистрированных в УЦ

Лица, не зарегистрированные в УЦ, если являются пользователями КСКПЭП, изготовленных этим УЦ, обязаны:

- перед использованием КСКПЭП, изготовленного этим УЦ, удостовериться, что назначения ключа и назначения сертификата, указанные в сертификате, соответствуют предполагаемому использованию сертификата, согласно настоящему Регламенту.

3.4.2. Обязанности лиц, зарегистрированных в УЦ

Лица, зарегистрированные в УЦ, если являются владельцами ключей ЭП, на соответствующие ключи проверки ЭП которых в этом УЦ изготовлены сертификаты, обязаны:

- хранить в тайне свой ключ ЭП, принимать всевозможные меры для предотвращения его потери, раскрытия, изменения или несанкционированного использования;
- не использовать для электронной подписи ключи электронной подписи, если ему известно, что эти ключи используются или использовались ранее другими лицами;
- использовать ключи ЭП только для целей, разрешённых назначениями ключа и назначениями сертификата, согласно настоящему Регламенту.

Лица, зарегистрированные в УЦ, если являются владельцами сертификатов ключей проверки ЭП, изготовленных этим УЦ, обязаны:

- использовать сертификаты своих ключей проверки ЭП только для целей, разрешённых назначениями ключа и назначениями сертификата, которые указаны в сертификате, согласно настоящему Регламенту;
- немедленно обращаться в УЦ с заявлением на аннулирование (отзыв) КСКПЭП в случае, если стало известно, что эти ключи используются или использовались ранее другими лицами.

Лица, зарегистрированные в УЦ, если им предоставлен Маркер временного доступа, который будет использован для обращения на страницу формирования ключа электронной подписи и запроса на КСКПЭП, обязаны:

- хранить в тайне Маркер временного доступа в течение срока действия маркера.

3.4.3. Обязанности лиц, которые проходят процедуру регистрации в УЦ

Лица, которые проходят процедуру регистрации в УЦ, обязаны:

- предоставлять регистрационную и идентифицирующую информацию в объёме, определённом положениями настоящего Регламента.

Лица, которые проходят процедуру регистрации в УЦ, если им предоставлен Маркер временного доступа, который будет использован для обращения на страницу формирования ключа электронной подписи и запроса на КСКПЭП, обязаны:

- хранить в тайне предоставленный Маркер временного доступа в течение срока действия маркера.

4. Политика конфиденциальности

4.1. Типы конфиденциальной информации

Ключ ЭП владельца сертификата ключа проверки ЭП является конфиденциальной информацией данного Пользователя УЦ. УЦ не депонирует и не архивирует ключи ЭП.

Маркер временного доступа, который используется для обращения на страницу формирования ключа электронной подписи и запроса на КСКПЭП, считается конфиденциальной информацией.

Персональная и корпоративная информация пользователей УЦ, содержащаяся в УЦ, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки ЭП, списка отозванных сертификатов, считается конфиденциальной и не публикуется.

Информация, хранящаяся в журналах аудита УЦ, считается конфиденциальной и не

подлежит разглашению.

Отчётные материалы по выполненным проверкам деятельности УЦ являются конфиденциальными, за исключением заключения по результатам проверок, публикуемого в соответствии с настоящим Регламентом.

4.2. Типы информации, не являющейся конфиденциальной

Информация, не являющейся конфиденциальной информацией, является открытой информацией.

Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации также определяется решением УЦ.

Информация, включаемая в сертификаты ключей проверки ЭП пользователей УЦ и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной.

Также не считается конфиденциальной информация о настоящем Регламенте.

4.3. Исключительные полномочия официальных лиц

УЦ не должен раскрывать информацию, относящуюся к типу конфиденциальной информации, каким бы то ни было третьим лицам, за исключением:

- случаев, определённых в настоящем Регламенте;
- случаев, требующих раскрытия в соответствии с действующим законодательством или при наличии судебного постановления.

5. Перечень реализуемых Удостоверяющим центром функций. Процедуры и механизмы.

5.1. Перечень реализуемых Удостоверяющим центром функций.

Удостоверяющий центр:

5.1.1. Создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 63-ФЗ «Об электронной подписи»;

5.1.2. Осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

5.1.3. Устанавливает сроки действия сертификатов ключей проверки электронных подписей;

5.1.4. Аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

5.1.5. Выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5.1.6. Ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в

том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

5.1.7. Устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

5.1.8. Создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

5.1.9. Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

5.1.10. Осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

5.1.11. Информировывает в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

5.1.12 Обеспечивает актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

5.1.13 Предоставляет безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;

5.1.14 Обеспечивает конфиденциальность созданных удостоверяющим центром ключей электронных подписей;

5.1.15. Отказывает заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

5.1.16. Отказывает заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи.

5.1.17. Не указывает в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

5.1.18. Наделяет доверенных лиц (далее Центры регистрации) полномочиями по вручению сертификатов ключей проверки электронных подписей от имени удостоверяющего центра. При вручении сертификата ключа проверки электронной подписи центр регистрации устанавливает личность получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата в соответствии с порядком реализации функций удостоверяющего центра и исполнения его обязанностей, установленным наделившим указанное доверенное лицо полномочиями по вручению сертификатов ключей проверки электронной подписи удостоверяющим центром с учетом предусмотренных пунктом 4

части 4 статьи 8 63-ФЗ «Об электронной подписи» требований.

5.1.19. Осуществляет проверку электронных подписей, ключи проверки которых указаны в выданных Центрами Регистраций сертификатах ключей проверки электронных подписей;

5.1.20. Обеспечивает электронное взаимодействие Центров Регистраций между собой, а также Центров Регистраций с Удостоверяющим центром.

5.2. Порядок и сроки выполнения действий для предоставления услуг Удостоверяющим центром

Для получения услуг Удостоверяющего центра Клиент должен обратиться в Центр Регистрации любым из доступных способов.

Клиент обсуждает набор услуг со своим персональным менеджером, который закрепляется за клиентом с момента первого обращения в Центр Регистрации.

Клиент получает полную информацию о тех требованиях, которые он должен выполнить при получении услуг Удостоверяющего центра, в том числе требования к документам для получения КСКПЭП.

Клиенту выставляется счет на услуги, которые он должен оплатить в течение трех рабочих дней.

После поступления средств на расчетный счет Общества, с Клиентом связывается уполномоченный сотрудник Центра Регистрации и назначается удобное время посещения офиса Центра Регистрации.

Клиент лично предоставляет в Центр Регистрации все необходимые документы.

Сотрудник Центра Регистрации проверяет предъявленные документы и все данные, которые будут включены в сертификат, в том числе с помощью получения необходимой информации через СМЭВ и при принятии положительного решения о регистрации, выполняет регистрацию Клиента и Пользователя УЦ в Удостоверяющем центре;

Клиент заключает с Обществом Клиентский договор.

5.3. Процедура регистрации пользователей УЦ

Под регистрацией пользователей УЦ понимается внесение регистрационной информации о пользователях УЦ в Реестр УЦ.

Процедура регистрации пользователей УЦ применяется в отношении Клиентов, обращающихся к услугам УЦ в части изготовления КСКПЭП пользователей УЦ и/или формирования ключей ЭП и ключей проверки ЭП пользователей УЦ с записью их на ключевой носитель.

5.3.1. Заявление на регистрацию

Для получения КСКПЭП Пользователь УЦ должен подать правильно заполненное Заявление на изготовление сертификата.

Для регистрации лица - будущего владельца квалифицированного сертификата Заявление должно содержать данные, установленные Статьей 17 63-ФЗ «Об электронной подписи».

Форма заявлений приведена в Приложениях 2а и 2б Регламента.

Заявление может быть подано в бумажном виде с подписью Пользователя УЦ и Клиента или в электронном виде, подписанное квалифицированной электронной подписью Клиента.

5.3.2. Идентификация Пользователя УЦ

При проверке Заявления уполномоченный сотрудник Центра Регистрации должен идентифицировать личность заявителя.

Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность - паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, уполномоченный сотрудник Центра Регистрации может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;

Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства. Если документы не на русском языке, то должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

Заявитель представляет в Центр Регистрации документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности заявителя, а также документы, подтверждающие сведения, на основании которых Удостоверяющим центром вносятся сведения в сертификат, в том числе:

Для заявителя-юридического лица - полное или сокращенное наименование юридического лица, основной государственный регистрационный номер, адрес местонахождения, страховой номер индивидуального лицевого счета Пользователя УЦ.

Для заявителя-физического лица - страховой номер индивидуального лицевого счета, идентификационный номер налогоплательщика.

Для заявителя-физического лица индивидуального предпринимателя - страховой номер индивидуального лицевого счета, идентификационный номер налогоплательщика, основной государственный регистрационный номер индивидуального предпринимателя.

Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц;

После идентификации личности заявителя, проверке Заявления и всех предоставленных документов, а также получения данных через СМЭВ для проверки данных, включаемых в КСКПЭП, уполномоченный сотрудник Центра Регистрации регистрирует Клиента и Пользователя УЦ в Удостоверяющем центре.

5.4. Создание ключей электронных подписей и ключей проверки электронных подписей.

5.4.1 Порядок создания ключей электронных подписей и ключей проверки электронных подписей

5.4.1.1. Пользователь УЦ создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный N 6382) с изменениями, внесенными

приказом ФСБ России 12 апреля 2010 г. N 173 "О внесении изменений в некоторые нормативные правовые акты ФСБ России" (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный N 17350) самостоятельно на своем рабочем месте, используя маркер временного доступа и записывает ключ электронной подписи на сертифицированный защищенный носитель и направляет запрос на КСКПЭП в Удостоверяющий центр через защищенный канал связи, который построен на основе web технологии с защитой по протоколу TLS с обязательной аутентификацией сервера.

Пользователь УЦ повторно приезжает в офис Центра Регистрации.

При повторном посещении Администратор УЦ проверяет запрос на сертификат на корректность запрошенных данных и выпускает КСКПЭП.

Пользователь УЦ ставит собственноручную подпись в бумажном документе, содержащем информацию из его КСКПЭП (данный документ передается на архивное хранение в Удостоверяющий центр) или подписывает электронный документ, содержащий информацию из его КСКПЭП посредством действующего квалифицированного сертификата.

5.4.1.2. Уполномоченный сотрудник Удостоверяющего центра после положительной проверки всех необходимых документов и регистрации Клиента и Пользователя УЦ в Удостоверяющем центре создает ключ электронной подписи и ключ проверки электронной подписи для заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)". Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона "Об электронной подписи" создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также необходимость выполнения требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049) в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя и записывает на сертифицированный ключевой носитель.

Уполномоченный сотрудник Удостоверяющего центра проверяет запрос на КСКПЭП на корректность данных и выпускает КСКПЭП.

Сохраненные на сертифицированном защищенном носителе ключ электронной подписи и КСКПЭП передаются Пользователю УЦ.

Пользователь УЦ ставит собственноручную подпись в бумажном документе, содержащем информацию из его КСКПЭП (данный документ передается на архивное хранение в Удостоверяющий центр) или подписывает электронный документ, содержащий информацию из его КСКПЭП посредством действующего квалифицированного сертификата.

Одновременно с выдачей КСКПЭП его владельцу выдается средство квалифицированной электронной подписи, соответствующее требованиям Приказа ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» и «Руководство по

обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» в виде ссылки на страницу сайта УЦ <https://www.garantexpress.ru/wp-content/uploads/2019/04/rukovodstvo.pdf>.

Все бумажные документы, заверенные собственноручной подписью Пользователя УЦ передаются на архивное хранение.

Сертификат создается не позднее 10 минут с момента получения Администратором УЦ запроса на сертификат.

Стоимость по созданию и выдаче сертификатов приведена в Приложении №13.

5.5. Сроки действия ключей электронной подписи УЦ

Максимальный срок действия ключа ЭП и сертификата ключа проверки ЭП Уполномоченного лица УЦ определяются требованиями применяемого средства криптографической защиты информации.

Для УЦ ООО «Электронный экспресс» установлены следующие максимальные сроки действия ключей ЭП и ключей проверки ЭП УЦ.

Срок действия ключа электронной подписи Удостоверяющего центра составляет 3 (три) года.

Срок действия ключа электронной подписи Удостоверяющего центра для изготовления КСКПЭП Пользователей УЦ не превышает 1 (один) год и 3 (три) месяца. Остальное время действия ключа электронной подписи Удостоверяющего центра можно использовать только для выпуска Списков аннулированных (отозванных) КСКПЭП.

Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты ввода ключа электронной подписи и соответствующего КСКПЭП в эксплуатацию.

Срок действия КСКПЭП Удостоверяющего центра составляет 15 (пятнадцать) лет. При истечении срока действия ключа электронной подписи УЦ производится его плановая смена.

5.6. Смена ключей ЭП Удостоверяющего центра

5.6.1. Плановая смена ключей ЭП Удостоверяющего центра

Плановая смена ключей (ключа ЭП и соответствующего ему ключа проверки ЭП) УЦ должна выполняться в течение срока действия ключа ЭП УЦ.

Процедура плановой смены ключа электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

- Администратор Удостоверяющего центра создает новый ключ электронной подписи;
- Формируется запрос на подчиненный КСКПЭП, который направляется в Головной Удостоверяющий Центр Минкомсвязи России;
- После изготовления Головным Удостоверяющим центром Минкомсвязи России подчиненного КСКПЭП Удостоверяющего центра и его регистрации в системе ЕСИА, новый ключ электронной подписи и КСКПЭП Удостоверяющего центра вводятся в эксплуатацию.

Предыдущий ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования Списков аннулированных (отозванных) КСКПЭП.

Все Пользователи УЦ информируются о плановой смене КСКПЭП Удостоверяющего

центра по электронной почте со ссылкой на новый подчиненный квалифицированный сертификат ключа проверки электронной подписи, размещенный на портале Минкомсвязи <https://e-trust.gosuslugi.ru> и размещением информации на сайте Удостоверяющего центра в сети Интернет.

5.6.2. Внеплановая смена ключей ЭП Удостоверяющего центра

Смена ключа электронной подписи Удостоверяющим центром осуществляется в случае нарушения конфиденциальности ключа электронной подписи или угрозы нарушения конфиденциальности такого ключа электронной подписи.

Случаи нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра:

- ключ ЭП был получен несанкционированным пользователем;
- ключ ЭП утрачен в связи с невыполнением регламентных процедур УЦ;

Виды угроз нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра:

- угрозы внешнего нарушителя;
- угрозы внутреннего нарушителя;
- угрозы в связи с невыполнением регламентных процедур УЦ;

В случае компрометации или утраты ключа электронной подписи Удостоверяющего центра выполняется внеплановая смена ключа электронной подписи Удостоверяющего центра.

Удостоверяющий центр официально уведомляет Пользователей УЦ о факте внеплановой смены ключа электронной подписи Удостоверяющего центра и причинах ее проведения по электронной почте и размещением информации на сайте Удостоверяющего центра в сети Интернет. Прекращают действие все квалифицированные сертификаты изготовленные скомпрометированным ключом электронной подписи Удостоверяющего центра, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

После получения официального уведомления о факте внеплановой смены ключа электронной подписи Удостоверяющего центра Пользователям УЦ **запрещается** использовать свои ключи электронной подписи и КСКПЭП.

