«Утверждаю»

Директор ООО Компания «Сервис ТВ-Инфо»

 /Лепехин Е.П./

01 июня 2013 года

В редакции от 15.01.2019г.

**РЕГЛАМЕНТ**

**Удостоверяющего центра**

**ООО Компания «Сервис ТВ-Инфо»**

Иваново

2019 год

1. Сведения об Удостоверяющем центре

**Общество с ограниченной ответственностью ООО Компания «Сервис ТВ-Инфо»,** именуемое в дельнейшем **«Удостоверяющий центр**», зарегистрировано на территории Российской Федерации в городе Иваново. Свидетельство о регистрации № 5429, серия 368, дата регистрации 22 ноября 2001г., выдано Регистрационной палатой Администрации г.Иваново. Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1033700056048 от 23.01.2003г.

Удостоверяющий центр имеет повышенную безопасность осуществляемой деятельности, связанной с использованием электронной подписи, созданной на основе выданного удостоверяющим центром сертификата.

Удостоверяющий центр в качестве профессионального участника рынка услуг по изготовлению и выдаче сертификатов ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании:

1. **Лицензия УФСБ России Ивановской области ЛЗС № 004824 Рег. № 722 Н от 17 ноября 2014 г. на осуществление следующих видов деятельности: разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляются для обеспечения собственных нужд юридическими лицами или индивидуальными предпринимателями).**

**Реквизиты ООО Компания «Сервис ТВ-Инфо»:**

Полное наименование: Общество с ограниченной ответственностью Компания «Сервис ТВ-Инфо»

 Юридический адрес: 153003, г. Иваново, ул. Парижской Коммуны, д. 16, офис 428

 Фактический адрес: 153003, г. Иваново, ул. Парижской Коммуны, д. 16, офис 428

**Банковские реквизиты** (наименование банка, БИК, ИНН, р/с, к/с):

 ИНН 3730011113 КПП 370201001 ОГРН 1033700056048

Банковские реквизиты: Ивановский РФ ОАО «РОССЕЛЬХОЗБАНК»

Р/счет 40702810938000000924 К/счет 30101810300000000780

БИК 042406780

 **Контактные телефоны, адрес электронной почты:**

Телефон: +7(4932)930909 Е-mail: edo@stv.indi.ru

1. Термины и определения

**Электронная подпись (ЭП)** - 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.

**Сертификат ключа проверки электронной подписи (СКПЭП)** - 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** (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган).

**Владелец сертификата ключа проверки электронной подписи** - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

**Ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи.

**Ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

**Удостоверяющий центр (УЦ)** - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

**Аккредитация удостоверяющего центра** - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

**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;

**Средства удостоверяющего центра** - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

**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.

**Участники электронного взаимодействия** - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

**Корпоративная информационная система** - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

**Информационная система общего пользования** - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

**Вручение сертификата ключа проверки электронной подписи** - передача доверенным лицом удостоверяющего центра, изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

1. Общие положения

3.1. Сведения об Удостоверяющем Центре

3.1.1. Удостоверяющий Центр ООО «Компания «Сервис ТВ-Инфо» находится по адресу 153003, Россия, г. Иваново, ул. Парижской Коммуны, 16. График работы: с Понедельника по Пятницу, с 9:00 до 18:00, без перерыва. Суббота и Воскресенье – выходной.

3.1.2 Справочный телефон: +7 (4932) 93-09-09. Адрес сайта: [www.сервиств.рф](http://www.сервиств.рф). Электронная почта: edo@stv.indi.ru

3.1.3 Заявители могут получить информацию по вопросам предоставления услуг Удостоверяющего центра путем обращения в свободной письменной, либо устной форме по указанным контактным данным.

3.2 Предмет Регламента

3.2.1. Регламент Удостоверяющего центра ООО КОМПАНИЯ «СЕРВИС ТВ-ИНФО», именуемый в дальнейшем «Регламент», основан и учитывает положения типового Регламента (ЖТЯИ.00078 01 90 06) Удостоверяющего центра организации, эксплуатирующей Программно-аппаратный комплекс (ПАК) «Удостоверяющий центра «КриптоПро УЦ» версии 2.0 (далее «КриптоПро УЦ»), входящего в комплект эксплуатационной документации «КриптоПро УЦ» (далее типовой Регламент), учитывает положения действующего законодательства Российской Федерации предусмотренные Федеральным законом 63-ФЗ об электронной подписи от 06.04.2011 года и устанавливает общий порядок и условия предоставления удостоверяющим центром услуг по изготовлению сертификатов ключей проверки электронной подписи и дополнительных услуг, связанных с управлением сертификатами ключей проверки электронной подписи.

3.2.2. Настоящий Регламент является договором присоединения на основании статьи 428
Гражданского кодекса РФ. Настоящий Регламент 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.

3.2.3. Права и обязанности сторон по настоящему Регламенту, а также вопросы, не урегулированные настоящим документом, регламентируются действующим законодательством Российской Федерации и типовым Регламентом «КриптоПро УЦ».

3.2.4. Настоящий Регламент размещен в электронной форме по адресу: <http://www.stv-it.ru/reglament>

3.2. Толкование Регламента

3.2.1. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

3.3. Изменение (дополнение) Регламента

3.3.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

3.3.2. Уведомление абонентов УЦ о внесении изменений (дополнений) в Регламент
осуществляется удостоверяющим центром путем размещения очередной редакции Регламента,
включающей указанные изменения (дополнения) на сайте удостоверяющего центра по адресу -<http://www.stv-it.ru/reglament>

3.4. Присоединение к Регламенту

* + 1. Фактом присоединения Пользователя УЦ к настоящему Регламенту является

наиболее ранний из моментов:

* предоставление Пользователем УЦ документов, необходимых для выпуска сертификата,
* оплата счета,
* присоединение к Регламенту, выраженное посредством КЭП.

3.4.2 С момента выполнения одного из требований, указанных в п. 4.3.1. Пользователь УЦ считается присоединившемся к Регламенту и является Стороной Регламента.

3.4.3 С момента присоединения Пользователя УЦ к настоящему Регламенту, Пользователь УЦ полностью и безоговорочно соглашается со всеми условиями настоящего Регламента приложений к нему.

3.4.4 Пользователь УЦ, присоединившийся к настоящему Регламенту, самостоятельно отслеживает изменения (дополнения), вносимые в настоящий Регламент в виде его новой редакции, путем самостоятельного ознакомления с текстом Регламента на сайт удостоверяющего центра по адресу: <http://www.stv-it.ru/reglament>

* 1. **Стоимость услуг Удостоверяющего центра.**

Удостоверяющий Центр оказывает свои услуги на коммерческой основе. Информация о стоимости услуг Удостоверяющего центра, сроках и порядке расчетов за оказание услуг Удостоверяющего центра указаны на сайте удостоверяющего центра по адресу: http://stv-it.ru/prays-list\_uc.