Процедура внеплановой смены ключа электронной подписи Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключа электронной подписи Удостоверяющего центра.

После получения официального уведомления о факте внеплановой смены ключа электронной подписи Удостоверяющего центра, Пользователям УЦ необходимо выполнить процедуру получения новых ключей электронной подписи и КСКПЭП как в первый раз в соответствии с действующим Порядком, установленным Регламентом. При внеплановой смене ключа электронной подписи Удостоверяющего центра перевыпуск КСКПЭП Пользователей УЦ осуществляется на безвозмездной основе.

5.6.3. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца квалифицированного сертификата.

Смена ключа электронной подписи владельца квалифицированного сертификата осуществляется в случаях прекращения действия сертификата ключа электронной подписи:

- 1) в связи с истечением установленного срока его действия;

2) на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

3) в иных случаях, установленных 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи;

и в случае аннулирования квалифицированного сертификата, выполненного в следующих случаях:

1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

2) установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;

3) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

Заявление на изготовление квалифицированного сертификата должно соответствовать форме Приложения 2а для юридических лиц и Приложения 2б для индивидуальных предпринимателей и физических лиц.

Заявление на смену ключа электронной подписи владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца квалифицированного сертификата, при этом в случае, если смена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата;

Выдача квалифицированного сертификата осуществляется в соответствии 5.4. Создание ключей электронных подписей, ключей проверки электронных подписей и выдача квалифицированных сертификатов.

Выдача квалифицированного сертификата осуществляется в соответствии с требованиями Статьи 18 63-ФЗ «Об электронной подписи» и раздела «Создание ключей электронных подписей, ключей проверки электронных подписей и выдача квалифицированных сертификатов» настоящего Порядка.

5.6.4. Создание и выдача квалифицированных сертификатов

1. Для получения квалифицированного сертификата заявитель обращается в Центр Регистрации с заявлением на создание и выдачу квалифицированного сертификата. Заявление на создание и выдачу квалифицированного сертификата должно быть оформлено по форме Приложения 2а для юридических лиц и Приложения 2б для физических лиц и индивидуальных предпринимателей. Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.

При обращении заявителя в Центр Регистрации устанавливается его личность по оригиналам следующих документов:

- 1) Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность;
- 2) Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства переведенного на русский язык и заверенному нотариально;
- 3) Личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц;

2. С целью исполнения Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», а именно п.1 ч.1 статьи 18 - при выдаче квалифицированного сертификата УЦ обязан идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата, а также исключения имеющих место случаев мошеннических действий (получение сертификатов по поддельным документам), для подтверждения получения квалифицированного сертификата конкретным лицом УЦ ведет фотографирование владельца сертификата. Поэтому обязательным критерием идентификации владельца сертификата при его личном присутствии, наряду с удостоверяющим личность документом, является его фотографирование сотрудником Центра Регистрации до выдачи сертификата.

3. При обращении в удостоверяющий центр заявитель указывает на ограничения использования квалифицированного сертификата (если такие ограничения им устанавливаются) и представляет следующие документы либо их надлежащим образом заверенные копии и сведения:

- 1) основной документ, удостоверяющий личность;
- 2) номер страхового свидетельства государственного пенсионного страхования заявителя - физического лица;
- 3) идентификационный номер налогоплательщика заявителя - физического лица;
- 4) основной государственный регистрационный номер заявителя - юридического лица;
- 5) основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя - индивидуального предпринимателя;
- 6) номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в пунктах 4-6 части 2 статьи 18 63-ФЗ «Об электронной подписи».

4. Удостоверяющий центр с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 статьи 18 63-ФЗ «Об электронной подписи». Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 63-ФЗ «Об электронной подписи» аккредитованный удостоверяющий центр запрашивает и получает из государственных информационных ресурсов:

- 1) выписку из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;

2) выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;

3) выписку из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

5. В случае, если полученные сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и аккредитованным удостоверяющим центром установлена личность заявителя - физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата, удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

6. При получении квалифицированного сертификата заявителем он должен под расписку ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате.

7 Удостоверяющий центр одновременно с выдачей квалифицированного сертификата выдает владельцу квалифицированного сертификата «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» в виде ссылки на страницу сайта УЦ <https://www.garantexpress.ru/wp-content/uploads/2019/04/rukovodstvo.pdf>.

8. При выдаче квалифицированного сертификата удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра

5.6.5. Порядок создания квалифицированного сертификата

При получении положительного решения о возможности выдачи квалифицированного сертификата Администратор УЦ сверяет данные заявления и переданного в УЦ запроса на квалифицированный сертификат, содержащий ключ проверки электронной подписи и проводит процедуру регистрации пользователя УЦ и изготовления квалифицированного сертификата

5.6.6. Порядок выдачи квалифицированного сертификата

Квалифицированный сертификат устанавливается на сертифицированный ключевой носитель и передаются Пользователю УЦ.

Пользователь УЦ ставит собственноручную подпись в бумажном документе, содержащем информацию из его КСКПЭП (данный документ передается на архивное хранение в Удостоверяющий центр) или подписывает электронный документ, содержащий информацию из его КСКПЭП посредством действующего квалифицированного сертификата.

Одновременно с выдачей КСКПЭП его владельцу выдается средство квалифицированной электронной подписи, соответствующее требованиям Приказа ФСБ

РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требованиям к средствам удостоверяющего центра» и «Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи» в виде ссылки на страницу сайта УЦ <https://www.garantexpress.ru/wp-content/uploads/2019/04/rukovodstvo.pdf>.

Все бумажные документы, заверенные собственноручной подписью Пользователя УЦ передаются на архивное хранение.

5.6.7. Срок создания и выдачи квалифицированного сертификата

Вся процедура создания и выдачи квалифицированного сертификата, с учетом выполнения всех требований по установлению личности и проверки всех данных включаемых в квалифицированный сертификат занимает не более 30 минут с момента обращения заявителя в Центр Регистрации с Заявлением на изготовление квалифицированного сертификата.

5.7. Процедура подтверждения действительности электронной подписи УЦ в квалифицированном сертификате ключа проверки ЭП

Для подтверждения действительности электронной подписи Удостоверяющего центра в изготовленном КСКПЭП, Клиент подает в Центр Регистрации письменное заявление.

Форма заявления приведена в Приложении № 7а, 7б настоящего Регламента. Обязательным приложением к заявлению является CD диск, содержащий файл КСКПЭП подвергающийся процедуре проверки (в кодировке Base64).

Срок оказания услуг по подтверждению действительности электронной подписи Удостоверяющего центра в КСКПЭП Пользователя УЦ составляет десять рабочих дней с момента поступления заявления в Центр Регистрации.

Стоимость оказания услуг определяется в соответствии с «Ценовыми предложениями», действующими на момент оказания услуг.

Подтверждение действительности электронной подписи Удостоверяющего центра в КСКПЭП Пользователя УЦ производится посредством выдачи заключения Удостоверяющего центра в письменной форме, подписанное всеми членами комиссии и заверенное печатью Удостоверяющего центра.

Заключение содержит:

- результат проверки электронной подписи Удостоверяющего центра (верна/неверна);
- на момент времени, указанного в заявлении, квалифицированный сертификат Пользователя УЦ действовал/не действовал;
- отчет по выполненной проверке;

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные для проведения проверки.

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.

Клиент получает отчет по выполненной проверке в Центре Регистрации.

5.8. Процедура подтверждения действительности электронной подписи, использованной для подписания электронных документов

Удостоверяющий центр осуществляет проведение экспертизы по подтверждению действительности электронной подписи в электронном документе в случае, если формат электронного документа с электронной подписью соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS). Решение о соответствии электронного документа с электронной подписью стандарту CMS принимает Удостоверяющий центр.

Для подтверждения подлинности электронной подписи в электронных документах Клиент подает заявление в Удостоверяющий центр по форме, приведенной в Приложении №8а или 8б. Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность электронной подписи которого необходимо подтвердить в электронном документе;
- время и дата формирования электронной подписи электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность электронной подписи.

Обязательным приложением к заявлению на подтверждение подлинности электронной подписи в электронном документе является электронный носитель, содержащий:

- КСКПЭП, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе – в виде файла стандарта CMS;
- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

Проведение подтверждения действительности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Для подтверждения действительности электронной подписи проводится проверка действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата удостоверяющего центра, выданного головным удостоверяющим центром.

В результате проведения подтверждения подлинности электронной подписи в электронном документе формируется заключение Удостоверяющего центра. Заключение содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- итоги проверки электронной подписи электронного документа;
- данные, представленные комиссии для проведения проверки.
- отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и итоги проверки;

- обоснование итогов проверки.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю. Срок проведения подтверждения подлинности электронной подписи в одном электронном документе и предоставление пользователю заключения по выполненной проверке составляет десять рабочих дней с момента поступления заявления в Удостоверяющий центр.

5.9. Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата

5.9.1. Основания прекращения действия или аннулирования квалифицированного сертификата.

Квалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона "Об электронной подписи":

- 1) в связи с истечением установленного срока его действия;
- 2) на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- 3) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;
- 4) в иных случаях, установленных настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

5.9.2. Случаи аннулирования сертификата ключа проверки электронной подписи Удостоверяющим центром

Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

- 1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- 2) установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- 3) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

5.9.3. Аннулирование квалифицированного сертификата

Аннулирование сертификата ключа проверки ЭП, изготовленного УЦ, осуществляется УЦ по заявлению на аннулирование сертификата ключа проверки ЭП его владельца (далее по тексту раздела — заявитель).

Сертификат прекращает свое действие:

- по истечении срока его действия;
- по заявлению владельца сертификата о прекращении действия КСКПЭП;

- в случае прекращения деятельности Удостоверяющего центра без передачи его функций другим лицам;

Удостоверяющий центр признает КСКПЭП аннулированным, если:

- не подтверждено, что владелец КСКПЭП владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком КСКПЭП;
- установлено, что содержащийся в КСКПЭП ключ проверки электронной подписи уже содержится в ином ранее созданном КСКПЭП;
- вступило в силу решение суда, которым установлено, что КСКПЭП содержит недостоверную информацию.

Срок внесения информации о прекращении действия или аннулировании Сертификата в Реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

Для аннулирования действия КСКПЭП, Пользователь УЦ подает письменное заявление на требуемое действие в Центр Регистрации.

Заявление на выполнение действий с КСКПЭП заверяется собственноручной подписью Пользователя УЦ — владельца КСКПЭП и Клиентом (если Клиент является юридическим лицом).

Форма заявления на аннулирование КСКПЭП Пользователя УЦ приведены в Приложениях №6а, 6б настоящего Порядка.

Заявление об аннулировании квалифицированного сертификата может быть подано как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.

Запросы на аннулирование КСКПЭП Пользователя УЦ являются наиболее приоритетными и выполняются в первую очередь.

Положительное решение о выполнении запрошенной операции с КСКПЭП Пользователя УЦ принимается сотрудником Центра Регистрации при идентификации Пользователя УЦ по документу удостоверяющему личность.

После выполнения запрошенного действия с КСКПЭП Пользователя УЦ будет выпущен и опубликован новый Список отозванных сертификатов.

Период действия списков отозванных сертификатов составляет 24 часа. Период планового обновления Списков отозванных сертификатов составляет 12 часов.

Адреса публикации Списков аннулированных (отозванных) КСКПЭП:

http://ca.garant.ru/cdp/accredited/garant_ac3.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac3.crl

http://ca.garant.ru/cdp/accredited/garant_ac4.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac4.crl

http://ca.garant.ru/cdp/accredited/garant_ac5.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac5.crl

http://ca.garant.ru/cdp/accredited/garant_ac6.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac6.crl

http://ca.garant.ru/cdp/accredited/garant_ac7.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac7.crl

http://ca.garant.ru/cdp/accredited/garant_ac8.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac8.crl

http://ca.garant.ru/cdp/accredited/garant_ac9.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac9.crl

http://ca.garant.ru/cdp/accredited/garant_ac10.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac10.crl

http://ca.garant.ru/cdp/accredited/garant_ac11.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac11.crl

http://ca.garant.ru/cdp/accredited/garant_ac12.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac12.crl

http://ca.garant.ru/cdp/accredited/garant_ac13.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac13.crl

Публикация в сети Интернет актуальных списков аннулированных (отозванных) КСКПЭП обеспечивает любому лицу безвозмездный доступ к данной информации.

Временем выполнения запрошенного действия с КСКПЭП Пользователя УЦ признается время публикация нового Списка отозванных сертификатов, изготовленного Удостоверяющим центром после произведенных действий с КСКПЭП.

Выполнение запрошенных действий с сертификатом ключа подписи Пользователя УЦ производится в течение 30 минут после обращения Пользователя УЦ в Центр Регистрации с соответствующим заявлением.

5.10 Порядок ведения реестра квалифицированных сертификатов

Реестр квалифицированных сертификатов ведется в соответствии с требованиями Приказа Министерства связи и массовых коммуникаций РФ от 22 августа 2017 г. N 436

1. Формирование реестра квалифицированных сертификатов включает в себя внесение сертификата ключа проверки электронной подписи в реестр квалифицированных сертификатов.

2. Ведение реестра квалифицированных сертификатов включает в себя:

внесение изменений в реестр квалифицированных сертификатов в случае изменения содержащихся в нем сведений;

внесение в реестр квалифицированных сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

3. Информация, внесенная в реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности аккредитованного удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

4. Хранение информации, содержащейся в реестре квалифицированных сертификатов, должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

5. Обеспечена защита информации, содержащейся в реестре квалифицированных

сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

6. Формирование и ведение реестра квалифицированных сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

7. Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре квалифицированных сертификатов формируется его резервная копия.

9. Обеспечена актуальность информации, содержащейся в реестре квалифицированных сертификатов.

5.10.1. Структура реестра квалифицированных сертификатов

10. Реестр квалифицированных сертификатов состоит из следующих разделов:

квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам;

квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам;

квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам, прекратившие свое действие;

квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам, прекратившие свое действие;

аннулированные квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам;

аннулированные квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам.

11. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам" содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
- 4) страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата;
- 5) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат;
- 6) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются).

12. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам" содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- 4) идентификационный номер налогоплательщика владельца квалифицированного сертификата;
- 5) реквизиты документа, подтверждающего факт внесения записи в Единый государственный реестр юридических лиц (для юридических лиц, зарегистрированных на территории Российской Федерации);

б) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат;

7) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются).

13. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам, прекратившие свое действие" содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
- 4) дата прекращения действия квалифицированного сертификата;
- 5) основание прекращения действия квалифицированного сертификата.

14. Раздел "квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам, прекратившие свое действие" содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- 4) дата прекращения действия квалифицированного сертификата;
- 5) основание прекращения действия квалифицированного сертификата.

15. Раздел "аннулированные квалифицированные сертификаты ключей проверки электронной подписи, выданные физическим лицам" содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
- 4) дата аннулирования квалифицированного сертификата;
- 5) основание аннулирования квалифицированного сертификата.

16. Раздел "аннулированные квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам" содержат следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- 4) дата аннулирования квалифицированного сертификата;
- 5) основание аннулирования квалифицированного сертификата.

5.10.2. Внесение сведений в реестр квалифицированных сертификатов

17. Сведения о прекращении действия квалифицированного сертификата вносятся удостоверяющим центром в реестр квалифицированных сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в части 6 статьи 14 Федерального закона N 63-ФЗ, или в течение двенадцати часов с момента, когда стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи в реестр

квалифицированных сертификатов.

18. Сведения об аннулировании квалифицированного сертификата вносятся в течение одного рабочего дня со дня вступления в законную силу решения суда, явившегося основанием для аннулирования, а также при аннулировании сертификатов ключей проверки электронной подписи по основаниям, указанным в пунктах 1 и 2 части 6.1 статьи 14 Федерального закона N 63-ФЗ. Квалифицированный сертификат считается аннулированным с момента внесения указанной записи в реестр квалифицированных сертификатов.

До внесения в реестр квалифицированных сертификатов сведений об аннулировании квалифицированного сертификата удостоверяющий центр уведомляет владельца квалифицированного сертификата об аннулировании его квалифицированного сертификата путем направления документа на бумажном носителе или электронного документа.

5.10.3. Предоставление сведений из реестра квалифицированных сертификатов

19. Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к реестру квалифицированных сертификатов в любое время в течение срока деятельности удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

20. Доступ заинтересованных лиц к реестру квалифицированных сертификатов с использованием информационно-телекоммуникационных сетей осуществляется путем размещения, формирования и ведения реестра квалифицированных сертификатов в информационной системе головного удостоверяющего центра, являющейся составной частью инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Доступ заинтересованных лиц к информационной системе головного удостоверяющего центра с целью получения сведений из реестра квалифицированных сертификатов осуществляется с использованием федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)" на безвозмездной основе.

21. Удостоверяющий центр обязан предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре квалифицированных сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи. Указанная информация предоставляется в форме выписки из реестра квалифицированных сертификатов и направляется обратившемуся лицу как почтовым отправлением, так и с использованием информационно-телекоммуникационных сетей (по выбору лица, обратившегося за получением информации из реестра квалифицированных сертификатов).

Срок предоставления информации не может превышать семи дней для направления информации почтовым отправлением и 24 часов для направления выписки посредством информационно-телекоммуникационных сетей.

5.11. Порядок технического обслуживания реестра квалифицированных сертификатов

Техническое обслуживание проводится планово в срок не более 12 часов 1 раз в 2 месяца в выходные дни.

О техническом обслуживании реестра квалифицированных сертификатов информация размещается на сайте удостоверяющего центра.

5.12. Порядок исполнения обязанностей Удостоверяющего центра

а) информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки проводится через предоставление Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

б) Выдача по обращению заявителя средств электронной подписи.

Средства электронной подписи должны в соответствии с частью 4 статьи 6 Федерального закона "Об электронной подписи" обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями;

в) обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

г) обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети "Интернет" в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов;

д) конфиденциальность созданных Удостоверяющим центром ключей электронных подписей обеспечивается выполнением регламентных процедур в соответствии с Руководством по безопасности ПАК «КриптоПро УЦ»;

е) по всем квалифицированным сертификатам в единую систему идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона "Об электронной подписи" передается необходимая информация

;

ж) по желанию лица, которому выдан квалифицированный сертификат, выполняется безвозмездная регистрация указанного лица в единой системе идентификации и аутентификации;

з) безвозмездно любому лицу предоставляется доступ к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов в сети Интернет:

http://ca.garant.ru/cdp/accredited/garant_ac3.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac3.crl

http://ca.garant.ru/cdp/accredited/garant_ac4.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac4.crl

http://ca.garant.ru/cdp/accredited/garant_ac5.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac5.crl

http://ca.garant.ru/cdp/accredited/garant_ac6.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac6.crl

http://ca.garant.ru/cdp/accredited/garant_ac7.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac7.crl

http://ca.garant.ru/cdp/accredited/garant_ac8.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac8.crl

http://ca.garant.ru/cdp/accredited/garant_ac9.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac9.crl

http://ca.garant.ru/cdp/accredited/garant_ac10.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac10.crl

http://ca.garant.ru/cdp/accredited/garant_ac11.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac11.crl

http://ca.garant.ru/cdp/accredited/garant_ac12.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac12.crl

http://ca.garant.ru/cdp/accredited/garant_ac13.crl

http://www.garantexpress.ru/cdp/accredited/garant_ac13.crl

5.13. Срок хранения сертификата ключа проверки ЭП

Хранение КСКПЭП пользователей УЦ в Реестре КСКПЭП УЦ, осуществляется в течение всего срока деятельности УЦ.

Срок архивного хранения сертификата ключа проверки ЭП устанавливается в соответствии со сроком, определённым разделом 6.6. настоящего Регламента.

5.14. Процедура предоставления КСКПЭП

Удостоверяющий центр предоставляет по запросу любого пользователя КСКПЭП в электронной форме, изготовленные Удостоверяющим центром. Запрос необходимо направлять по электронной почте на адрес uc@garant.ru. Запрос должен содержать ФИО и ИНН владельца КСКПЭП физического лица и название организации и ИНН владельца КСКПЭП юридического лица.

Удостоверяющий центр публикует в сети Интернет страницу поиска КСКПЭП, изготовленных Удостоверяющим центром: <https://www.garantexpress.ru/reestr/>

Поиск ведется по серийному номеру сертификата. Результатом поиска будет файл сертификата или информация, что сертификат с данным серийным номером не найден.

5.15. Механизм доказательства обладания ключом ЭП, соответствующим ключу проверки ЭП

Заявления на изготовление сертификата ключа проверки ЭП, поступающие в УЦ от владельцев ключей ЭП и ключей проверки ЭП, должны содержать собственноручную подпись заявителя и, в качестве реквизита документа, сам запрос на сертификат, в формате криптографических сообщений PKCS#10 Base-64.

Электронная подпись запроса на сертификат из заявления на изготовление сертификата ключа проверки ЭП и наличие собственноручной подписи заявителя подтверждают, что заявитель является владельцем ключа ЭП, соответствующего ключу проверки ЭП из заявления на изготовление сертификата ключа проверки ЭП (так как только владелец ключа ЭП может поставить такую электронную подпись).

5.16. Порядок проведения разбора конфликтной ситуации, связанной с применением электронной подписи в электронном документе

Настоящий раздел описывает порядок разбора конфликтной ситуации на основе работы согласительной комиссии, формируемой из числа участников информационной системы и сотрудников удостоверяющего центра, как третьей стороны, обеспечивающей подтверждение подлинности электронной подписи в электронных документах в отношении сертификатов ключей проверки электронной подписи, созданных удостоверяющим центром. Удостоверяющий центр в описанном случае является организатором работы согласительной комиссии.

В общем случае порядок разбора конфликтной ситуации устанавливается оператором информационной системы, либо соглашением между участниками информационной системы и может отличаться от приведенного.

Разрешение конфликтных ситуаций, возникающих в информационной системе и связанных с применением электронной подписи, осуществляется согласительной комиссией. Согласительная комиссия создается с целью разрешения конфликтных ситуаций при обмене (в связи с обменом) и применении электронных документов, подписанных электронной подписью.

Конфликтная ситуация может возникнуть между участниками информационной системы. При возникновении разногласий участник информационной системы (сторона-инициатор), обязан направить в удостоверяющий центр заявление о разногласиях, возникших при обмене (в связи с обменом) и применением электронных документов с другим участником информационной системы (сторона-ответчик), подписанное собственноручной подписью уполномоченного на данное действие лицом, с подробным изложением причин разногласий и предложением создать комиссию по ее разрешению.

По заявлению о разногласиях удостоверяющий центр формирует согласительную комиссию, в которую входят:

- Представитель удостоверяющего центра - председатель комиссии.
- Пользователь информационной системы - представитель участника информационной системы (сторона-инициатор), который непосредственно участвовал в информационном обмене электронными документами, по которым возникли разногласия;
- Пользователь информационной системы - представитель участника

информационной системы (сторона-ответчик), который непосредственно участвовал в информационном обмене электронными документами, по которым возникли разногласия.

Комиссия осуществляет свою деятельность по месторасположению удостоверяющего центра. Язык работы согласительной комиссии - русский.

Сторона-инициатор представляет заявление о разногласии (уведомление о возникших разногласиях) с указанием:

- даты подачи заявления (уведомления);
- информации, идентифицирующей инициатора и ответчика;
- обстоятельств, на которых основаны заявленные требования;
- обоснованного расчета заявленных требований;
- нормы законодательных и иных нормативных правовых актов, на основании которых заявляется требование;
- прилагаемые к заявлению (уведомлению) о разногласии документы, составляющие доказательную базу.

До начала работы согласительной комиссии стороне - инициатору рекомендуется убедиться в целостности установленных на его технических средствах программного обеспечения, в том числе средства электронной подписи, а также отсутствии несанкционированных действий со стороны третьих лиц.

Сторона-ответчик обязана в период работы комиссии представить стороне-инициатору и комиссии возражения по каждому требованию, изложенному в заявлении о разногласиях, либо согласиться с предъявляемыми требованиями.

В возражениях ответчика на каждое требование должны содержаться документально обоснованные ответы или сделана ссылка на доказательства, которые могут быть представлены в ходе работы комиссии.

Любая сторона в ходе работы комиссии может внести ходатайства об изменении или дополнении своих требований или возражений.

Комиссия в ходе разбирательства в любой момент может затребовать от сторон предоставления документов, вещественных или иных доказательств в устанавливаемый комиссией срок.

Рассмотрение конфликтной ситуации производится на основании всех представленных документов, доказательств.

В том случае, если обстоятельства, имеющие значение для принятия решения по делу, могут быть исследованы только на основе применения специальных научных знаний, комиссия вправе назначить экспертизу по подтверждению подлинности электронной подписи в электронном документе.

Проведение экспертизы возлагается на удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, с использованием которого была сформирована электронная подпись электронного документа, являющегося предметом разногласий. Запрос на проведение экспертизы оформляется заявлением на подтверждение подлинности электронной подписи в электронном документе, подающемся в удостоверяющий центр от лица участника информационной системы - владельца сертификата ключа проверки электронной подписи. Порядок проведения экспертных работ Удостоверяющим центром по подтверждению подлинности электронной подписи в электронном документе устанавливается Удостоверяющим центром. Для проведения удостоверяющим центром указанных работ электронные документы и их электронная подпись экспортируются из информационной системы в соответствующие файлы и предоставляются вместе с заявлением на подтверждение подлинности электронной подписи в удостоверяющий центр. Результатом проведения экспертных работ

удостоверяющего центра является заключение удостоверяющего центра.

Экспертиза может быть назначена комиссией по обоснованному ходатайству любой из сторон или по ее собственной инициативе.

По итогам работы согласительной комиссии составляется акт, в котором содержится краткое изложение выводов комиссии и решение комиссии по рассматриваемому разногласию.

Помимо изложения выводов согласительной комиссии и решения комиссии акт должен содержать следующие данные:

- состав комиссии;
- дату и место составления акта;
- дату и время начала и окончания работы комиссии;
- краткий перечень мероприятий, проведенных комиссией;
- выводы комиссии;
- собственноручные подписи членов комиссии;
- указание на особое мнение члена (или членов комиссии), в случае наличия такового.

Акт составляется в 3-х экземплярах и предоставляется по одному экземпляру для каждой из сторон конфликтной ситуации, а также удостоверяющему центру.

6. Дополнительные положения

6.1. Идентифицирующие данные Уполномоченного лица УЦ

Каждое Уполномоченное лицо УЦ идентифицируется следующими данными:

- Фамилия, имя, отчество:
- Организация:
- Подразделение:
- Адрес электронной почты:
- Субъект Федерации:

6.2. Требования к средствам электронной подписи, используемым в составе Удостоверяющего центра и требования к средствам электронной подписи пользователей УЦ

Средства электронной подписи аккредитованного Удостоверяющего центра и средства электронной подписи пользователя Удостоверяющего центра должны удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. №796.

Формирование и проверка электронной подписи на серверных компонентах Удостоверяющего центра, а именно на Центре сертификации и Центре регистрации (или Центрах Регистрации, если таковых в Удостоверяющем центре более одного) осуществляется Администратором УЦ или в автоматическом режиме, под контролем лица, ответственного за создание и проверку ЭП в ЦС.

На Автоматизированном рабочем месте Администратора Центра регистрации выполнение операции создания электронной подписи под запросами на регистрацию, запросами на сертификат, запросами на управление статусом сертификата осуществляется только после того, как привилегированный пользователь (Администратор, Оператор,

Администратора Аудита) ознакомится с содержимым подписываемого документа. После ознакомления - привилегированный пользователь подтверждает создание электронной подписи. Выполнение операции создания электронной подписи заканчивается уведомлением о выполнении операции, связанной с созданием электронной подписи (положительный результат свидетельствует об успешном создании ЭП, отрицательный - ЭП не создана).

На Автоматизированных рабочих местах Администратора Центра регистрации и разбора конфликтных ситуаций выполнение операции проверки электронной подписи сопровождается ознакомлением с электронным документом, информированием о внесении изменений в электронный документ (при изменении электронного документа появляется сообщение - электронная подпись - «Не верна»), отображением сертификата ключа проверки ЭП подписчика данного электронного документа.

6.3. Сроки действия ключей ЭП и квалифицированных сертификатов ключей проверки ЭП пользователей УЦ

Максимальный срок действия ключа ЭП Пользователя УЦ, соответствующего квалифицированному сертификату ключа проверки ЭП, владельцем которого он является, определяется требованиями средства криптографической защиты информации, с помощью которого сформирован и используется данный ключ ЭП.

Начало периода действия ключа ЭП Пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП Пользователя УЦ.

Срок действия ключа проверки ЭП устанавливается равным сроку действия сертификата ключа проверки ЭП.

Максимальный срок действия сертификата ключа проверки ЭП Пользователя УЦ определяется требованиями средства криптографической защиты информации, использующим ключ ЭП пользователя, соответствующий указанному сертификату.

Для УЦ ООО «Электронный экспресс» установлены следующие максимальные сроки действия ключей ЭП и ключей проверки ЭП Пользователей УЦ.

Начало периода действия ключа электронной подписи Пользователя УЦ - владельца КСКПЭП исчисляется с даты и времени начала действия соответствующего КСКПЭП.

При формировании КСКЭП не допускается в качестве даты начала действия сертификата указывать дату отличную от даты момента формирования КСКПЭП.

Срок действия КСКПЭП Пользователя УЦ составляет 1 (один) год.

6.4. Меры защиты ключей ЭП

Ключи ЭП пользователей УЦ должны записываться при их генерации на типы ключевых носителей, которые поддерживаются используемым средством криптографической защиты информации.

Ключи ЭП на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство криптографической защиты информации.

Если процедуру генерации ключей Пользователя УЦ выполняет сотрудник УЦ, то он должен сообщить сформированный пароль (ПИН-код) владельцу ключей ЭП.