* 1. **Область применения Регламента.**

Настоящий Регламент 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. Перечень функций (оказываемых услуг) Удостоверяющего Центра
	1. **Назначение Удостоверяющего центра.**

УЦ предназначен для обеспечения участников корпоративных информационных систем

средствами и спецификациями для использования сертификатов ключей проверки ЭП 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.
	1. **Услуги Удостоверяющего центра.**

В процессе своей деятельности УЦ предоставляет потребителям или Пользователям УЦ

следующие виды услуг:

* внесение в Реестр УЦ регистрационной информации о Пользователях УЦ;
* изготовление СКПЭП Пользователей УЦ в электронной форме;
* изготовление копий сертификатов ключей проверки ЭП Пользователей УЦ на бумажных
* носителях;
* формирование ключей ЭП и ключей проверки ЭП по обращениям Пользователей УЦ с
* записью их на ключевой носитель;
* ведение Реестра изготовленных СКПЭП Пользователей УЦ;
* предоставление СКПЭП в электронной форме, находящихся в Реестре изготовленных
* сертификатов, по запросам Пользователей УЦ;
* аннулирование (отзыв) СКПЭП по обращениям владельцев СКПЭП;
* предоставление Пользователям УЦ сведений об аннулированных СКПЭП;
* подтверждение подлинности электронных подписей в документах, представленных в
* электронной форме, по обращениям Пользователей УЦ;
* подтверждение подлинности электронных подписей Уполномоченных лиц УЦ в
* изготовленных ими СКПЭП по обращениям Пользователей УЦ;
* распространение средств электронной подписи по обращениям Пользователей УЦ.
	1. **Пользователи Удостоверяющего центра.**

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;

Физическое лицо может представлять другое лицо при наличии соответствующей

Доверенности.

* 1. **Разрешение споров**

Сторонами в споре, в случае его возникновения, считаются УЦ и Пользователь УЦ.

Стороны принимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путём переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе переговоров, рассматриваются в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

* 1. **Ответственность**

УЦ не несёт никакой ответственности в случае нарушения Пользователями УЦ положений настоящего Регламента.

* 1. **Прекращение деятельности**

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

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

* 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 квалифицированных сертификатов;
* передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

4.Деятельность Удостоверяющего центра

1. Открытый перечень услуг, оказываемых Удостоверяющим центром в соответствии с настоящим Регламентом:
* создание сертификатов ключей проверки электронных подписей и выдача такие сертификаты лицам, обратившимся за их получением (Пользователям УЦ);
* установление сроков действия сертификатов ключей проверки электронных подписей;
* аннулирование выданных удостоверяющим центром сертификатов ключей проверки электронных подписей;
* ведение Реестра выданных и аннулированных этим Удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов);
* создание по обращениям Пользователей УЦ ключи электронных подписей и ключи проверки электронных подписей;
* проверка уникальности ключей проверки электронных подписей в Реестре сертификатов;
* проверка электронных подписей;
* выдача по обращению Пользователя УЦ средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверябшим центром);
* осуществление иной деятельности, связанной с использованием электронной подписи.

5.Вознаграждение удостоверяющего центра

5.1. Удостоверяющий Центр осуществляет свою деятельность на возмездной основе.

5.2. Вознаграждение Удостоверяющего центра по настоящему Регламенту устанавливается в соответствии с прейскурантом на услуги Удостоверяющего центра (<http://stv-it.ru/prays-list_uc>).

6. Предоставление информации

6.1. Сторона, присоединившаяся к Регламенту, предоставляет в удостоверяющий центр следующие сведения и копии документов, их подтверждающие:

6.1.1. Для юридических лиц:

* Основной государственный регистрационный номер заявителя.
* Номер свидетельства о постановке на налоговый учет в налоговом органе заявителя – иностранной организации (в том числе, филиалов, представительств и иных обособленных подразделений) или идентификационный номер налогоплательщика заявителя – иностранной организации.
* Паспорт владельца сертификата.
* Паспорт получателя сертификата.
* СНИЛС владельца сертификата, оригинал или копия, заверенная Клиентом (Юридическим лицом).
* Доверенность, подтверждающая полномочия владельца сертификата ключа подписи (в случае, если владелец сертификата не имеет права действовать от лица юридического лица без доверенности).
* Доверенность на получение сертификата ключа подписи (в случае, если сертификат получает сотрудник организации, не имеющий право действовать без доверенности).

6.1.2. Для индивидуальных предпринимателей:

* Основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя, оригинал или копия, заверенная нотариально либо Клиентом (ИП при наличии печати).
* Паспорт владельца сертификата.
* Паспорт получателя сертификата.
* СНИЛС владельца сертификата, оригинал или копия, заверенная Клиентом (ИП при наличии печати).
* Доверенность, подтверждающая полномочия владельца сертификата ключа электронной подписи (в случае, если владелец сертификата не имеет права действовать от лица индивидуального предпринимателя без доверенности).
* Доверенность на получение сертификата ключа проверки подписи (в случае, если сертификат получает не Индивидуальный предприниматель).

6.1.3. Для физических лиц:

* Паспорт владельца сертификата.
* СНИЛС владельца сертификата.
* Идентификационный номер налогоплательщика заявителя.
* Доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц.

6.2. Удостоверяющий центр вносит сведения в сертификат Пользователя УЦ при их полном совпадении с данными, указанными в Едином государственном реестре юридических лиц (далее – ЕГРЮЛ) и Едином государственном реестре индивидуальных предпринимателей (далее ЕГРИП).

6.3 Удостоверяющий центр оставляет за собой право запросить у стороны, присоединившейся к Регламенту, дополнительные документы, в случае предусмотренного законодательством установления операторами государственных, муниципальных информационных систем общего пользования дополнительных требований к сертификатам ключей проверки электронной подписи пользователей соответствующих информационных сетей для обеспечения информационной безопасности, а также иные документы, подтверждающие сведения, включаемые в сертификат Пользователя УЦ пунктом 8 части 2 статьи 17 Федерального закона от 06.04.2011г. № 63-ФЗ «Об электронной подписи» (в случае необходимости).

6.4 В момент выдачи ЭП в офисе Удостоверяющего центра ведется видео (фотофиксация) получателя ЭП.

**6.5 Порядок установления личности заявителя:**

6.5.1 Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность – паспарту гражданина Российской Федерации.

6.5.2 Личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или иному документу, удостоверяющему личность гражданина иностранного государства.

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

6.5.4 Получатель электронной подписи должен предоставить оригинал документа, удостоверяющего личность.

Документами, удостоверяющими личность гражданина РФ на территории РФ являются:

* Паспорт гражданина РФ, удостоверяющий личность гражданина РФ на территории РФ, действует на территории РФ с 01 октября 1997 года.
* Паспорт моряка (с 2014 года – удостоверение личности моряка) является документом, удостоверяющим личность его владельца как за границей, так и в пределах РФ.
* Свидетельство о рождении является документом, удостоверяющим личность лиц (граждан РФ), не достигших 14-летнего возраста.
* Удостоверение личности военнослужащего РФ является документом, удостоверяющим личности и правовое положение военнослужащего РФ.
* Военный билет является документом, удостоверяющим личность солдат, матросов, сержантов и старшин, проходящих военную службу по призыву или контракту, а также курсантов военных образовательных учреждений профессионального образования на время их обучения.
* Временное удостоверение личности гражданина РФ по форме №2-П – документ, удостоверяющий личность ограниченного срока действия (для утративших паспорт граждан, а также граждан, в отношении которых до выдачи паспорта проводится дополнительная проверка). Временное удостоверение выдается на срок, указанный в этом документе.
* Служебное удостоверение работника прокуратуры.

Документы, удостоверяющие личность иностранных граждан на территории РФ:

* Паспорт иностранного гражданина (национальный паспорт или национальный заграничный паспорт) или иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина – для иностранных граждан, если они постоянно проживают на территории РФ.
* Дипломатический паспорт иностранного гражданина является документом, удостоверяющим личность для иностранных граждан, временно пребывающих и проживающих на территории РФ.
* Документ, выданный иностранным государством и признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность лица без гражданства.
* Иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина или лице без гражданства.
* Разрешение на временное проживание является документом, удостоверяющим личность иностранного гражданина или лице без гражданства (оформленное в виде документа установленной формы, выдаваемого в РФ лицу без гражданства, не имеющему документа, удостоверяющего личность). Данный документ подтверждает право иностранного гражданина или лица без гражданства временно проживать в Российской Федерации до получения вида на жительство.
* Вид на жительство в РФ является документом, удостоверяющим личность лица без гражданства, подтверждающим его право на постоянное проживание в РФ.
* Удостоверение беженца или свидетельство о рассмотрении ходатайства о признании беженцем на территории РФ является документом, удостоверяющим личность лица (иностранного гражданина или лица без гражданства), ходатайствующего о признании беженцем (статьи 4, 7 Федерального закона от 19.02.1993 №4528-1 «О беженцах»).

Все документы на иностранном языке должны быть апостилированы в консульстве (посольстве) РФ за границей (на территории того государства, где эти документы выданы), либо в консульстве (посольстве) иностранного государства (выдавшего документы, удостоверяющие личность) на территории РФ и иметь заверенный перевод ан русский язык.

6.5.5 Требования к паспорту получателя:

* Паспорт гражданина РФ не должен быть просрочен, паспорт меняется в возрасте 20 и 45 лет.
* Документ не должен быть поврежден или испорчен.
* Данные в документе должны совпадать с данными, указанными в доверенности на получение ЭП.

7. Права и обязанности сторон

7.1. Удостоверяющий центр обязан:

1. 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.
2. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
3. 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.
4. Обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.
5. Нести ответственность в соответствии с законодательством Российской Федерации за вред, причиненный по его вине третьим лицам.
6. Обеспечить любому лицу безвозмездный доступ с использованием информационно-коммуникационных сетей к выданным Удостоверяющим центром квалифицированных сертификатов и к актуальному списку аннулированных квалифицированных сертификатов в любое время в течение срока деятельности этого Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными актами.

 7.1.7 Вносить в сертификаты только достоверную и актуальную информацию,

подтвержденную соответствующими документами.

 7.1.8 Производить регистрацию СКПЭП в единой системе идентификации и

аутентификации в соответствии с пунктом 5 статьи 18 Федерального закона «Об

электронной подписи».

 7.1.9 По желанию лица, которому выдан квалифицированный сертификат, безвозмездно

осуществить регистрацию указанного лица в единой системе идентификации и

аутентификации.

 7.1.10 Отказать заявителю в создании СКПЭП в случае отрицательного результата проверки

в реестре сертификатов уникальности ключа проверки электронной подписи, указанного

заявителем для получения СКПЭП.

 7.1.11 Использовать ключи ЭП Удостоверяющего центра только для подписи издаваемых

им СКПЭП и списков отозванных сертификатов.

 7.1.12 Изготовить ключ ЭП и ключ проверки ЭП зарегистрированному Пользователю УЦ с

использованием средств электронной подписи, сертифицированных в соответствии с

действующим законодательством Российской Федерации.

 7.1.13 Обеспечить сохранение в тайне изготовленного ключа ЭП в пределах средств,

находящихся в зоне ответственности Удостоверяющего центра.

 7.1.14 Записать ключи на отчуждаемый магнитный носитель, в соответствии с

требованиями по эксплуатации программного и/или аппаратного средства, выполняющего

процедуру генерации ключей.

 7.1.15 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.

 7.1.16 Обеспечить уникальность регистрационных (серийных) номеров изготавливаемых

СКПЭП Пользователей УЦ.

 7.1.17 Обеспечить уникальность значений ключей проверки ЭП в изготовленных СКПЭП

Пользователей УЦ.

 7.1.18 Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса

г. Москва. Удостоверяющий центр обязан синхронизировать по времени все свои

программные и технические средства обеспечения деятельности.

 7.1.19 Обеспечить регистрацию заявителя в Удостоверяющем центре в соответствии с

порядком, определенным в настоящем Регламенте.

 7.1.20 Аннулировать (отозвать) СКПЭП Пользователя УЦ по соответствующему

заявлению на аннулирование (отзыв) СКПЭП, в соответствии с порядком, определенным в

настоящем Регламенте.

 7.1.21 Аннулировать (отозвать) СКПЭП Пользователя УЦ в случае компрометации ключа

ЭП уполномоченного лица Удостоверяющего центра, с использованием которого был

издан СКПЭП.

 7.1.22 Публиковать актуальный список отозванных сертификатов на сетевом ресурсе http://stv-it.ru/ и обеспечить его круглосуточную доступность. Данные об адресе распространения списка

отозванных сертификатов содержатся в СКПЭП.

7.2. Удостоверяющий центр имеет право:

1. Отказать в изготовлении сертификата ключа проверки электронной подписи Пользователя УЦ в случае ненадлежащего оформления заявления на изготовление сертификата ключа подписи и/или в случае непредставления/предоставления документов не в полном объеме, и/или подлинность которых вызывает сомнение.
2. Отказать в изготовлении сертификата ключа подписи Пользователю УЦ в случае, если использованное Пользователем УЦ для формирования запроса на сертификат ключа проверки электронной подписи средство криптографической защиты информации не поддерживается Удостоверяющим Центром.
3. Отказать в изготовлении сертификата ключа подписи Пользователю УЦ в случае невыполнения Пользователем УЦ обязанностей, установленных Федеральным законом №63-ФЗ от 06 апреля 2011 года, принимаемыми в соответствии с ним нормативными правовыми актами, а так же Регламентом УЦ.
4. Отказать в изготовлении СКПЭП, если предоставленные Заявителем сведения не прошли проверку в соответствии с п.2.2, 2.3 ст.18 Федерального закона №63-ФЗ от 06 апреля 2011 года.
5. Отказать в отзыве сертификата в случае ненадлежащего оформления заявления на отзыв сертификата ключа подписи и в случае непредставления/предоставления документов не в полном объеме и/или подлинность которых вызывает сомнение.
6. Отказать Пользователю УЦ в исполнении услуги удаленного отзыва сертификата в случае невозможности аутентификации Пользователя УЦ.
7. Отказать Пользователю УЦ в изготовлении сертификата ключа проверки подписи при расхождении данных, предоставленных Заявителем, с данными, указанными в ЕГРЮЛ и ЕГРИП.
8. Отозвать сертификат в случае установленного факта компрометации соответствующего закрытого ключа, с уведомлением Владельца отозванного сертификата ключа подписи.

7.2.9. УЦ вправе выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе.

 7.2.10 Отказать в отзыве СКПЭП в случае, если истек установленный срок действия ключа

ЭП. соответствующего этому СКПЭП.

 7.2.11 Отказать в изготовлении СКПЭП Абонента УЦ в случае ненадлежащего оформления

заявления на изготовление СКПЭП.

 7.2.12 Отказать в аннулировании (отзыве) СКПЭП Абонента УЦ в случае ненадлежащего

оформления соответствующего заявления на аннулирование СКПЭП (отзыв).

 7.2.13 Отказать в аннулировании (отзыве) СКПЭП Абонента УЦ в случае, если истек

установленный срок действия закрытого ключа, соответствующего СКПЭП.

 7.2.14 В одностороннем порядке аннулировать (отозвать) СКПЭП Абонента УЦ с

обязательным уведомлением владельца аннулированного (отозванного) СКПЭП и

указанием обоснованных причин.

* 1. Владелец сертификата ключа проверки электронной подписи обязан:

 7.3.1. Обеспечить конфиденциальность ключа электронной подписи. Не использовать ключ электронной подписи и немедленно обратиться в аккредитованный удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;

7.3.2. Использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).

7.3.3 Извещать Удостоверяющий центр обо всех изменениях в документах, перечисленных в п.6 настоящего Регламента.

7.3.4. Самостоятельно нести ответственность, установленную действующим законодательством Российской Федерации перед третьими лицами, а также нести риск причинения убытков из-за несоблюдения требований, изложенных в пп. 7.3.1, 7.3.2 настоящего Регламента.