Ответственность за сохранение пароля (ПИН-кода) в тайне возлагается на владельца ключей ЭП.

Сотрудники УЦ, являющиеся владельцами ключей ЭП, также выполняют указанные в разделе меры защиты ключей ЭП.

6.5. Информация из квалифицированного сертификата ключа проверки ЭП на бумажном носителе или в электронном виде

При получении КСКПЭП заявителем он должен быть под расписку ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в КСКПЭП.

Оператор обязан осуществить проверку соответствия сертификата ключа проверки электронной подписи в электронном виде или в распечатанной копии этого сертификата. Только после успешного проведения указанной проверки сведения предоставляются на подпись владельцу сертификата.

При оформлении данной расписки в бумажной или в электронной форме указанная информация должна включать сведения, установленные Статьей 17 Федерального закона №63-ФЗ «Об электронной подписи».

6.6. Архивное хранение документированной информации

6.6.1. Хранение сертификатов ключей электронной подписи в электронном виде.

Хранение КСКПЭП Пользователей УЦ в электронном виде в Удостоверяющем центре осуществляется в течение всего срока его деятельности

6.6.2. Состав архивируемых документов

Архивное хранение всех документов осуществляет Общество.

Перечень документов Центра Регистрации, подлежащих отправке в Общество и архивному хранению в Обществе:

- заявления Клиентов на регистрацию и изготовление КСКПЭП и согласие на обработку персональных данных;
- копии документов, удостоверяющих личность;
- копии СНИЛС;
- копии ОГРН, ОГРНИП (при предоставлении);
- копии документов на бумажном носителе с собственноручной подписью Пользователя УЦ, содержащие информацию из КСКПЭП;
- заявления на аннулирование (отзыв) КСКПЭП;
- заявления на проверку электронной подписи Удостоверяющего центра в КСКПЭП Пользователя УЦ.
- заявления на проверку электронной подписи в документах;
- .

6.6.3. Источник комплектования архивного фонда

Источником комплектования архивного фонда УЦ являются подразделения (Службы) УЦ, обеспечивающие документирование.

6.6.4. Архивохранилище

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

6.6.5. Срок архивного хранения

Документы, подлежащие архивному хранению, являются документами временного хранения. Срок хранения бумажных архивных документов – 5 лет после окончания срока действия КСКПЭП Пользователя УЦ.

6.6.6. Уничтожение архивных документов

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Службы безопасности УЦ и назначаемой приказом руководителя УЦ.

7. Структуры сертификатов и списков отозванных сертификатов

7.1. Структура квалифицированного сертификата

Квалифицированный сертификат ключа проверки электронной подписи в электронной форме создается в формате X.509 версии 3, структура квалифицированного сертификата ключа проверки ЭП должна удовлетворять требованиям Федерального закона №63-ФЗ «Об электронной подписи» (с учетом изменений, вносимых Федеральным законом №445-ФЗ) и Приказа ФСБ России от 27.12.2011 г. №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Структура квалифицированного сертификата ключа проверки электронной подписи:

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer	УЦ - Издатель сертификата	Согласно Таблицы заполнения поля Субъект (для ЮЛ, авторматическое создание/проверка ЭП)
Validity Period	Срок действия сертификата	Действителен с (not Before): дд.мм.гггг чч:мм:сс UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	Согласно Таблицы заполнения поля Субъект
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Issuer Signature	ЭП УЦ – издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001 или ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
Authority Key Identifier	Идентификатор ключа УЦ - издателя сертификата	Идентификатор ключа подписи Удостоверяющего центра, на котором подписан данный сертификат; УЦ - издатель сертификата, заполняется Согласно Таблицы заполнения поля Субъект (для ЮЛ,

		автоматическое создание/проверка ЭП); Серийный номер сертификата УЦ
Key Usage (critical)	Область использования ключа	Набор областей использования ключа (реализуется установкой соответствующих битов в значение «1»).
Certificate Policies	Политика сертификации	Идентификатор политики - класс средства ЭП Например: Для средства ЭП класса КС1: [1] Политика сертификата Идентификатор политики = Класс средства ЭП КС1 Для средства ЭП класса КС2: [1] Политика сертификата Идентификатор политики = Класс средства ЭП КС1 [2] Политика сертификата Идентификатор политики = Класс средства ЭП КС2 Для средства ЭП класса КС3: [1] Политика сертификата Идентификатор политики = Класс средства ЭП КС1 [2] Политика сертификата
		Идентификатор политики = Класс средства ЭП КС2 [3] Политика сертификата Идентификатор политики = Класс средства ЭП КС3
Subject Sign Tool	Средство ЭП владельца сертификата	Наименование средства ЭП владельца сертификата Например: КриптоПро CSP
Issuer Sign Tool	Средство ЭП и средство УЦ, используемые для создания сертификатов	Наименование средства ЭП и средства УЦ, а также реквизитов документа, подтверждающего соответствие указанных средств требованиям, установленным законодательством РФ (в случае отсутствия действующего сертификата соответствия на средство ЭП или средство УЦ допускается указывать номер положительного заключения) Например: Средство электронной подписи: "СКЗИ "КриптоПро CSP" версии 3.9, вариант исполнения 2 Заключение на средство ЭП: Сертификат соответствия № СФ/____ - ____ от ____ . ____ . ____ г." Средство УЦ: "ПАК "КриптоПро УЦ" версии 2.0, вариант исполнения 1 Заключение на средство УЦ: Сертификат соответствия № СФ/____ - ____ от ____ . ____ . ____ г."
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа подписи владельца сертификата
Extended Key Usage (необязательное дополнение)	Расширенная область использования ключа	Набор расширенных областей использования ключа - объектных идентификаторов
CRL Distribution Point (необязательное дополнение)	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL= http://ResourceServer/Path/Name.crl , где ResourceServer - имя сервера, Path - путь к файлу списка отозванных сертификатов, Name - наименование файла списка отозванных сертификатов

Authority Information Access (необязательное дополнение)	Адрес Службы актуальных статусов сертификатов, Адрес размещения информации о сертификате УЦ	URL адреса Службы актуальных статусов сертификатов. Заносится в сертификаты, статус которых может быть установлен по протоколу OCSP URL адреса размещения файла сертификата УЦ
Private Key Period (необязательное дополнение)	Период использования ключа подписи	Действителен с (not Before): дд.мм.гггг чч:мм:сс UTC Действителен по (not After): дд.мм.гггг чч:мм:сс UTC
		В сертификат могут быть добавлены дополнительные поля и дополнения согласно RFC 5280

Таблица заполнения поля Субъект квалифицированного сертификата ключа проверки электронной подписи

Физическое лицо	Физическое лицо индивидуальный предприниматель	Юридическое лицо с информа- цией о представителе (россий- ское юрлицо)	Юридическое лицо без ин- формации о представителе (автоматическое создание и/или проверка ЭП) (российское юрлицо)	Юридическое лицо с инфор- мацией о представителе (иностранное юрлицо)	Юридическое лицо без ин- формации о представителе (автоматическое создание и/или проверка ЭП) (иностранное юрлицо)
commonName (общее имя) - ФИО	commonName (общее имя) - ФИО	commonName (общее имя) - полное или сокращенное наименование юридического лица в соответствии с учреди- тельными документами	commonName (общее имя) - полное или сокращенное наименование юридического лица в соответствии с учре- дительными документами	commonName (общее имя) - полное или сокращенное наименование юридического лица в соответствии с учре- дительными документами	commonName (общее имя) - полное или сокращенное наименование юридического лица в соответствии с учре- дительными документами
surname (фамилия) - фамилия	surname (фамилия) - фамилия	surname (фамилия) - фамилия представителя		surname (фамилия) - фами- лия представителя	
givenName (приобре- тенное имя) - имя и отчество	givenName (приобре- тенное имя) - имя и отчество	givenName (приобретенное имя) - имя и отчество представителя		givenName (приобретенное имя) - имя и отчество пред- ставителя	
countryName (наиме- нование страны) двухсимвольный код	countryName (наиме- нование страны) двухсимвольный код	countryName (наименование страны) - двухсимвольный код - RU	countryName (наименование страны) - двухсимвольный код - RU	countryName (наименование страны) - двухсимвольный код	countryName (наименование страны) - двухсимвольный код
stateOrProvinceName (наименование штата или области) - наиме- нование субъекта РФ	stateOrProvinceName (наименование штата или области) - наиме- нование субъекта РФ	stateOrProvinceName (наимено- вание штата или области) - наименование субъекта РФ	stateOrProvinceName (наименование штата или области) - наименование субъекта РФ		

localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)	localityName (наименование населенного пункта)
streetAddress (название улицы, номер дома) - опционально	streetAddress (название улицы, номер дома) - опционально	streetAddress (название улицы, номер дома)	streetAddress (название улицы, номер дома)	streetAddress (название улицы, номер дома)	streetAddress (название улицы, номер дома)
		organizationName (наименование организации)	organizationName (наименование организации)	organizationName (наименование организации)	organizationName (наименование организации)
		organizationUnitName (подразделение)	organizationUnitName (подразделение) - опционально	organizationUnitName (подразделение)	organizationUnitName (подразделение) - опционально
		title (должность) - должность представителя		title (должность) - должность представителя	
E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально	E-mail (адрес электронной почты) - опционально
		OGRN (ОГРН)	OGRN (ОГРН)		
SNILS (СНИЛС)	SNILS (СНИЛС)	SNILS (СНИЛС) - представителя			
INN (ИНН)	INN (ИНН)	INN (ИНН) - юридического лица	INN (ИНН) - юридического лица	INN (ИНН) - юридического лица	INN (ИНН) - юридического лица
	OGRNIP (ОГРНИП)				

Структура квалифицированного сертификата ключа проверки электронной подписи Удостоверяющего центра ООО «Электронный экспресс» приведена в Приложении № 9

Структуры квалифицированного сертификата ключа проверки электронной подписи Пользователя УЦ - юридического лица и Пользователя УЦ - физического лица приведены в Приложении № 10 и в Приложении № 11 .

7.2. Структура списка отозванных сертификатов, изготавливаемого УЦ в электронной форме

УЦ изготавливает списки отозванных сертификатов ключей проверки ЭП пользователей УЦ и Уполномоченного лица УЦ в электронной форме (далее по тексту раздела — СОС) формата X.509 версии 2.

7.2.1. Расширения списка отозванных сертификатов.

При изготовлении списка отозванных сертификатов УЦ использует следующие расширения:

- Расширение «Authority Key Identifier» содержит идентификатор ключа Уполномоченного лица УЦ;
- Расширение «Reason Code» содержит код причины отзыва сертификата ключа проверки ЭП;
- Расширение «Microsoft CA Version» содержит номер сертификата службы сертификатов.

Структура Списка отозванных сертификатов приведена в Приложении №12.

8. Программные и технические средства обеспечения деятельности УЦ

Для реализации своих услуг и обеспечения жизнедеятельности УЦ использует следующие программные и технические средства:

- Программный комплекс обеспечения реализации целевых функций УЦ (ЖТЯИ.00078-01 99 01), далее по тексту — ПК УЦ;
- Технические средства обеспечения работы ПК УЦ, далее по тексту — ТС УЦ;
- Программные и программно-аппаратные средства защиты информации, далее по тексту - СЗИ УЦ.

8.1. Программный комплекс обеспечения реализации целевых функций УЦ

Каждый логический компонент «КриптоПро УЦ» должен оснащаться необходимым набором программных компонент «КриптоПро УЦ», которые поставляются в виде единого пакета установки «КриптоПро УЦ. Комплекс программ» (ЖТЯИ.00078-01 99 01).

Пакет установки «КриптоПро УЦ» устанавливает следующие программы:

- Программный компонент УЦ «Диспетчер УЦ»
- Роль УЦ «Сервер центров сертификации»
- Роль УЦ «Сервер центров регистрации»
- Роль УЦ «Сервер CDP»
- Программный компонент УЦ «Консоль управления ЦР»
- Программный компонент УЦ «Консоль экспертизы ЭП»

Роль УЦ — это набор программ, которые при правильной установке и настройке позволяют компьютеру выполнять определённую функцию УЦ. Роли УЦ определяют основную функцию, назначение или цель использования компьютера. Можно назначить компьютер для выполнения одной роли, которая интенсивно используется в УЦ, или для выполнения нескольких ролей, если каждая из них применяется лишь изредка.

Логические компоненты УЦ могут разворачиваться не только на серверных, но и на

клиентских операционных системах (в отличие от Windows, где «Диспетчер сервера» доступен только на серверных операционных системах и все Роли могут быть добавлены только на серверах).

Роли УЦ позволяют настроить сервер или рабочую станцию в качестве одной или нескольких логических структурных элементов УЦ. Они обычно имеют собственные базы данных, в которых создаются очереди запросов. После правильной установки и настройки Роли УЦ функционируют автоматически. Это позволяет компьютерам, на которых они установлены, выполнять назначенные задачи при ограниченном участии пользователя.

Набор программных компонент «КриптоПро УЦ», которые необходимо установить на компьютерной системе для разворачивания на ней определённого логического структурного компонента, приведён в таблице ниже.

Таблица 4. Программные компоненты УЦ, требуемые для разворачивания логических структурных компонент УЦ

Логический компонент УЦ	Требуемые программные компоненты «КриптоПро УЦ»
Центр сертификации	Программный компонент УЦ «Диспетчер УЦ», Роль УЦ «Сервер центров сертификации»
Центр регистрации	Программный компонент УЦ «Диспетчер УЦ», Роль УЦ «Сервер центров регистрации»
АРМ обслуживающего персонала	Программный компонент УЦ «Консоль управления ЦР»
АРМ разбора конфликтных ситуаций	Программный компонент УЦ «Консоль экспертизы ЭП»
АРМ пользователя	Специальные программные компоненты «КриптоПро УЦ» не требуются

Центр сертификации является логическим компонентом УЦ и предназначен для обеспечения реализации следующих целевых функций УЦ:

- Формирования КСКПЭП пользователей УЦ в электронной форме с использованием ключа ЭП и квалифицированного сертификата ключа проверки ЭП Уполномоченного лица УЦ;
- Формирования списков отозванных сертификатов ключей проверки ЭП пользователей УЦ в электронной форме с использованием ключей ЭП и к КСКПЭП Уполномоченных лиц УЦ на основе эталонной копии списка отозванных сертификатов ключей проверки ЭП пользователей УЦ;
- Ведения эталонной копии Реестра сертификатов ключей проверки ЭП УЦ;
- Ведения эталонной копии списка отозванных сертификатов ключей проверки ЭП пользователей УЦ;
- Обеспечения уникальности ключей проверки ЭП в изданных с КСКПЭП пользователей УЦ.

Ответственность за эксплуатацию Центра сертификации возлагается на Уполномоченных лиц УЦ.

Центр регистрации является логическим компонентом УЦ и предназначен для обеспечения реализации следующих целевых функций УЦ:

- Ведения Реестра зарегистрированных пользователей УЦ;
- Ведения Реестра КСКПЭП УЦ;
- Ведения Реестра заявлений на изготовление КСКПЭП пользователей УЦ в электронной форме;
- Ведения Реестра заявлений на аннулирование (отзыв) КСКПЭП пользователей УЦ в

- электронной форме;
- Ведения Реестра запросов на регистрацию пользователей УЦ в электронной форме;
- Предоставления программных средств для незарегистрированных пользователей УЦ для обеспечения реализации их права передать по сети в УЦ запрос на регистрацию в электронной форме;
- Предоставления программных средств для зарегистрированных пользователей УЦ для обеспечения реализации их прав в части пользования предоставляемыми программными средствами.