7.3.5 В случае увольнения или смены должности сотрудника, на которого была оформлена ЭП, выполнить действия в соответствии с пп. 10.3 и 10.4 настоящего Регламента. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявлении на прекращение действия которого направлено в УЦ.

7.3.6. Применять средства квалифицированной электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство электронной подписи.

7.3.7. Перед началом работы с носителями ключевой информации проверить штатное функционирование антивирусного программного обеспечения, убедиться в наличии и, при необходимости, обеспечить своевременную установку обновлений операционной системы и прикладных программ.

7.3.8. Принять меры по исключению несанкционированного доступа в помещения посторонних лиц, в которых размещены аппаратные средства с установленным средством квалифицированной подписи.

7.3.9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированной электронной подписи и ключей их проверки средства электронной подписи, сертифицированные в соответствии с правилами, установленными действующим законодательством РФ.

7.3.10. Получить в точке выдачи УЦ сертификат в течение 5 дней с момента оплаты и предоставления необходимых документов. В случае нарушения Пользователем УЦ настоящего пункта денежные средства не возвращаются.

7.4. Владелец сертификата ключа проверки электронной подписи имеет право:

7.4.1 Получить копию сертификата ключа проверки электронной подписи на бумажном носителе.

7.4.2 Права лиц, не зарегистрированных в УЦ:

Эту группу Пользователей УЦ 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:

* обращаться в УЦ с целью получения (приобретения) средств электронной подписи;

7.4.3 Права лиц, зарегистрированных в УЦ.

Эту группу Пользователей УЦ 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 СКПЭП;
* пользоваться предоставляемыми УЦ программными средствами для получения и

установки на своё рабочее место изготовленных СКПЭП;

* обращаться в УЦ для аннулирования (отзыва) СКПЭП, в течение срока действия

соответствующих ключей ЭП либо СКПЭП.

7.4.4 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 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.

7.5. Владельцу квалифицированного сертификата ключа проверки электронной подписи запрещается:

7.5.1 Оставлять без контроля аппаратные средства, на которых эксплуатируются средства электронной подписи.

7.5.2 Оставлять без контроля носители ключевой информации.

7.5.3 Сообщать PIN – код к ключевому носителю кому бы то ни было.

7.5.4 Вносить какие-либо изменения в программное обеспечение средств электронной подписи, разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации.

7.5.4 Записывать на ключевые носители постороннюю информацию.

7.5.6 Обрабатывать на аппаратных средствах, оснащенных средствами квалифицированной электронной подписи, информацию, содержащую государственную тайну.

7.5.7 Передавать электронную подпись третьим лицам.

7.6. Порядок оказания услуг Удостоверяющим центром:

7.6.1. Все изменения в стандартную форму договора на оказание услуг Удостоверяющим центром вносятся путем протокола разногласий и протокола согласования разногласий.

7.6.2. Оплата услуг по выпуску сертификата осуществляет на основании выставленного счета авансовым платежом в размере 100% (сто процентов) стоимости оказываемых услуг.

7.6.3. Срок изготовления сертификата составляет 5 (пять) рабочих дней с момента осуществления следующих действий в совокупности:

- предоставления всех документов, необходимых для выпуска сертификата;

- зачисления денежных средств на расчетный счет УЦ.

7.6.4. Разъяснения касательно деятельности и порядка оказания услуг Удостоверяющим центров может получить любое лицо при подаче соответствующего запроса, оформленного надлежащим образом, путем направления его на почтовый адрес УЦ или по адресу электронной почты, указанной в п.1 настоящего Регламента.

7.6.5 В целях ознакомления с полным текстом изменений и дополнений настоящего Регламента владельцы сертификатов обязаны не реже одного раза в 10 календарных дней обращаться на официальный сайт УЦ по адресу: [**http://www.stv-it.ru/reglament**](http://www.stv-it.ru/reglament)

8. Ответственность сторон

8.1. Удостоверяющий центр несет имущественную ответственность, установленную в соответствии с действующим законодательством Российской Федерации.

8.2 Удостоверяющий центр не несет ответственность за ущерб, понесенный лицом в результате доверия к сертификату, если удостоверяющий центр выполнил все требования Федерального закона №63-ФЗ от 06 апреля 2011г. и соглашения с владельцем сертификата.

8.3. Удостоверяющий центр не несет ответственность за неисполнение или ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях и других документах Пользователя УЦ или стороны, присоединившейся к Регламенту.

8.4 Удостоверяющий центр несет ответственность за сохранение конфиденциальной информации.

9. Конфиденциальность информации

9.1. **Типы конфиденциальной информации.**

9.1.1. Закрытый ключ, соответствующий сертификату ключа проверки электронной подписи, является конфиденциальной информацией лица Пользователя УЦ. Удостоверяющий центр не осуществляет хранение закрытых ключей Операторов и Пользователей удостоверяющего центра.

9.1.2. Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, находящаяся в Реестре удостоверяющего центре, не подлежащая непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи,
считается конфиденциальной.

9.2. Типы информации, не являющейся конфиденциальной.

9.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой
информацией.

9.2.2. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

9.2.3. Информация, включаемая в сертификаты ключей подписей и списки отозванных
сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

9.2.4. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

9.3. Исключительные полномочия Удостоверяющего центра.

9.3.1. Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

9.4. Обработка персональных данных пользователей Удостоверяющим центром.

9.4.1 Цель обработки персональных данных Удостоверяющим центром - идентификация и аутентификация субъекта персональных данных в качестве пользователя УЦ, а так же пользователя информационных систем с применением ЭЦП, в которых используются сертификаты ключей подписи Пользователя УЦ.

Обработка персональных данных в удостоверяющем центре осуществляется на основании письменного согласия владельца сертификата ключа проверки электронной подписи.

Пользователь не может быть зарегистрирован в реестре удостоверяющего центра без заключения договора, а также письменного согласия на обработку персональных данных, в порядке, установленном настоящим Регламентом.

9.4.4. Персональные данные, обрабатываемые удостоверяющим центром: фамилия, имя, отчество, паспортные данные, СНИЛС, идентификационный номер налогоплательщика пользователя УЦ.

 В сертификат ключа подписи, изготавливаемый УЦ, вносят фамилию, имя, отчество, идентификационный номер налогоплательщика. По требованию УЦ с согласия пользователя УЦ в сертификат ключа проверки электронной подписи могут быть включены дополнительные
персональные данные.

Персональные данные, вносимые в сертификат ключа проверки электронной подписи, на основании согласия пользователя УЦ относятся к категории общедоступных.

Удостоверяющий центр осуществляет следующие действия с персональными данными: сбор, систематизацию, использование, распространение, хранение и уничтожение персональных данных в соответствии с Федеральным законом от 27.06.2007г. №152-ФЗ «О персональных данных».

Сбор и систематизация персональных данных пользователей УЦ осуществляется в ходе приема установленных удостоверяющим центром форм заявлений от лиц, проходящих процедуру регистрации/перерегистрации в соответствии с настоящим Регламентом.

Полученные персональные данные используются для регистрации пользователей УЦ в реестре удостоверяющего центра и для изготовления сертификатов ключей проверки электронной подписи путем внесения данных в соответствующие поля сертификата ключа проверки электронной подписи.

Список должностных лиц удостоверяющего центра, допущенных к обработке персональных данных пользователя УЦ, утверждается распоряжением руководителя УЦ.

Согласие на обработку персональных данных пользователя УЦ может быть отозвано по письменному заявлению пользователя УЦ (Приложение № 2 настоящего Регламента). При этом сотрудником УЦ производится уничтожение на бумажных носителях. Согласие на обработку персональных данных, содержащихся в сертификатах ключей подписи, не может быть отозвано и действует до принятия решения о прекращении пользования услугами удостоверяющего центра.

10. Порядок осуществления Удостоверяющим центром деятельности по выпуску, отзыву и приостановлению сертификата подписи

УЦ осуществляет регистрацию пользователей УЦ только в том случае, если указанное лицо присоединилось к Регламенту в соответствии с пунктом 3.4 настоящего Регламента.

Ключ ЭП и соответствующий ему ключ проверки ЭП могут быть изготовлены в удостоверяющем центре на специализированном рабочем месте, аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, которые размещены в аттестованных помещениях, доступ в которое ограничен, ключ ЭП, созданный таким образом, записывается Удостоверяющим центром на ключевой носитель, который выдается Пользователю, либо доверенному лицу заявителя по окончании процедуры выдачи Сертификата.

10.1. Регистрация пользователя удостоверяющего центра и изготовление первого сертификата ключа подписи.

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

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

10.1.1. Регистрация пользователя в удостоверяющем центре и изготовление первого сертификата ключа подписи осуществляется на основании заявления на регистрацию при личном прибытии пользователя, проходящего процедуру регистрации или его уполномоченного представителя, действующего на основании доверенности на осуществление регистрации в Удостоверяющем центре, в офис удостоверяющего центра.

Заявление на изготовление сертификата ключа проверки ЭП в бумажной форме представляет собой документ ан бумажном носителе, заверенный собственноручной подписью заявителя.

Заявление содержит данные, установленные 63-ФЗ «Об электронной подписи».

К данному заявлению прилагаются все необходимые документы, которые подтверждают заносимые в квалифицированный сертификат данные.

10.1.2. Предоставление документов на изготовление СКПЭП, указанных в п.6.1 настоящего регламента.

10.1.3 Сотрудник УЦ обязан назначить заявителю время получения сертификата ключа подписи в офисе УЦ.

10.1.4 Сотрудник УЦ/третье лицо выполняет процедуру идентификации лица, проходящего

процедуру регистрации, путем установления личности по паспорту и проверке

подлинности документов.

 10.1.5 Документы на электронных и бумажных носителях выдаются Пользователю УЦ с

соблюдением требований по обеспечению конфиденциальности.

 10.1.6 При получении квалифицированного сертификата заявитель под расписку знакомится

с информацией, содержащейся в квалифицированном сертификате. Заявителю выдается

лист ознакомления с данными СКПЭП, на котором заявитель ставит свою подпись, а

уполномоченное лицо удостоверяющего центра, вручающее сертификат, собственноручной

подписью подтверждает факт ознакомления заявителя с информацией своей, содержащейся

в сертификате. Один экземпляр Листа ознакомления передается заявителю, второй

экземпляр остается в УЦ.

 10.1.7 УЦ может выдать бланк сертификата на бумажном носителе по запросу владельца

СКПЭП, подписанный Уполномоченным лицом УЦ.

 10.1.8 Удостоверяющий центр одновременно с выдачей сертификата подписи выдает его

владельцу правила использования СКЗИ и ЭП.

 10.1.9 Сотрудник УЦ на основе предоставленных заявительных документов, а также

установления личности Пользователя, на специализированном рабочем месте осуществляет

изготовление ключей, изготовленные ключи записывает на ключевой носитель.

 10.1.10 Ключевой носитель должен удовлетворять следующим требованиям:

* входить в перечень разрешенных типов носителей, указанных в эксплуатационной

документации к СКЗИ, на котором формируется ключ ЭП и соответствующий ему ключ

проверки ЭП;

* иметь тип устройства, входящий в перечень, определяемый Службой безопасности УЦ;
* быть проинициализированным (отформатированным);
* не содержать никакой информации, за исключением данных инициализации.

Допускается не форматировать носитель, если на него записан действующий ключ

Пользователя УЦ (владельца сертификата), обратившегося за новым сертификатом.

Ключевые носители, не удовлетворяющие указанным требованиям, для записи ключевой

информации не принимаются.

10.1.11 Ключевой носитель, содержащий изготовленные ключи, передаётся владельцу

(Заявителю).

10.2. Изготовление сертификата ключа подписи.

Изготовление сертификата ключа подписи Пользователя УЦ осуществляется при плановой и внеплановой смене ключей подписи Пользователя УЦ.

10.2.1 Внеплановая смена ключей осуществляется Пользователем УЦ в следующих случаях:

* Компрометация закрытого ключа пользователя УЦ (утеря, кража и пр.).
* Компрометация закрытого ключа уполномоченного лица УЦ.
* Смена уполномоченного лица.
* Смена реквизитов владельца.
* Поломка ключевого носителя.
* Ошибки в реквизитах или применениях.

10.2.2 Изготовление сертификата ключа проверки электронной подписи Пользователя УЦ при внеплановой смене производится в соответствии с п.10.1 настоящего Регламента.

10.3. Отзыв сертификата.

10.3.1. Удостоверяющий центр отзывает сертификат ключа проверки электронной подписи Пользователя УЦ в следующих случаях:

10.3.1.1. При истечении срока его действия.

10.3.1.2. По заявлению в письменной форме владельца сертификата ключа в случае:

* Смены уполномоченного лица.
* Смены реквизитов владельца.
* Поломки ключевого носителя.
* Утери, кражи и иной компрометации ключа.
* Ошибки в реквизитах или применениях.

10.3.1.3. В случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам в порядке, установленном Федеральным законом от 06.04.2011г. № 63-ФЗ «Об электронной подписи».

10.3.1.4. Если не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в сертификате.

10.3.1.5. Если установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи.

10.3.1.6. В случае вступления в силу решения суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

10.3.2 В случае истечения полномочий УЦ имеет право отозвать сертификат самостоятельно. Без уведомления владельца сертификата.

10.3.3. Заявление на отзыв сертификата ключа подписи может подаваться в Удостоверяющий центр в бумажной форме (при личном прибытии Пользователя УЦ в офис удостоверяющего центра) либо почтовой или курьерской доставкой с обязательным нотариальным удостоверением подписи заявителя.

10.3.4. В случае отзыва сертификата ключа подписи, Удостоверяющий центр в течение одного рабочего дня оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени отзыва сертификата.

10.3.5 Срок внесения информации об отзыве 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.

**10.4. Уничтожение криптоключей.**

10.4.1 Уничтожение криптоключей (исходной ключевой информации) производится путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования) согласно технической документации на используемый ключевой носитель.

10.4.2 Криптоключи уничтожаются пользователями СКЗИ с записью в соответствующих журналах поэкземплярного учета.

**10.5. Ведение реестра сертификатов.**

Ведение реестра квалифицированных сертификатов включает B себя:

* Внесение изменений B реестр квалифицированных сертификатов в случае изменения сведений.
* Внесение в реестр квалифицированных сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

Информация, внесенная B реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности аккредитованного удостоверяющего центра.

Реестр квалифицированных сертификатов состоит из следующих разделов:

* Квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам, индивидуальным предпринимателям, физическим лицам.
* Аннулированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам, индивидуальным предпринимателям, физическим лицам.

10.5.1. Раздел «квалифицированные сертификаты ключей проверки электронной подписи,

выданные физическим лицам» содержит следующие обязательные поля:

* Уникальный номер квалифицированного сертификата.
* Даты начала и окончания действия квалифицированного сертификата.
* Фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата.
* Реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата (номер, серия, дата выдачи).
* Страховой номер индивидуального лицевого счета владельца квалифицированного сертификата.
* Иная информация о владельце квалифицированного сертификата (по требованию заявителя),

10.5.2. Раздел «квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам» содержит следующие обязательные поля:

* Уникальный номер квалифицированного сертификата.
* Даты начала и окончания действия квалифицированного сертификата.
* Наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата.
* Идентификационный номер налогоплательщика владельца квалифицированного сертификата.
* Реквизиты свидетельства о государственной регистрации юридического лица (для юридических

лиц, зарегистрированных на территории Российской Федерации).