Ответственность за эксплуатацию Центра регистрации возлагается на Службу регистрации УЦ.

АРМ обслуживающего персонала ЦР предназначен для обеспечения реализации своих функциональных обязанностей сотрудникам Службы регистрации и Службы безопасности УЦ.

АРМ разбора конфликтных ситуаций предназначен для обеспечения своих функциональных обязанностей сотрудникам Административной службы УЦ в части взаимодействия с пользователями УЦ при разрешении вопросов, связанных с подтверждением электронной подписи Уполномоченного лица УЦ в КСКПЭП, изготовленных УЦ в электронной форме.

8.2. Технические средства обеспечения работы ПКУЦ

Технические средства обеспечения работы ПКУЦ включают в себя:

- Выделенный сервер Центра сертификации;
- Выделенный сервер Центра регистрации;
- Телекоммуникационное оборудование;
- Компьютеры рабочих мест сотрудников Служб УЦ;
- Устройства печати на бумажных носителях (принтеры).

Ответственность за эксплуатацию технических средств и общесистемного программного обеспечения возлагается на Техническую службу УЦ.

8.3. Программные и программно-аппаратные средства защиты информации

Программные и программно-аппаратные средства защиты информации включают в себя:

- Средства криптографической защиты информации;
- Межсетевой экран для обеспечения защиты информации при сетевом взаимодействии с Центром регистрации;
- Программно-аппаратные комплексы защиты от несанкционированного доступа типа «электронный замок»;
- Устройства для обеспечения бесперебойного питания серверов Центра сертификации и Центра регистрации;
- Устройства обеспечения температурно-влажностного режима и кондиционирования служебных и рабочих помещений УЦ;
- Устройства обеспечения противопожарной безопасности помещений УЦ.

На компонентах УЦ должны использоваться средства криптографической защиты информации (средства электронной подписи), входящие в состав комплектации «КриптоПро УЦ».

Ответственность за эксплуатацию программных и программно-аппаратных средств защиты информации возлагается на Техническую службу УЦ.

8.4. Перечень событий, регистрируемых программным комплексом обеспечения реализации целевых функций УЦ

Основные типы событий, регистрируемые программными компонентами УЦ:

- Центром Сертификации:
 - Поступление запроса на сертификат;
 - Издание сертификата;
 - Издан СОС;
 - Невыполнение внутренней операции программной компоненты;
 - Системные события общесистемного программного обеспечения.
- Центром Регистрации:
 - Помещен запрос на регистрацию;
 - Принят запрос на регистрацию;
 - Отклонен запрос на регистрацию;
 - Помещен запрос на сертификат;
 - Принят запрос на сертификат;
 - Отклонен запрос на сертификат;
 - Установка сертификата подтверждена пользователем;
 - Помещен запрос на отзыв сертификата;
 - Принят запрос на отзыв сертификата;
 - Отклонен запрос на отзыв сертификата;
 - Помещен запрос на первый сертификат;
 - Запрошен список отозванных сертификатов;
 - Опубликован список отозванных сертификатов;
 - Невыполнение внутренней операции программной компоненты;
 - Установлено сетевое соединение с внешней программной компонентой;
 - Системные события общесистемного программного обеспечения.
 - Структуры записей событий приведены в эксплуатационной документации ПКУЦ и общесистемного программного обеспечения.
 -

8.5. Перечень данных программного комплекса обеспечения реализации целевых функций УЦ, подлежащих резервному копированию

При эксплуатации программного комплекса обеспечения реализации целевых функций УЦ ежедневно выполняется резервное копирование данных компонент ПК УЦ.

Перечень данных ПК УЦ, подлежащих резервному копированию, включает в себя:

- Базу данных Службы сертификатов ПК УЦ, включающую журнал выданных сертификатов, очередь запросов, сертификаты ключей проверки ЭП Уполномоченных лиц УЦ;
- Базу данных Службы регистрации ПК УЦ;
- Журналы аудита компонент ПК УЦ в составе, определённом эксплуатационной документацией ПКУЦ.

8.6. Порядок технического обслуживания средств обеспечения деятельности УЦ

Порядок технического обслуживания средств обеспечения деятельности удостоверяющего центра, построенного на базе программно-аппаратного комплекса

«Удостоверяющий Центр «КриптоПро УЦ» содержит описание и правила выполнения работ по техническому обслуживанию средств удостоверяющего центра.

Техническое обслуживание средств обеспечения деятельности удостоверяющего центра направлено на обеспечение постоянной готовности указанных средств к использованию по прямому назначению и предотвращению выхода их из строя.

Техническое обслуживание средств обеспечения деятельности удостоверяющего центра включает:

- техническое обслуживание вычислительной техники и периферийного оборудования;
- техническое обслуживание общесистемного и специализированного программного обеспечения.

8.6.1. Техническое обслуживание вычислительной техники и периферийного оборудования

К средствам вычислительной техники и периферийному оборудованию удостоверяющего

центра относятся

- Сервер Центра сертификации;
- Сервер Центра регистрации;
- Автоматизированные рабочие места привилегированных пользователей Удостоверяющего центра (администраторов и операторов удостоверяющего центра);
- Автоматизированное рабочее место разбора конфликтных ситуаций;
- Межсетевой экран;
- Программно-аппаратный криптографический модуль (ПАКМ) «КриптоПро HSM» (может отсутствовать в случае использования на Центре сертификации СКЗИ «КриптоПро CSP»);
- Источник бесперебойного питания (может отсутствовать в случае использования в эксплуатирующей организации единой централизованной системы бесперебойного питания);
- Сетевое и коммутационное оборудование.

Все виды работ по техническому обслуживанию вычислительной техники и периферийного оборудования проводятся по установленному графику, вне зависимости от технического состояния изделия. Уменьшать установленный объем и изменять периодичность технического обслуживания не рекомендуется.

Для поддержания работоспособности удостоверяющего центра необходимо производить периодические осмотры входящего в него оборудования.

Техническое обслуживание вычислительной техники и периферийного оборудования должно включать в себя следующие виды работ:

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
1.	Проверка внешнего вида корпусов оборудования, сетевого и соединительного шнуров на	Ежедневно	Проводится визуально	Допускается проводить внешний осмотр оборудования без выключения напряжения питания. Эксплуатация оборудования с

	отсутствие повреждений			повреждениями категорически запрещается.
2.	Проверка работоспособности	Ежедневно	Проверяется исправность оборудования посредством выполнения штатных задач, запускаемых в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3.	Проверка пломбировки, маркировки, целостности корпусов оборудования	Ежедневно	Проводится визуально	При нарушении пломбировки, маркировки, целостности корпуса оборудования дальнейшая эксплуатация изделия запрещена до установления причин нарушения пломбировки, маркировки, целостности корпуса
4.	Очистка от пыли и грязи	Один раз в месяц	Отключить изделие от сети переменного тока. Удалить с поверхности изделия пыль, грязь и влагу. Для очистки изделия от пыли и грязи допускается использование мягкой ветоши (легкая безворсовая ткань, например, марля хлопчатобумажная ГОСТ 11109 - 74) и неагрессивных моющих растворов.	Очистку выполнять путем последовательной протирки поверхностей: 1) влажной салфеткой, смоченной в 5 % растворе бытовых моющих средств; 2) влажной салфеткой, смоченной в чистой воде; 3) сухой салфеткой. При протирке не допускать попадания влаги на разъемные соединения и токоведущие цепи
5.	Контрольная проверка работоспособности оборудования	Один раз в год	Проверку оборудования необходимо выполнять путем прогона контрольной задачи	Контрольная проверка оборудования необязательна в случае его устойчивой работоспособности по назначению
6.	Текущий ремонт	По мере необходимости	Оборудование может быть отремонтировано у эксплуатирующей организации. В случае выхода из строя подлежит	

			замене или ремонту в условиях предприятия-изготовителя.	
7.	Дополнительные работы	Согласно руководства по эксплуатации на конкретное оборудование	В том случае, если требованиями эксплуатационной документации на конкретное оборудование предусмотрено обязательное выполнение определенных работ по его техническому обслуживанию, то данные работы должны быть включены в указанный перечень проводимых работ	

Оборудование рекомендуется периодически (один раз в год) подвергать техническому осмотру с участием специалистов предприятия-изготовителя или специалистов рекомендуемого предприятием-изготовителем сервисного центра.

По истечении срока гарантии оборудования рекомендуется заключение с предприятием-изготовителем или соответствующим сервисным центром договора на техническое обслуживание оборудования.

Запрещается осуществлять самовольную регулировку, ремонт, переустановку или вносить какие-либо изменения в конструкцию оборудования.

Техническое обслуживание оборудования, входящего в состав удостоверяющего центра, производится в соответствии с инструкциями по эксплуатации каждого аппарата в него входящего.

Все неисправности оборудования, обнаруженные при периодических осмотрах, должны устраняться по мере их выявления и регистрироваться в соответствующем журнале.

8.6.2. Техническое обслуживание общесистемного и специализированного программного обеспечения

Общесистемное программное обеспечение включает в себя структурные компоненты операционной системы, средства управления базами данных, а также стандартные средства администрирования операционной системы.

К специализированному программному обеспечению относятся:

- Средства криптографической защиты информации (СКЗИ «КриптоПро CSP», ПАКМ «КриптоПро HSM»);
- Средства обеспечения деятельности удостоверяющего центра (ПАК «Удостоверяющий центр «КриптоПро УЦ»);
- Антивирусные средства;
- Средства резервного хранения данных.

Техническое обслуживание общесистемного программного обеспечения включает в себя выполнение следующих видов работ:

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5

1.	Проверка целостности загрузочных секторов диска и общесистемных файлов	При включении серверов Центра сертификации, Центра регистрации, АРМ привилегированных пользователей, АРМ разбора конфликтных ситуаций, ПАКМ «КриптоПро HSM»	Проводится средствами аппаратно-программного модуля доверенной загрузки типа «Электронный замок» до загрузки операционной системы	
2.	Проверка работоспособности операционной системы	Ежедневно	Проверяется исправность системы посредством выполнения общесистемных задач, запускаемых в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3.	Проверка на наличие вирусов	Ежедневно	Осуществляется с использованием специализированных средств антивирусного контроля. Рекомендуется использовать в автоматическом режиме	
4.	Обновление операционной системы	По мере выхода критических обновлений операционной системы	Осуществляется с использованием стандартных средств администрирования операционной системы (Windows Update)	
5.	Создание резервного образа диска	Один раз в неделю	Осуществляется с использованием специализированных средств резервного хранения данных	
6.	Проверка наличия свободного дискового пространства на системном диске и удаление ненужных файлов	Один раз в месяц	Проводится с использованием стандартных средств администрирования операционной системы	
7.	Проверка состояния файловой системы	Один раз в три месяца	Проводится с использованием стандартных средств администрирования операционной системы	
8.	Восстановление работоспособности операционной системы	По мере необходимости	Осуществляется посредством восстановления или переустановки операционной	

			системы, а также восстановления образа всего диска	
--	--	--	--	--

Техническое обслуживание специализированного программного обеспечения включает в себя выполнение следующих видов работ:

№ п/п	Наименование работы	Периодичность выполнения работы	Порядок проведения	Примечание
1	2	3	4	5
1	Проверка целостности программных модулей СКЗИ и ПАК «КриптоПро УЦ»	При включении серверов Центра сертификации, Центра регистрации, АРМ привилегированных пользователей, АРМ разбора конфликтных ситуаций, ПАКМ «КриптоПро НСМ»	Проводится средствами аппаратно-программного модуля доверенной загрузки типа «Электронный замок» до загрузки операционной системы	
2	Проверка работоспособности СКЗИ и ПАК «КриптоПро УЦ»	Ежедневно	Проверяется исправность средств в связи с основной деятельностью удостоверяющего центра (по назначению)	Проводится с учётом местных условий эксплуатации
3	Обновление антивирусных баз	Ежедневно	Осуществляется с использованием специализированных средств антивирусного контроля. Рекомендуется использовать в автоматическом режиме	
4	Создание резервных копий баз данных удостоверяющего центра	Ежедневно	Осуществляется с использованием специализированных средств резервного хранения данных. Рекомендуется выполнять в автоматическом режиме	
5	Создание резервного образа диска	Один раз в неделю	Осуществляется с использованием специализированных средств резервного хранения данных	
6	Контрольная проверка работоспособности СКЗИ «КриптоПро CSP» и ПАК «КриптоПро УЦ»	Один раз в 6 месяцев	Проверку работоспособности средств обеспечения деятельности удостоверяющего центра необходимо выполнять путем выполнения	

			тестовых задач, связанных с основной деятельностью удостоверяющего центра.	
7	Восстановление работоспособности удостоверяющего центра	По мере необходимости	Осуществляется посредством восстановления или переустановки программных компонент удостоверяющего центра, а также восстановления образа всего диска	

В части технического обслуживания средств криптографической защиты информации и средств обеспечения деятельности удостоверяющего центра рекомендуется заключение соответствующего договора с организацией разработчиком указанных средств, либо с организацией - лицензиатом ФСБ России, имеющей соответствующую лицензию на техническое обслуживание шифровальных (криптографических) средств. Помимо этого, сотрудники указанной организации, которых планируются привлечь к проведению данных работ, должны иметь документ (сертификат), подтверждающий прохождение обучения сотрудника на специализированных курсах.

В указанный договор рекомендуется включать следующие обязательства Исполнителя по выполнению услуг по техническому обслуживанию и сопровождению деятельности удостоверяющего центра:

№	Уровень	Наименование услуги
		Описание
1.	формализованный	Консультации по выбору конфигурации оборудования и общесистемного программного обеспечения серверов УЦ
2.	не формализованный	Консультации по установке компонент УЦ
3.	не формализованный	Консультации по администрированию компонент УЦ
4.	формализованный	Восстановление комплекта поставки УЦ (в случае его разрушения)
5.	не формализованный	Консультация по переносу информационных баз данных компонент УЦ
6.	формализованный	Консультация по организации резервного копирования баз данных компонент УЦ
7.	не формализованный	Консультация по восстановлению поврежденных баз данных компонент УЦ с резервных копий
8.	не формализованный	Консультации по восстановлению работоспособности компонент УЦ (в случае ее потери)
9.	не формализованный	Дистанционное выполнение работ по восстановлению работоспособности компонент УЦ (в случае ее потери)
10.	формализованный	Информирование о появлении новых сборок версии УЦ, находящейся в эксплуатации у Заказчика
11.	формализованный	Информирование о появлении новых версий УЦ
12.	формализованный	Предоставление новых сборок версии УЦ, находящейся в эксплуатации у Заказчика
13.	не формализованный	Консультирование по обновлению сборок версии УЦ, находящейся в эксплуатации у Заказчика

9. Роли обслуживающего персонала средств обеспечения деятельности УЦ

Удостоверяющий Центр осуществляет разделение ролей обслуживающего персонала

средств обеспечения деятельности УЦ. Каждая роль имеет свой набор задач, возможность осуществления которых задаётся параметрами безопасности, сопоставленными данной роли.

Перечень и описание обязанностей ролей, выполняемых обслуживающим персоналом УЦ на сервере ЦС и на сервере ЦР приведён в таблицах ниже.

Ролевое администрирование сервера ЦС

Роли и группы	Разрешение безопасности Службы сертификатов	Описание
Локальный администратор (Сервера ЦС)		Установка и разворачивание ЦС, формирование и уничтожение ключа ЭП и сертификатом ключа проверки ЭП ЦС (совместно с Администратором ЦС), управление ключом шифрования и сертификатом Веб-сервера ЦС, регистрация ЦР, архивирование и восстановление баз ЦР. Это роль операционной системы. Определяется членством в группе локальных администраторов операционной системы.
Администратор ЦС Аудитор(Сервер а ЦС)	Управление ЦС Управление аудитом и журналом безопасности	Настройка и обслуживание ЦС, загрузка ключа ЭП ЦС. Это роль ЦС, которая включает в себя возможность назначать все остальные роли. Эта роль также называется Уполномоченное лицо УЦ. Данные разрешения назначаются с помощью Диспетчера УЦ. Настройка, просмотр и обслуживание журналов аудита. Аудит — это функциональная возможность операционной системы. Аудитор — это роль операционной системы.

Ролевое администрирование сервера ЦР

Роли и группы	Разрешение безопасности Сервера ЦР	Описание
Локальный администратор (Сервера ЦР)		Установка и разворачивание ЦР, управление ключом ЭП и сертификатом ЦР, управление ключом шифрования и сертификатом Вебсервера ЦР, регистрация администраторов службы регистрации, архивирование и восстановление баз ЦР. Это роль операционной системы. Определяется членством в группе локальных администраторов операционной системы.
Администра-тор службы регистрации	Администратор службы регистрации	Настройка и обслуживание всей службы регистрации. Это роль клиента ЦР, которая включает в себя возможность назначать все остальные роли ЦР и настраивать Центр регистрации. Данные разрешения назначаются с помощью Диспетчера УЦ и Консоли управления ЦР. Администраторы службы регистрации выполняют свои функции через Консоль управления ЦР
Аудитор(Сервер а ЦР)	Управление аудитом и журналом безопасности	Настройка, просмотр и обслуживание журналов аудита. Аудит — это функциональная возможность операционной системы. Аудитор — это роль операционной системы.
Администра-тор ЦР	Чтение, Подача запросов, Одобрение запросов, Настройка параметров, Настройка безопасности	Администратор ЦР — это клиенты ЦР, которым разрешено регистрировать пользователей и запрашивать сертификаты в ЦС. Настраивается в Консоли Управления ЦР. Администратор ЦР отличается от Оператора ЦР

		возможностью создавать других Операторов ЦР и настраивать ЦР, в том числе параметры безопасности. Администраторы ЦР выполняют свои функции через Консоль управления ЦР.
Оператор ЦР	Чтение, Подача запросов, Одобрение запросов	Оператор ЦР — это клиенты ЦР, которым разрешено регистрировать пользователей и запрашивать сертификаты в ЦС. Операторы ЦР выполняют свои функции через Консоль управления ЦР.

10. Обеспечение безопасности

10.1. Инженерно-технические меры защиты информации

10.1.1. Размещение технических средств УЦ

Сервера Центра сертификации, Центра регистрации и телекоммуникационное оборудование размещены в серверном помещении.

Сервера Центра сертификации, Центра регистрации и телекоммуникационное оборудование размещаются в шкафу-стойке (cabinet).

Остальные технические средства УЦ размещаются в рабочих помещениях УЦ по схеме организации рабочих мест персонала.

10.1.2. Физический доступ в помещения

Серверное помещение УЦ оборудовано системой контроля доступа с идентификацией по карте.

Серверное помещение оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

Рабочие и служебные помещения УЦ не подключены к системе контроля доступа и оборудованы механическими замками

Идентификационные карты для доступа в серверное помещение выдаются сотрудникам из состава Службы безопасности и Технической службы УЦ по приказу руководителя УЦ.

Ключи механических замков рабочих помещений УЦ выдаются сотрудникам УЦ по распоряжению руководителя Административной службы УЦ на основании схемы организации рабочих мест персонала.

10.1.3. Электроснабжение и кондиционирование воздуха

Технические средства УЦ подключены к общегородской сети электроснабжения.

Электрические сети и электрооборудование, используемые в УЦ, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Сервера Центра сертификации и Центра регистрации, телекоммуникационное оборудование подключены к источникам бесперебойного питания, обеспечивающие их работу в течение не менее 1 часа после прекращения основного электроснабжения.

Технические средства, эксплуатируемые на рабочих местах сотрудников УЦ, источниками бесперебойного питания не оборудуются.

Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-

влажностного режима, вентиляции и очистки воздуха.

Служебные помещения УЦ, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях оборудованы средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения УЦ оборудованы средствами вентиляции и кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

10.1.4. Подверженность воздействию влаги

Защита серверов Центра сертификации и Центра регистрации и телекоммуникационного оборудования от воздействия влаги обеспечивается их размещением в шкафу-стойке (cabinet).

10.1.5. Предупреждение и защита от возгорания

Серверное помещение УЦ оборудовано системой автоматического пожаротушения, пожарной сигнализации и дымоудаления.

Пожарная безопасность помещений УЦ обеспечивается в соответствии с нормами и требованиями СНиП по классу Ф3.5, устанавливаемыми законодательством Российской Федерации.

10.1.6. Хранение документированной информации

Документальный фонд УЦ, как фондообразователя, подлежит хранению в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

10.1.7. Уничтожение документированной информации

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками УЦ, обеспечивающими документирование.

10.2. Программно-аппаратные меры защиты информации

10.2.1. Организация доступа к техническим средствам УЦ

Доступ к техническим средствам УЦ, размещённым в серверном помещении, осуществляется с использованием системы контроля доступа.

Идентификационные карты доступа в серверное помещение выдаются сотрудникам на основании приказа руководителя УЦ.

Организация доступа к техническим средствам УЦ, размещённых на рабочих местах сотрудников УЦ, возлагается на сотрудников УЦ, ответственных за эксплуатацию данных технических средств.

10.2.2. Организация доступа к программным средствам УЦ

Сервера Центра сертификации и Центра регистрации оснащены сертифицированными

программно-аппаратными комплексами защиты от несанкционированного доступа «Электронный замок» - Программно-аппаратный комплекс «Соболь». Версия 3.0.

Рабочие места сотрудников УЦ, на которых эксплуатируются программные приложения «АРМ администратора ЦР» и «АРМ разбора конфликтных ситуаций» также оснащены сертифицированными программно-аппаратными комплексами защиты от несанкционированного доступа типа «Электронный замок» - Программно-аппаратный комплекс «Соболь». Версия 3.0.

Устройство типа «Электронный замок» при локальной аутентификации администраторов на технических компонентах УЦ ограничивает количество подряд следующих неудачных попыток доступа числом не более 3.

Доступ системных администраторов общесистемного программного обеспечения серверов Центра сертификации и Центра регистрации для выполнения регламентных работ осуществляется в присутствии сотрудников Службы безопасности УЦ, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения (Центра сертификации и/или Центра регистрации).

10.2.2.1. Общий перечень объектов доступа УЦ

К объектам доступа УЦ относятся:

- технические средства компонент УЦ;
- программное обеспечение компонент УЦ: ПО центра сертификации, ПО Центра регистрации, ПО АРМ администратора Центра регистрации, ПО АРМ разбора конфликтных ситуаций, ПО, предназначенное для регистрации и управления сертификатами пользователей УЦ;
- базы данных компонент УЦ: база данных ЦС, база данных ЦР;
- ключи ЭП и сертификаты ключей проверки ЭП;
- списки отозванных сертификатов УЦ.

10.2.2.2. Перечень объектов доступа, предоставляемых сотрудникам УЦ

Сотрудникам Административной службы УЦ:

- технические средства Центра сертификации и Центра регистрации УЦ;
- технические средства АРМ разбора конфликтных ситуаций;
- программное обеспечение Центра сертификации и Центра регистрации УЦ;
- база данных Центра сертификации и Центра регистрации УЦ;
- ключи ЭП и сертификаты ключей проверки ЭП, используемые для эксплуатации Центра сертификации и Центра регистрации;
- списки отозванных сертификатов УЦ.

Сотрудникам Службы регистрации УЦ:

- технические средства АРМ администратора Центра регистрации;
- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- личные ключи ЭП и сертификаты ключей проверки ЭП сотрудников Службы регистрации;
- служебные ключи и служебные сертификаты ключей проверки ЭП пользователей УЦ;
- рабочие сертификаты ключей проверки ЭП пользователей УЦ;
- списки отозванных сертификатов.

Сотрудникам Службы безопасности УЦ:

- технические средства АРМ администратора Центра регистрации;

- программное обеспечение АРМ администратора Центра регистрации;
- база данных Центра регистрации;
- личные ключи ЭП и сертификаты ключей проверки ЭП сотрудников Службы безопасности;
- служебные сертификаты ключей проверки ЭП пользователей УЦ;
- рабочие ключи и рабочие сертификаты ключей проверки ЭП пользователей УЦ;
- списки отозванных сертификатов.

Сотрудникам технической службы УЦ:

- технические средства компонент УЦ;
- программное обеспечение компонент УЦ;
- базы данных Центра сертификации и Центра регистрации.

10.2.2.3. Перечень объектов доступа, предоставляемых аутентифицированным пользователям УЦ при осуществлении сетевого взаимодействия с программными средствами УЦ

Незарегистрированным пользователям УЦ, проходящим процедуру регистрации в УЦ:

- программное обеспечение формирования запроса на регистрацию Пользователя УЦ в электронном виде;
- программное обеспечение формирования запроса на регистрацию Пользователя УЦ в бумажном виде;

Зарегистрированным пользователям УЦ:

- квалифицированный сертификат ключа проверки ЭП Уполномоченного лица УЦ в электронной форме;
- список отозванных сертификатов ключей проверки ЭП в электронной форме;
- квалифицированный сертификат ключа проверки ЭП пользователей УЦ в электронной форме;
- программное обеспечение предоставления учётной информации о квалифицированных сертификатах ключей проверки ЭП аутентифицированного Пользователя УЦ и их статусе;
- программное обеспечение предоставления учётной информации о запросах (заявлениях) в электронной форме, поступивших в УЦ от аутентифицированного Пользователя УЦ и статусе их обработки;
- программное обеспечение формирования ключей и заявления на изготовление квалифицированного сертификата ключа проверки ЭП в электронной форме аутентифицированного Пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изготовленного сертификата ключа проверки ЭП Пользователя УЦ;
- программное обеспечение формирования электронного бланка копии сертификата ключа проверки ЭП Пользователя УЦ в бумажной форме;
- программное обеспечение формирования заявления на аннулирование (отзыв) квалифицированного сертификата ключа проверки ЭП в электронной форме Пользователя УЦ;
- программное обеспечение предоставления учётной информации о сертификатах ключей проверки ЭП пользователей УЦ и самих сертификатах ключей проверки ЭП пользователей УЦ в электронной форме.
- личные ключи и сертификаты ключей проверки ЭП Пользователя УЦ.

10.2.3. Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого УЦ:

- Программные модули средств электронной подписи и криптографической защиты информации;
- Программные модули Комплекса программ Удостоверяющего центра.

Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом УЦ, утверждаемый руководителем УЦ.

Система контроля целостности программных модулей, подлежащих контролю целостности, основывается на аппаратном контроле целостности и общесистемного программного обеспечения до загрузки операционной системы.

Данная система контроля целостности обеспечивается использованием сертифицированного устройства типа «электронный замок».

Контроль целостности программных модулей средств электронной подписи и криптографической защиты информации осуществляется средствами средств электронной подписи и криптографической защиты информации.

Периодичность выполнения мероприятий по контролю целостности — ежедневно.

Ответственность за выполнение мероприятий по контролю целостности программных средств возложена на Службу безопасности УЦ.

10.2.4. Контроль целостности технических средств

Контроль целостности технических средств УЦ обеспечивается опечатыванием корпусов устройств, препятствующим их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию и после выполнения регламентных работ.

Контроль целостности печатей осуществляется в начале каждой рабочей смены.

Ответственность за выполнение мероприятий по контролю целостности технических средств возложена на Службу безопасности УЦ.

10.2.5. Защита внешних сетевых соединений

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности УЦ и программными средствами, предоставляемыми УЦ пользователям УЦ, в процессе обмена документами в электронной форме, осуществляется путём шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Российской Федерации.

В качестве шифровальных (криптографических) средств пользователей УЦ, используемых для защиты конфиденциальной информации, используется средство электронной подписи Пользователя УЦ.

Защита программно-технических средств обеспечения деятельности Удостоверяющего Центра от несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования межсетевого экрана сертифицированного ФСБ России 4-го класса защиты - АПКШ «Континент» 3.7. ЦУС Платформа IPS10. КСЗ.

При организации сетевого взаимодействия компонентов ПАК «КриптоПро УЦ 2.0» между собой размещены в одной контролируемой зоне.

Технические средства с установленным ПАК «КриптоПро УЦ 2.0» не подключены к

техническим средствам общедоступных сетей связи, в том числе, сети Интернет.

10.2.5.1. Перечень информации, подлежащей защите

Поступающая в УЦ информация:

- Заявление на регистрацию в электронной форме;
- Заявление на изготовление квалифицированного сертификата ключа проверки ЭП в электронной форме;
- Заявление на аннулирование (отзыв) квалифицированного сертификата ключа проверки ЭП в электронной форме;
- Маркер временного доступа, который используется для обращения на страницу формирования ключа электронной подписи и запроса на КСКПЭП,

Передаваемая из УЦ информация:

- Бланк копии сертификата ключа проверки ЭП для вывода на бумажный носитель;
- Список квалифицированных сертификатов ключа проверки ЭП Пользователя УЦ и их статус;
- Список запросов на квалифицированные сертификаты ключей проверки ЭП Пользователя УЦ и их статус;
- Список запросов на аннулирование (отзыв) квалифицированных сертификатов ключей проверки ЭП Пользователя УЦ и их статус.

10.3. Организационные меры защиты информации

10.3.1. Предъявляемые требования к персоналу УЦ

Уполномоченное лицо УЦ имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более 2 лет.

Сотрудники Службы безопасности УЦ имеют высшее профессиональное образование и прошли курсы повышения квалификации в области информационной безопасности с получением специализации в области систем с открытым распределением ключей.

10.3.2. Профессиональная переподготовка и повышение квалификации персонала

Профессиональная переподготовка персонала УЦ не осуществляется.

Сотрудники УЦ осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 2 года.

10.3.3. Организация сменной работы

Деятельность УЦ по работе с пользователями УЦ в части приёма заявлений в бумажной форме и изготовления сертификатов ключей проверки ЭП организована в одну рабочую смену с 9.00 до 18.00 в будние дни.

Выходными днями являются: суббота, воскресенье, а также дни общенациональных праздников.