* Реквизиты документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц).
* Иная информация о владельце квалифицированного сертификата (по требованию заявителя).

10.5.3. Раздел «аннулированные квалифицированные сертификаты ключей проверки электронной

подписи, выданные физическим лицам» содержит следующие обязательные поля:

* Уникальный номер квалифицированного сертификата.
* Даты начала и окончания действия квалифицированного сертификата.
* Фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата.
* Дата аннулирования квалифицированного сертификата.
* Основание аннулирования квалифицированного сертификата.

10.5.4. Раздел «аннулированные квалифицированные сертификаты ключей проверки электронной подписи, выданные юридическим лицам» содержит следующие обязательные поля:

* Уникальный номер квалифицированного сертификата.
* Даты начала и окончания действия квалифицированного сертификата.
* Наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата.
* Дата аннулирования квалифицированного сертификата.
* Основание аннулирования квалифицированного сертификата.

10.5.5. Аккредитованный удостоверяющий центр обязан обеспечивать актуальность информации,

содержащейся в реестре квалифицированных сертификатов.

10.5.6. Аккредитованный удостоверяющий центр обеспечивает защиту информации,

содержащейся в реестре квалифицированных сертификатов, от неправомерного доступа,

уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока

своей деятельности.

10.5.7. Хранение информации, содержащейся в Реестре, осуществляется в форме, позволяющей

проверить ее целостность и достоверность.

Формирование и ведение единого реестра осуществляется в условиях, обеспечивающих

предотвращение НСД к нему.

10.5.8. Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся

в реестре, формируется его резервная копия.

10.5.9. Информация о прекращении действия квалифицированного сертификата вносится

удостоверяющим центром в соответствующий раздел реестра квалифицированных сертификатов в

течение одного рабочего дня со дня наступления обстоятельств, повлекших за собой прекращение

действия квалифицированного сертификата. Действие квалифицированного сертификата прекращается с момента внесения записи об этом B реестр квалифицированных сертификатов.

**10.6. Структура сертификата ключа проверки ЭП и списков аннулированных сертификатов.**

10.6.1. Структура сертификата ключа проверки ЭП, изготавливаемого Удостоверяющим центром в

электронной форме.

Удостоверяющий центр издает сертификаты ключей проверки ЭП Пользователей УЦ в

электронной форме (далее по тексту раздела - сертификаты) формата Х.509 версии 3.

Структура сертификата соответствует требованиям Приказа ФСБ России от 27.12.2011 г. №795

«Об утверждении требований о форме квалифицированного сертификата ключа проверки

электронной подписи».

Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи может быть

занесено:

1. в поле Subject (идентифицирует владельца сертификата): - Поле Е (Email) - адрес электронной

почты; - Поле Т (Title) - должность представителя ЮЛ, данные которого занесены в сертификат

наряду с наименованием ЮЛ (если владелец сертификата - ЮЛ);

2. расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа)

набор объектных идентификаторов, устанавливающих ограничения на применение

квалифицированной ЭП совместно c сертификатом ключа проверки ЭП (если такие ограничения

установлены);

3. расширение CRL Distribution Point (Точка распространения списка аннулированных

сертификатов) - набор адресов точек распространения списков аннулированных сертификатов;

4. расширение Authority Information Access (Доступ к информации о центре) - адрес размещения

сертификата Уполномоченного лица Удостоверяющего центра;

5. иные поля и расширения по усмотрению Удостоверяющего центра.

10.6.2. Сертификат ключа проверки ЭП на бумажном носителе.

При получении сертификата Клиент должен ознакомиться c информацией, содержащейся в

сертификате. Лист ознакомления с сертификатом ключа проверки ЭП печатается на листе белой

бумаги формата А4, не содержащим средств защиты от копирования и подделки.

10.6.3 Структура списка аннулированных сертификатов, изготавливаемого Удостоверяющим центром в электронной форме.

Удостоверяющий центр издает списки аннулированных сертификатов в электронной форме формата X.509 версии 2.

Описание и содержание формы списка аннулированных сертификатов (CRL) Удостоверяющего центра представлено ниже:

|  |  |  |
| --- | --- | --- |
| **Название**  | **Описание**  | **Содержание** |
| **Базовые поля списка отозванных сертификатов** |
| Version  | Версия  | V2 |
| Issuer  | Издатель СОС (списка отозванных сертификатов)  | Идентификационные данные Удостоверяющего центра. |
| thisUpdate  | Время издания СОС  | дд.мм.гггг чч:мм:сс GMT |
| nextUpdate  | Время, по котороедействителен СОС | дд.мм.гггг чч:мм:сс GMT |

|  |  |  |
| --- | --- | --- |
| revokedCertificates  | Список отозванныхсертификатов | Последовательность элементов следующеговида1.Серийный номер сертификата(CertificateSerialNumber)2.Время обработки заявления нааннулирование (отзыв) сертификата (Time)3.Код причины отзыва сертификата (ResonCode)"0" Не указана"1" Компрометация ключа"2" Компрометация ЦС"3" Изменение принадлежности"4" Сертификат заменен"5" Прекращение работы |
| signatureAlgorithm  | Алгоритм подписи  | ГОСТ Р 34.11/34.10-2001 |
| Issuer Sign  | Подпись издателя СОС  | Подпись издателя в соответствии с ГОСТ Р34.11/34.10-2001 |
| **Расширения списка отозванных сертификатов** |  |  |
| Authority Key Identifier  | Идентификатор ключаиздателя | Идентификатор закрытого ключауполномоченного лица Удостоверяющегоцентра, на котором подписан СОС |
| SzOID\_CertSrv\_CA\_Version | Объектныйидентификаторсертификата издателя | Версия сертификата уполномоченного лицаУдостоверяющего центра |

11. Сроки действия сертификатов ключей подписи

Срок действия сертификата ключа подписи при использовании СКЗИ «КриптоПро CSP» - 1 год и 3 месяца или 3 года (для ключей уполномоченного лица, при условии, что общее время использования ключа ЭП для выполнения целевых функций в течение 3-х лет его действия ограничено 1 годом и 3 месяцами, остальное время ключ ЭП используется только для подписи списков отозванных сертификатов).

Сроки действия сертификата ключа проверки ЭП составляют 16 и 18 лет соответственно.

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

12. Дополнительные положения

12.1. Плановая смена ключей уполномоченного лица удостоверяющего центра.

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) Уполномоченного лица Удостоверяющего центра выполняется в период действия закрытого ключа Уполномоченного лица Удостоверяющего центра. Процедура плановой смены ключей Уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

• Уполномоченное лицо Удостоверяющего центра генерирует новый закрытый и соответствующий ему открытый ключ;

• Уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра. Уведомление пользователей УЦ о проведении плановой смены ключей уполномоченного лица удостоверяющего центра осуществляется посредством публикации информации на официальном сайте удостоверяющего центра по адресу: <http://www.stv-it.ru/>

Старый закрытый ключ уполномоченного лица удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных удостоверяющим центром в период действия старого закрытого ключа уполномоченного лица удостоверяющего центра.

12.2. Внеплановая смена ключа уполномоченного лица удостоверяющего центра.

В случае компрометации закрытого ключа уполномоченного лица удостоверяющего центра сертификат уполномоченного лица удостоверяющего центра отзывается, Пользователи УЦ уведомляются об указанном факте путем публикации информации о компрометации на сайте удостоверяющего центра по адресу: <http://www.stv-it.ru>. Все сертификаты, подписанные с использованием скомпрометированного ключа уполномоченного лица Удостоверяющего центра, считаются аннулированными.

12.3. Компрометация ключа Пользователя УЦ.

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

В случае компрометации или угрозы компрометации закрытого ключа Пользователь Удостоверяющего центра осуществляет отзыв сертификата и внеплановую смену сертификата.

12.4. Прекращение оказания услуг удостоверяющим центром.

Прекращение оказания услуг удостоверяющим центром может быть произведено на основании одностороннего решения одной из Сторон в порядке, установленном законодательством Российской Федерации. Все сертификаты ключей подписи, изготовленные Удостоверяющим центром отзываются.

 12.5. Архивное хранение информации и сведений Удостоверяющим центром.

12.5.1. На основании Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ч.1

ст. 15) «Аккредитованный удостоверяющий центр хранит следующую информацию:

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.

Хранение информации осуществляется в соответствии с ч.1 ст. 15, ч. 7 статьи 13 Федерального

закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

12.5.2. Документы Удостоверяющего центра, подлежащие архивному хранению, являются

документами временного хранения, архив ведется B электронном и бумажном виде. Хранение в

удостоверяющем центре сертификатов ключей подписи Пользователей УЦ осуществляется в

течение всего периода их действия и 3 (три) года после их отзыва или истечения срока их

действия.

12.5.3. Архивному хранению подлежат следующие документы:

* заявление на изготовление сертификата ключа подписи;
* реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
* доверенность на получение ЭП;
* доверенность на полномочного сотрудника;
* бланк СКПЭП (электронный);
* лист ознакомления с данными СКПЭП (бумажный).

12.5.4. Хранение бумажного архива осуществляется B помещении ОКЗ.

* В одно дело группируются Документы одного календарного года.
* На титульном листе указывается период начала ведения дела И окончания.
* Дело должно содержать не более 250 листов, допускается чуть больше, чтобы комплект документов от одного клиента был полным.
* После того, как в папке накоплено 250 листов, документы, составляющие дело, прошиваются в 2 прокола толстой нитью, заверяются подписью сотрудника ОКЗ. На нить приклеивается лист бумаги 10\*5 см, на котором ставится подпись сотрудника ОКЗ с расшифровкой и печать, чтобы половина печати была размещена на приклеенном листе, а половина на основном. На листе должно быть указано:

Прощито, пронумеровано, скреплено печатью и заверено подписью на 250 (двухстах пятидесяти) листах.

Ф.И.О./\_\_\_\_\_\_\_\_\_\_\_\_\_/

 подпись

12.5.5. Электронный архив представляет собой реестр заявок на выпуск/отзыв ЭП с вложенными

цветными сканами или фотоснимками документов, которые согласно п.12.5.3 подлежат хранению в электронном виде.

12.5.6. Уничтожение бумажного архива после истечения срока хранения документов.

Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией,

формируемой из числа сотрудников ОКЗ УЦ и назначаемой приказом руководителя УЦ.

1. Комиссия составляет список архивных дел, по которым истек срок хранения. Список

составляется по шаблону <архив документов клиентов с … по …>

2. Комиссия готовит Акт уничтожения документов.

3. Архивные дела, указанные в акте, уничтожаются полностью путем сжигания или

разрезания (с помощью шредера) на мелкие части, склеивание которых невозможно для

воссоздания документа.

12.6. Обстоятельства непреодолимой силы.

12.6.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих

обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-

мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

12.6.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне

разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства, включая

военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои

функционирования программного обеспечения, пожары, взрывы И иные техногенные катастрофы,

Действия (бездействие) государственных и муниципальных органов, повлекшие невозможность

исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

12.6.3. B случае возникновения форс-мажорных обстоятельств, срок исполнения Сторонами своих

обязательств по настоящему Регламенту отодвигается соразмерно времени, B течение которого

действуют такие обстоятельства.

12.6.4. Сторона, для которой создалась невозможность исполнения своих обязательств по

настоящему Регламенту, должна немедленно известить B письменной форме другую Сторону о

наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а

также представить доказательства существования названных обстоятельств.

12.6.5. Не извещение или несвоевременное извещение о наступлении обстоятельств

непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

12.6.6. B случае, если невозможность полного или частичного исполнения Сторонами какого-либо

обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств

и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем

порядке от дальнейшего исполнения этого обязательства и B этом случае ни одна из Сторон не

вправе требовать возмещения возникших у нее убытков другой Стороной.

12.7. Уничтожение ключевых документов на ключевых носителях.

12.7.1. Неиспользованные или выведенные из действия ключевые документы подлежат

уничтожению пользователем (обладателем конфиденциальной информацией/владельцем

сертификата), на месте.

12.7.2. Ключи на ключевых носителях, срок действия которых истек, уничтожаются

пользователем путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего

ключевые носители могут использоваться для записи на них новой ключевой информации.

12.8. Уничтожение ПАК СКЗИ, дистрибутивов и документации к ним.

12.8.1. Уничтожение экземпляра СКЗИ, установленного на ПЭВМ, производится пользователем

(владельцем СКЗИ) самостоятельно путем стирания программы и ее следов с ПЭВМ B

соответствии с эксплуатационной и технической документацией к СКЗИ. Факт уничтожения

фиксируется в техническом (аппаратном) журнале (типовая форма журнала приведена в

Приложении 3 Инструкции, утвержденной приказом ФАПСИ от 13 июня 2001 года № 152).

12.8.2. Уничтожение дистрибутива СКЗИ осуществляется владельцем дистрибутива

самостоятельно путем нанесения ему неустранимого физического повреждения, исключающего

возможность его использования, а также восстановления. Факт уничтожения фиксируется в

журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним,

ключевых документов обладателя конфиденциальной информации (типовая форма журнала

приведена в Приложении 2 Инструкции, утвержденной приказом ФАПСИ от 13 июня 2001 года

152)

12.9. Меры защиты ключей ЭП

* Ключи ЭП пользователей УЦ должны записываться при их генерации на типы ключевых носителей, которые поддерживаются используемым СКЗИ.
* Ключи ЭП на ключевом носителе защищаются паролем (ПИН-кодом).
* Пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое СКЗИ. 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.

12.10. Информация из сертификата ключа проверки ЭП на бумажном носителе

При получении квалифицированного сертификата заявителем он должен быть ПОД расписку

ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в

квалифицированном сертификате. Пользователю УЦ предоставляется Выписка из СКПЭП (Лист

ознакомления).

13. Порядок исполнения обязанностей Удостоверяющего центра

13.1. 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.

Данная обязанность реализуется посредством предоставления владельцу электронной подписи,

одновременно с самой подписью, правил использования СКЗИ и ЭП, сущность которых сводится

к определению обязанностей владельца сертификата, в том числе по обеспечению режима

конфиденциальности информации.

13.2. Обеспечение актуальности информации в реестре сертификатов и ее защиты от НСД

Режим конфиденциальности является общим требованием в отношении всей сферы применения

электронной подписи, он обеспечивается посредством применения специальных шифровальных

средств, способствующих защите информации от несанкционированного проникновения.

13.3. Ведение реестров и предоставление информации из реестра сертификатов.

УЦ обязан вести Реестр всех изготовленных сертификатов ключей проверки ЭП пользователей УЦ

B течение установленного срока хранения.

Реестр сертификатов ключей проверки ЭП ведётся в электронном виде.

Информация предоставляется безвозмездно. Заявка подается при личном прибытии Пользователя

УЦ в офис удостоверяющего центра, либо почтовой или курьерской доставкой. Выписка из Реестра должна позволять определить действительность сертификатов ключей проверки ЭП пользователей УЦ.