10.3.4. Организация доступа персонала к документам и документации

Доступ сотрудников УЦ к документам и документации, составляющей документальный

фонд организации, организован в соответствии с должностными инструкциями и функциональными обязанностями.

10.3.5. Охрана здания и помещений

УЦ имеет собственную (привлекаемую) службу охраны здания и помещений, обеспечивающую:

- Обнаружение и задержание нарушителей, пытающихся проникнуть в здание (помещения) УЦ;
- Сохранность материальных ценностей и документов;
- Предупреждение происшествий и ликвидацию их последствий.

10.4. Юридические меры защиты информации

УЦ имеет разрешение (лицензии) по всем видам деятельности, связанных с предоставлением услуг (см. 2.2).

Системы безопасности УЦ и защиты информации созданы и поддерживаются на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с действующим законодательством Российской Федерации.

Все меры по защите информации в УЦ введены в действие приказами руководителя УЦ.

Для обеспечения деятельности УЦ использует средства электронной подписи и криптографической защиты информации, сертифицированные в соответствии с действующим законодательством Российской Федерации.

Исключительные имущественные права на информационные ресурсы УЦ находятся в собственности УЦ.

Пользователям УЦ предоставляются неисключительные имущественные права на копии сертификатов и списков отозванных сертификатов, изготавливаемые УЦ в объёме прав согласно разделу 3.2 настоящего Регламента.

11. Взаимодействие Удостоверяющего центра с федеральными органами исполнительной власти в сфере использования электронной подписи

Для использования пользователями Удостоверяющего центра квалифицированной электронной подписи и изготовления квалифицированных сертификатов ключей проверки ЭП Удостоверяющий центр аккредитован Уполномоченным федеральным органом исполнительной власти в области применения электронной подписи (Статья 6, пункт 2, ФЗ №63-ФЗ «Об электронной подписи»).

Порядок и требования к аккредитации устанавливаются ФЗ №63-ФЗ «Об электронной подписи» (Статья 16) и Правилами аккредитации Удостоверяющих центров, устанавливаемых федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

СПИСОК ЛИТЕРАТУРЫ

- № 63-ФЗ. «Об электронной подписи.» *Федеральный закон*. Москва, 6 Апреля 2011 г.
- PKCS #9. «Selected Object Classes and Attribute Types Version 2.0.» Ноябрь 2000 г. *RFC 2985*.
<<http://tools.ietf.org/html/rfc2985>>.
- RFC 3647. «Certificate Policy and Certification Practices Framework.» Ноябрь 2003 г. *Internet X.509 Public Key Infrastructure*, <<http://tools.ietf.org/html/rfc3647>>.
- RFC 4519. «Schema for User Applications.» Июнь 2006 г. *Lightweight Directory Access Protocol (LDAP)*. <<http://tools.ietf.org/html/rfc4519>>.
- RFC 5280. «Certificate and Certificate Revocation List (CRL) Profile.» Май 2008 г. *InternetX.509 Public Key Infrastructure*, <<http://tools.ietf.org/html/rfc5280>>.
- ЖТЯИ.00078-01 30 01. ПAK КpиптoПpo УЦ 2.0. Фopмyляp. 2013.
- ЖТЯИ.00078-01 90 02. ПAK КpиптoПpo УЦ 2.0. Pyкoвoдcтвo пo ycтaнoвкe. 2013.
- ЖТЯИ.00078 01 90 06 ПAK КpиптoПpo УЦ 2.0. Tипoвoй pеглaмeнт. 2013
- MCЭ-TX.509. «Стpyкчypы ceртифиkатoв oткpытых ключей и aтpибyтoв.» Aвгyст 2008 г.
Инфopмaциoнныe тexнoлoгии - Bзaимocвязь oткpытых cистeм - Cпpавoчник.
<<http://www.itu.int/rec/T-REC-X.509-200508-1/en>>.
- MCЭ-T X.520. «Избpанные типы aтpибyтoв.» Aвгyст 2005 г. *Инфopмaциoнныe тexнoлoгии - Bзaимocвязь oткpытых cистeм - Cпpавoчник*. <<http://www.itu.int/rec/T-REC-X.520-200508-1/en>>.

**Список документов необходимых Пользователю для регистрации в
Удостоверяющем центре и получения КСКПЭП.**

Для юридических лиц:

1. Заявление на регистрацию Клиента и изготовление КСКПЭП в Удостоверяющем центре и Согласие на обработку персональных данных.
2. Копия Свидетельства ОГРН (либо сведения об ОГРН).
3. Страховое свидетельство государственного пенсионного страхования заявителя.
4. Документ, удостоверяющий личность владельца сертификата, в соответствии с законодательством РФ - паспорта на разворотах с фотографией и местом регистрации по месту жительства.

Для индивидуальных предпринимателей:

1. Заявление на регистрацию Клиента и изготовление КСКПЭП в Удостоверяющем центре и Согласие на обработку персональных данных.
2. Страховое свидетельство государственного пенсионного страхования заявителя.
3. Копия Свидетельства ОГРНИП (либо сведения об ОГРНИП).
4. Документ, удостоверяющий личность владельца КСКПЭП, в соответствии с законодательством РФ - паспорта на разворотах с фотографией и местом регистрации по месту жительства.

Для физических лиц:

1. Заявление на регистрацию Клиента и изготовление КСКПЭП в Удостоверяющем центре и Согласие на обработку персональных данных.
2. Страховое свидетельство государственного пенсионного страхования заявителя.
3. Документ, удостоверяющий личность владельца КСКПЭП, в соответствии с законодательством РФ - паспорта на разворотах с фотографией и местом регистрации по месту жительства.

Для юридических лиц

Заявление

на регистрацию Пользователя и изготовление квалифицированного сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «Электронный экспресс» (УЦ ГАРАНТ).

(полное наименование организации, включая организационно-правовую форму)	
В лице	(должность руководителя или уполномоченного сотрудника)
(фамилия, имя, отчество)	
действующего на сновании	
просит зарегистрировать уполномоченного представителя	
(фамилия, имя, отчество)	

в Реестре УЦ ГАРАНТ, наделить полномочиями Пользователя УЦ ГАРАНТ, установленные Регламентом ЮЗД и изготовить КСКПЭП в соответствии с указанными в настоящем заявлении данными и ограничениями:

(CN) Наименование Организации	
(SN) Фамилия	
(G) Имя Отчество	
(O) Наименование организации	
(OU) Наименование подразделения	
(T) Должность	
(L) Город	
(S) Субъект Федерации	
(C) Страна	RU
(E) Адрес электронной почты	
(OGRN) ОГРН организации	
(INN) ИНН организации	
(SNILS) СНИЛС владельца сертификата	

Используемое средство электронной подписи	
---	--

Ограничения квалифицированного сертификата:

Владелец квалифицированного
сертификата
паспорт серии _____ № _____ выдан « _____ » _____ года

подпись

Ф.И.О.

наименование органа, выдавшего документ

Руководитель (должность)

подпись

Ф.И.О.

М.П.

(заполняется уполномоченным лицом Центра Регистрации)

Заявление зарегистрировано в Центре Регистрации:

(название организации — Центра Регистрации)

« _____ » _____ 201 ____ года.

Уполномоченное лицо Центра Регистрации

подпись

Ф.И.О.

Для индивидуальных предпринимателей (ИП) и физических лиц

Заявление

на регистрацию Пользователя и изготовление квалифицированного сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «Электронный экспресс» (УЦ ГАРАНТ).

Я,

(фамилия, имя, отчество)

паспорт серии _____ № _____ выдан « _____ » _____ года

(наименование органа, выдавшего документ)

прошу зарегистрировать меня в Реестре УЦ ГАРАНТ, наделить полномочиями Пользователя УЦ ГАРАНТ, установленные Регламентом ЮЗД, и изготовить КСКПЭП в соответствии с указанными в настоящем заявлении данными и ограничениями:

(CN) Фамилия, Имя, Отчество	
(L) Город	
(S) Субъект Федерации	
(C) Страна	RU
(E) Адрес электронной почты	
(INN) ИНН владельца сертификата	
(SNILS) СНИЛС владельца сертификата	
(OGRNIP) ОГРНИП (для индивидуальных предпринимателей)	

Используемое средство электронной подписи	
---	--

Ограничения квалифицированного сертификата:

Владелец квалифицированного сертификата *

подпись _____ Ф.И.О.

паспорт серии _____ № _____ выдан « _____ » _____ 201 _____ года

(наименование органа, выдавшего документ)

(заполняется уполномоченным лицом Центра Регистрации)

Заявление зарегистрировано в Центре Регистрации:

(название организации — Центра Регистрации)

_____ » _____ 201 _____ года.

Уполномоченное лицо Центра Регистрации

подпись

Ф.И.О.

*

Для ИП. Заполняется в случае получения сертификата не на заявителя. В этом случае заявление должно быть нотариально заверенным.

Для юридических лиц.

ИНН	ОКАТО
Юридический адрес:	

Доверенность

Город _____ Дата выдачи « _____ » _____ 201__ г.

(сокращенное наименование юридического лица, включая организационно-правовую форму)
в лице _____
(должность лица, уполномоченного действовать от имени юридического лица)

(фамилия, имя, отчество)
действующего на основании _____
настоящей доверенностью уполномочивает

паспорт серии _____	№ _____	(фамилия, имя, отчество доверенного лица) выдан « _____ » _____	года
(наименование органа, выдавшего документ)			

- Предоставить в Удостоверяющий центр ООО «Электронный экспресс» (УЦ ГАРАНТ) документы, необходимые для изготовления квалифицированного сертификата Пользователя УЦ - полномочного представителя

(сокращенное наименование юридического лица, включая организационно-правовую форму)
• Получить сертификат ключа проверки электронной подписи Удостоверяющего центра ООО «Электронный экспресс» (УЦ ГАРАНТ), все сертификаты входящие в цепочку квалифицированных сертификатов, необходимых для проверки электронной подписи в квалифицированном сертификате Удостоверяющего центра ООО «Электронный экспресс» (УЦ ГАРАНТ), маркер временного доступа и/или сформированные ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи Пользователя УЦ (в том числе, подписать Заявление на регистрацию Пользователя и изготовление КСКПЭП и бумажный документ с информацией из КСКПЭП) -

(фамилия, имя, отчество владельца сертификата)		
Владелец квалифицированного сертификата	подпись _____	Ф.И.О. _____
паспорт серии _____	№ _____	выдан « _____ » _____ года

(наименование органа, выдавшего документ)
Настоящая доверенность действительна по _____ 201__ г.
Доверенность выдана без права передоверия.
Подпись уполномоченного представителя _____
подпись _____ Ф. И. О. _____

подтверждаю

(должность руководителя, название организации)	подпись _____	Ф. И. О. _____
--	---------------	----------------

М.П. _____ 201__ года.

Согласие на обработку персональных данных.

Я,

(фамилия, имя, отчество)

проживающий по адресу

индекс страна субъект Федерации город район улица дом кв.

паспорт серии _____ № _____ выдан « _____ » _____ года.

(наименование органа, выдавшего документ)

даю свое согласие на обработку моих персональным данными, перечисленных в настоящем согласии.

Перечень персональных данных, на обработку которых дается согласие:

Фамилия, имя, отчество, ИНН, место работы (организация), должность, подразделение, город, страна, адрес электронной почты, телефон, паспортные данные.

Паспортные данные не включаются в состав сертификата.

Даю согласие на включение моих персональных данных, таких как фамилия, имя, отчество, ИНН, место работы (организация), должность, подразделение, город, страна, адрес электронной почты, в общедоступный источник персональных данных — справочник квалифицированных сертификатов, что делает перечисленные персональные данные общедоступными персональными данными.

Цель обработки персональных данных:

Изготовление и обслуживание квалифицированного сертификата в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» и регистрации пользователя в прикладных системах. А также для иных целей определенных законодательством Российской Федерации.

Согласие выдается:

Оператору 1:

ООО «Электронный экспресс»

(полное наименование организации, включая организационно-правовую форму)

Адрес: 119991 Россия Москва Москва Ленинские горы 1 77
индекс страна субъект Федерации город район улица дом стр кор кв.

Оператору 2:

(полное наименование Центра Регистрации, включая организационно-правовую форму)

Адрес:

индекс страна субъект Федерации город район улица дом стр кор кв.

Действия с персональными данными, на совершение которых дается согласие:

Сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, уничтожение.

Общее описание используемых операторами способов обработки персональных данных:

Оператор 2 осуществляет регистрацию персональных данных на серверах Оператора 1 и возможное уточнение этих персональных данных, т.е. Оператор 2 выполняет сбор и уточнение (обновление, изменение) персональных данных. Оператор 1 выполняет на своих серверах систематизацию, хранение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных. Оператор 1 выпускает квалифицированный сертификат с персональными данными, на которые дано согласие на включение в общедоступный источник персональных данных и публикует его в общедоступном справочнике квалифицированных сертификатов (в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»).

Срок действия настоящего согласия и порядок его отзыва:

Данное согласие действительно на весь срок хранения моего квалифицированного сертификата в Удостоверяющем центре ГАРАНТ (ООО «Электронный экспресс») в электронном и (или) бумажном виде. Указанный срок определен в Федеральном законе от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи». Согласие может быть отозвано путем подачи письменного заявления на отзыв согласия Оператору 1 или Оператору 2 и письменного заявления на отзыв квалифицированного сертификата в соответствии с Регламентом Юридически значимого документооборота. При этом время хранения персональных данных определяется Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

подпись

Ф. И.О.Заявителя

»

201 _____ года.

**Удостоверяющий центр ООО «Электронный экспресс» (УЦ ГАРАНТ).
Квалифицированный сертификат ключа проверки электронной подписи.**

Владелец квалифицированного
сертификата

подпись

Ф.И.О.

_____» _____ 201 ____ года.

Уполномоченное лицо УЦ
ГАРАНТ

подпись

Ф.И.О.

М.П.

_____» _____ 201 ____ года.

Для юридических лиц

**Заявление
на аннулирование (отзыв) квалифицированного сертификата ключа проверки электронной
подписи Пользователя Удостоверяющего центра ООО «Электронный экспресс» (УЦ
ГАРАНТ).**

_____ (полное наименование организации, включая организационно-правовую форму)

в лице

_____ (должность руководителя или уполномоченного сотрудника)

_____ (фамилия, имя, отчество)

действующего на основании

просит аннулировать (отозвать) квалифицированный сертификат:

_____ (серийный номер сертификата)

выданный на имя

_____ (Ф.И.О владельца сертификата)

в связи с

_____ (причина аннулирования (отзыва) квалифицированного сертификата: компрометация ключа электронной подписи, прекращение работы и т.д.).

Владелец квалифицированного
сертификата

_____ подпись

_____ Ф.И.О.

_____ » _____ 201 ____ года.

_____ Руководитель (должность)

_____ подпись

_____ Ф.И.О.

М.П.

_____ » _____ 201 ____ года.

_____ (заполняется уполномоченным лицом Центра Регистрации)

Данное заявление на аннулирование (отзыв) квалифицированного сертификата зарегистрировано

_____ (название организации — Центра Регистрации)

« _____ » _____ 201 ____ года.

Уполномоченное лицо Центра Регистрации

_____ подпись

_____ Ф.И.О.

Для индивидуальных предпринимателей (ИП) и физических лиц

**Заявление
на аннулирование (отзыв) квалифицированного сертификата ключа проверки электронной
подписи Пользователя Удостоверяющего центра ООО «Электронный экспресс» (УЦ
ГАРАНТ).**

Я, _____

(Ф.И.О.)
паспорт серии _____ № _____ выдан « _____ » _____ Года

(наименование органа, выдавшего документ)
прошу аннулировать (отозвать) КСКПЭП

(серийный номер КСКПЭП)
выданный на имя _____

(Ф.И.О. владельца КСКПЭП)
в связи с _____

(причина аннулирования (отзыва) КСКПЭП: компрометация ключа электронной подписи, прекращение работы и т.д.).

Владелец КСКПЭП

подпись

Ф.И.О.

_____ » _____ 201 ____ года.

_____ (заполняется уполномоченным лицом Центра Регистрации)

Данное Заявление на аннулирование (отзыв) КСКПЭП зарегистрировано,

(Ф.И.О. владельца КСКПЭП)
личность идентифицирована, сведения, указанные в Заявлении проверены.

(название организации — Центра Регистрации)
« _____ » _____ 201 ____ года.

Уполномоченное лицо Центра
Регистрации

подпись

Ф.И.О.

Для юридических лиц

Заявление
на подтверждение подлинности электронной подписи Удостоверяющего центра ООО
«Электронный экспресс» (УЦ ГАРАНТ) в квалифицированном сертификате ключа проверки
электронной подписи Пользователя УЦ,
изготовленного УЦ ГАРАНТ.

_____ (полное наименование организации, включая организационно-правовую форму)

в лице

_____ (должность руководителя или уполномоченного сотрудника)

_____ (фамилия, имя, отчество)

действующего на основании

Просит подтвердить подлинность электронной подписи Удостоверяющего Центра ООО «Электронный экспресс» (УЦ ГАРАНТ) в КСКПЭП, изготовленном УЦ ГАРАНТ на имя:

_____ (ФИО владельца проверяемого КСКПЭП)

_____ (серийный номер сертификата)

и установить статус этого КСКПЭП (действовал/не действовал) на момент:

_____ (дата и время, на момент наступления которых требуется установить статус КСКПЭП)*

Руководитель (должность)

подпись

Ф.И.О.

М.П.

« ____ » _____ 201 ____ года.

_____ (заполняется уполномоченным лицом Центра Регистрации)

Данное Заявление на подтверждение электронной подписи в КСКПЭП зарегистрировано

_____ (название организации — Центра Регистрации)

« ____ » _____ 201 ____ года.

_____*

Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус КСКПЭП устанавливается на момент времени принятия заявления Удостоверяющим центром ГАРАНТ

Уполномоченное лицо Центра Регистрации _____
подпись Ф.И.О.

Приложение № 7 б

Для индивидуальных предпринимателей (ИП) и физических лиц

Заявление
на подтверждение подлинности электронной подписи Удостоверяющего Центра ООО
«Электронный экспресс» (УЦ ГАРАНТ) в квалифицированном сертификате ключа проверки
электронной подписи Пользователя УЦ,
изготовленного УЦ ГАРАНТ.

Я, _____
(Ф.И.О.)
паспорт серии ____ № ____ выдан « ____ » ____ года

(наименование органа, выдавшего документ)
прошу подтвердить подлинность электронной подписи Удостоверяющего Центра ООО «Электронный экспресс» (УЦ ГАРАНТ) в КСКПЭП, изготовленном УЦ ГАРАНТ на имя:

(ФИО владельца проверяемого КСКПЭП)

(серийный номер сертификата)
и установить статус этого КСКПЭП (действовал/не действовал) на момент:

(дата и время, на момент наступления которых требуется установить статус КСКПЭП)*

Пользователь Удостоверяющего _____
центра подпись Ф.И.О.

« ____ » ____ 201 ____ года.

(заполняется уполномоченным лицом Центра Регистрации)

Данное Заявление на подтверждение электронной подписи в КСКПЭП зарегистрировано,
личность

(Ф.И.О. Пользователя УЦ)
идентифицирована, сведения, указанные в Заявлении проверены.

(название организации — Центра Регистрации)
« ____ » ____ 201 ____ года.

Уполномоченное лицо Центра Регистрации _____
подпись Ф.И.О.

*

Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Для юридических лиц

**Заявление
на подтверждение подлинности электронной подписи
в электронном документе.**

_____ в лице	_____ (должность руководителя или уполномоченного сотрудника)
_____ действующего на основании	_____ (фамилия, имя, отчество)

Просит подтвердить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий КСКПЭП, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № МД–XXX;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № МД–XXX
3. Время¹ на момент наступления которых требуется подтвердить подлинность электронной подписи:
 час _____ минута _____ день _____ месяц _____ год _____

_____ Руководитель (должность)	_____ подпись	_____ Ф.И.О.
М.П.		
« _____ » _____ 201 ____ года.		

_____ (заполняется уполномоченным лицом Центра Регистрации)
Данное Заявление на подтверждение подлинности электронной подписи в электронном документе зарегистрировано
_____ (название организации — Центра Регистрации)
« _____ » _____ 201 ____ года.

¹

Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то подтверждение подлинности электронной подписи устанавливается на момент времени принятия заявления Удостоверяющим центром ГАРАНТ.

Уполномоченное лицо Центра Регистрации

подпись

Ф.И.О.

Для индивидуальных предпринимателей (ИП) и физических лиц

**Заявление
на подтверждение подлинности электронной подписи
в электронном документе.**

Я, _____ (Ф.И.О.)
паспорт серии ____ № ____ выдан « ____ » ____ года

(наименование органа, выдавшего документ)

прошу подтвердить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий КСКПЭП, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № МД-XXX;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № МД-XXX
4. Время¹ на момент наступления которых требуется подтвердить подлинность электронной подписи:
час ____ минута ____ день ____ месяц ____ год ____

Пользователь Удостоверяющего центра _____
подпись Ф.И.О.

М.П.

« ____ » ____ 201 ____ года.

(заполняется уполномоченным лицом Центра Регистрации)

Данное Заявление подтверждение подлинности электронной подписи в электронном документе
зарегистрировано,
личность

(Ф.И.О Пользователя УЦ)
идентифицирована, сведения, указанные в Заявлении проверены.

(название организации — Центра Регистрации)
« ____ » ____ 201 ____ года.
Уполномоченное лицо Центра Регистрации

подпись Ф.И.О.

1

Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени).
Если время и дата не указаны, то подтверждение подлинности электронной подписи устанавливается на
момент времени принятия заявления Удостоверяющим центром ГАРАНТ.

**Структура квалифицированного сертификата ключа проверки электронной подписи
Удостоверяющего центра ООО «Электронный экспресс» (УЦ ГАРАНТ).**

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CN = УЦ 1 ИС ГУЦ C = RU S = 77 г. Москва L = Москва O = Минкомсвязь России STREET = 125375 г. Москва ул. Тверская д.7 E = dit@minsvyaz.ru ОГРН = 1047702026701 ИНН = 007710474375
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = ООО "Электронный экспресс" OU = Удостоверяющий центр O = ООО "Электронный экспресс" L = Москва S = 77 г.Москва Street = Ленинские горы, д. 1, стр. 77 OGRN = 1097746293886 INN = 007729633131 C = RU E = uc@garant.ru
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа Удостоверяющего центра
BasicConstraints (critical)	Основные ограничения	SubjectType (Тип владельца сертификата) =ЦС Path Length Constraint (Ограничение на длину пути –ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров)= Отсутствует
CA Version	Версия ЦС.	Версия сертификата Удостоверяющего центра
Расширения сертификата		
Key Usage	Использование ключа	Цифровая подпись, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL)
Certificate Policies	Политики сертификатов	OID=1.2.643.100.113.1 OID=1.2.643.100.113.2
SubjectSignNool (OID.1.2.643.100.111)	Наименование средства ЭП	КриптоПро CSP v.3.9
IssuerSignTool (OID.1.2.643.100.112)	SignTool caTool signToolCert caToolCert	Полное наименование средства ЭП Полное наименование средства аккредитованного УЦ Реквизиты заключения ФСБ о подтверждении соответствия средства ЭП Реквизиты заключения ФСБ о подтверждении соответствия средства УЦ
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа владельца сертификата.
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа Уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат.
Authority Information Access (AIA)	Адрес КСКПЭП УЦ ГАРАНТ	http://ca.garant.ru/ca/accredited/garant_ac4.cer

**Структура квалифицированного сертификата ключа проверки электронной подписи Клиента
- юридического лица.**

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CN = Аккредитованный УЦ ГАРАНТ OU = Удостоверяющий центр O = ООО Электронный экспресс L = Москва Street = Ленинские горы, д. 1, стр. 77 OGRN = 1097746293886 INN = 7729633131 C = RU E = uc@garant.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец КСКПЭП	CN = Название организации или Фамилия, Имя, Отчество SN = Фамилия G = Имя Отчество O = Наименование организации OU = Наименование подразделения T = Должность L = Город S = Субъект Федерации C = Страна E = Адрес электронной почты OGRN = ОГРН организации INN = ИНН организации SNILS = СНИЛС владельца сертификата
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage	Использование ключа	Неотрекаемость, Цифровая подпись, Шифрование ключей, Шифрование данных.
Extended Key Usage	Улучшенный ключ	OID=1.3.6.1.5.5.7.3.4 - защищенная электронная почта; OID=1.3.6.1.5.5.7.3.2 – проверка подлинности клиента; OID=1.2.643.2.2.34.6 – пользователь Центра Регистрации;
Certificate Policies	Политики сертификатов	Указываются идентификаторы, описывающие ограничения использования сертификата. Класс средств ЭП
SubjectSignNool (OID.1.2.643.100.111)	Наименование средства ЭП	КриптоПро CSP v.3.6
IssuerSignTool (OID.1.2.643.100.112)	SignTool caTool signToolCert caToolCert	КриптоПро CSP v.3.6 ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 1.5 (вариант исполнения 1) Реквизиты заключения ФСБ о подтверждении соответствия средства ЭП СФ/128-1822
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа владельца сертификата.
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа Удостоверяющего центра, на котором подписан данный сертификат.
CRL Distribution Point (CDP)	Точка распространения списка отозванных сертификатов	http://ca.garant.ru/cdp/accredited/garant_ac2.crl http://www.garantexpress.ru/cdp/accredited/garant_ac2.crl
Authority Information Access (AIA)	Адрес КСКПЭП УЦ ГАРАНТ	http://ca.garant.ru/ca/accredited/garant_ac2.cer

**Структура квалифицированного сертификата ключа проверки электронной подписи Клиента
- физического лица.**

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CN = ООО Электронный экспресс OU = Удостоверяющий центр O = ООО Электронный экспресс L = Москва Street = Ленинские горы, д. 1, стр. 77 OGRN = 1097746293886 INN = 7729633131 C = RU E = uc@garant.ru
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец КСКПЭП	CN = Фамилия, Имя, Отчество L = Город S = Субъект Федерации C = Страна E = Адрес электронной почты INN = ИНН организации SNILS = СНИЛС владельца сертификата
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage	Использование ключа	Неотрекаемость, Цифровая подпись, Шифрование ключей, Шифрование данных.
Extended Key Usage	Улучшенный ключ	OID=1.3.6.1.5.5.7.3.4 - защищенная электронная почта; OID=1.3.6.1.5.5.7.3.2 – проверка подлинности клиента; OID=1.2.643.2.2.34.6 – пользователь Центра Регистрации;
Certificate Policies	Политики сертификатов	Указываются идентификаторы, описывающие ограничения использования сертификата. Класс средств ЭП
SubjectSignNool (OID.1.2.643.100.111)	Наименование средства ЭП	КриптоПро CSP v.3.9
IssuerSignTool (OID.1.2.643.100.112)	SignTool caTool signToolCert caToolCert	Средство электронной подписи: "КриптоПро CSP" (версия 3.9) Заключение на средство ЭП: Сертификат соответствия ФСБ России СФ/124-2539 от 15.01.2015 Средство УЦ: "КриптоПро УЦ" (версии 2.0) Заключение на средство УЦ: Сертификат соответствия ФСБ России № СФ/128-2881 от 12.04.2016
Subject Key Identifier	Идентификатор ключа владельца сертификата	Идентификатор ключа владельца сертификата.
Authority Key Identifier	Идентификатор ключа издателя сертификата	Идентификатор ключа Удостоверяющего центра, на котором подписан данный сертификат.
CRL Distribution Point (CDP)	Точка распространения списка отозванных сертификатов	http://ca.garant.ru/cdp/accredited/garant_ac4.crl http://www.garantexpress.ru/cdp/accredited/garant_ac4.crl
Authority Information Access (AIA)	Адрес КСКПЭП УЦ ГАРАНТ	http://ca.garant.ru/ca/accredited/garant_ac4.cer

Структура Списка отозванных сертификатов

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = ООО Электронный экспресс OU = Удостоверяющий центр O = ООО Электронный экспресс L = Москва Street = Ленинские горы, д. 1, стр. 77 OGRN = 1097746293886 INN = 7729633131 C = RU E = uc@garant.ru
Effective date	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
Next update	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
Revoked Certificates	Список отозванных сертификатов	Последовательность элементов следующего вида • Серийный номер сертификата (Serial Number) • Время обработки заявления на аннулирование (отзыв) или приостановление действия сертификата (Revocation Date) • Код причины отзыва сертификата (CRL Reason Code): "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия
Signature algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа Удостоверяющего центра, которым подписан СОС
CA Version	Версия сертификата издателя	Версия сертификата Удостоверяющего центра

Ценовые предложения ООО «Электронный экспресс».

Услуги по обеспечению юридически значимого электронного документооборота при сдаче отчетности и другом взаимодействии с государственными органами и организациями с одним сертификатом электронной подписи (ЭП)

1 593 руб. В т.ч. НДС 243 руб.

Услуги по обеспечению юридически значимого электронного документооборота при сдаче отчетности и другом взаимодействии с государственными органами и организациями с одним сертификатом ЭП, включая сопровождение сертификата ЭП

4 779 руб. В т.ч. НДС 729 руб.

Услуги по обеспечению юридически значимого электронного документооборота при внутрикорпоративном взаимодействии с одним сертификатом ЭП

3 068 руб. в т.ч. НДС 468 руб.

Услуги по обеспечению юридически значимого документооборота для участия в электронных торгах

6 313 руб. в т.ч. НДС 963 руб.

Экспертиза авторства и подлинности ЭЦП в электронном Документе

5 428 руб. в т.ч. НДС 828 руб.

Ценовые предложения доступны на сайте Общества:

http://www.garantexpress.ru/wp-content/uploads/2016/02/Cost_uslugi_new1.pdf

Примечания:

1. Условия, на основании которых ООО «Электронный экспресс» предоставляет услуги по организации ЮЗД юридическим и физическим лицам, определены и утверждены «Регламентом оказания услуг юридически значимого электронного документооборота (Регламента ЮЗД)».

2. Ценовые предложения не являются публичной офертой.