Для получения статуса в заявке необходимо сообщить:

* Серийный номер сертификата.

или

* ИНН заявителя.
* СНИЛС владельца.
* Даты начала и окончания действия квалифицированного сертификата.

13.4. Обеспечение конфиденциальности ключей электронной подписи.

Ключ электронной подписи, соответствующий СКПЭП является конфиденциальной информацией

лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не осуществляет

копирование и хранение ключей электронных подписей Пользователей.

Уничтожение ключей производится согласно пунктам 10.4 и 12.7 настоящего Регламента.

13.5. Осуществление регистрации квалифицированного сертификата в единой системе

идентификации и аутентификации.

При выдаче квалифицированного сертификата аккредитованный 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). При выдаче

квалифицированного сертификата аккредитованный удостоверяющий центр по желанию лица,

которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию

указанного лица в единой системе идентификации и аутентификации.

13.6. Сроки действия ключей Уполномоченных лиц УЦ.

Максимальный срок действия ключа ЭП и сертификата ключа проверки ЭП Уполномоченного

лица УЦ определяются требованиями применяемого СКЗИ.

При использовании СКЗИ «КриптоПро СSР» - 1 год и 3 месяца или 3 года (при условии, что

общее время использования ключа ЭП для выполнения целевых функций B течение 3-х лет его

действия ограничено 1 годом и 3 месяцами, остальное время ключ ЭП используется только для

подписи списков отозванных сертификатов). Сроки действия сертификата ключа проверки ЭП

составляют 16 и 18 лет соответственно.

Начало периода действия ключа ЭП Уполномоченного лица УЦ исчисляется с даты и времени

начала действия соответствующего сертификата ключа проверки ЭП.

13.7. Требования к средствам электронной надписи, использующимся 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 удовлетворяют требованиям

Федерального закона №63-Ф3 «Об электронной подписи» и требованиям Приказа ФСБ РФ от

27.12.2011 r. №796.

13.8. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП пользователей УЦ.

Максимальный срок действия ключа ЭП Пользователя УЦ, соответствующего сертификату ключа

проверки ЭП, владельцем которого он является, определяется требованиями СКЗИ,

использующим 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 СКЗИ, использующим ключ ЭП пользователя, соответствующий указанному

сертификату.

13.9. Меры защиты ключей ЭП.

Ключи ЭП пользователей УЦ должны записываться при их генерации на типы ключевых

носителей, которые поддерживаются используемым СКЗИ.

Ключи ЭП на ключевом носителе защищаются паролем (ПИН-кодом). Пароль (ПИН-код)

формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на

используемое СКЗИ.

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.

14. Обеспечение безопасности

14.1. Инженерно-технические меры защиты информации

14.1.1. Размещение технических средств УЦ Сервера Центра сертификации, Центра регистрации и

телекоммуникационное оборудование размещены в серверном помещении. Остальные технические средства УЦ размещаются в рабочих помещения

УЦ по схеме организации рабочих мест персонала.

14.1.2. Электроснабжение и кондиционирование воздуха.

Сервера Центра сертификации и Центра регистрации 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.

Рабочие и прочие служебные помещения УЦ оборудованы средствами вентиляции и

кондиционирования воздуха в соответствии с санитарно-гигиеническими нормами СНиП,

устанавливаемыми законодательством Российской Федерации.

14.1.3. Пожарная безопасность помещений УЦ обеспечивается в соответствии с нормами и

требованиями СНиП, устанавливаемыми законодательством Российской Федерации.

14.2. Программно-аппаратные меры защиты информации

14.2.1. Организация доступа к техническим средствам УЦ.

Доступ к техническим средствам УЦ, размещенным в серверном помещении, осуществляется с

использованием системы контроля доступа. Организация доступа к техническим средствам УЦ,

размещённых на рабочих местах сотрудников УЦ, возлагается на сотрудников УЦ, ответственных

за эксплуатацию данных технических средств.

14.2.2. Все компоненты УЦ оснащены сертифицированными средствами защиты от НСД. Рабочие

места сотрудников УЦ, на которых эксплуатируются прикладные компоненты УЦ оснащены

сертифицированными средствами защиты от НСД. 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 ПО серверов Центра сертификации и Центра регистрации для

выполнения регламентных работ осуществляется в присутствии сотрудников, отвечающих за

эксплуатацию соответствующего прикладного ПО (Центра сертификации и/или Центра

регистрации).

14.2.2.1. Общий перечень объектов доступа УЦ.

К объектам доступа УЦ относятся:

* технические средства компонент УЦ;
* ПО 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.

14.2.3. Контроль целостности ПО

Контролю целостности подлежат следующие программные компоненты из состава программного

обеспечения, эксплуатируемого УЦ:

* Программные модули средств ЭП 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 ПО до загрузки ОС. Данная система контроля целостности обеспечивается

использованием сертифицированного устройства типа «электронный замок». Контроль

целостности программных модулей средств ЭП и криптографической защиты информации

осуществляется средствами средств ЭП и криптографической защиты информации.

14.2.4. Контроль целостности технических средств.

Контроль целостности технических средств УЦ обеспечивается опечатыванием корпусов

устройств, препятствующим их неконтролируемому вскрытию. Опечатывание устройств

выполняется перед вводом технических средств B эксплуатацию и после выполнения

регламентных работ. Контроль целостности печатей осуществляется B начале каждой рабочей

смены.

14.3. Организационные меры защиты информации.

14.3.1. Предъявляемые требования к персоналу УЦ.

Уполномоченное лицо УЦ имеет высшее профессиональное образование и профессиональную

подготовку в области информационной безопасности, а также стаж работы B этой области более 2

лет.

14.3.2. Профессиональная переподготовка и повышение квалификации персонала Сотрудники УЦ

осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не

реже одного раза в 5 лет.

14.3.3. 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, воскресение, а также дни общенациональных праздников.

14.4. Юридические меры защиты информации.

УЦ имеет разрешение (лицензии) по всем вицам деятельности, связанным с предоставлением

услуг.

Все меры по защите информации B УЦ введены B действие приказами директора ООО Компания «Сервис ТВ-Инфо».

Для обеспечения деятельности УЦ использует средства ЭП и криптографической защиты

информации, сертифицированные в соответствии с действующим законодательством Российской

Федерации.

Исключительные имущественные права на информационные ресурсы УЦ находятся в

собственности УЦ.

15. Политика конфиденциальности

15.1. Типы конфиденциальной информации

Ключ ЭП владельца сертификата ключа проверки ЭП является конфиденциальной

информацией данного Пользователя УЦ.

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.

15.2. 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.

15.3. 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.

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 СКПЭП, 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, B

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 ПО, 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 СКПЭП, с

использованием которого была сформирована ЭП 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 СКПЭП (см.

пункт 6.1 настоящего Регламента). 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 ЭП 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.

17. Список приложений

17.1 Приложение №1. Правила использования средств криптографической защиты информации.

17.2 Приложение №2. Форма заявления об отзыве согласия на обработку персональных данных.

Приложение №1

к Регламенту Удостоверяющего центра ООО КОМПАНИЯ «СЕРВИС ТВ-ИНФО»

Директору ООО Компания «Сервис ТВ-Инфо»

Лепехину Е.П.

153003, город Иваново, улица Парижской Коммуны, дом 16.

Правила использования средств криптографической защиты информации

1. Средства электронной подписи - шифровальные (криптографические) средства (СКЗИ),

используемые для реализации хотя бы одной из следующих функций - создание

электронной подписи, проверка электронной подписи, создание ключа электронной

подписи и ключа проверки, имеющие подтверждение соответствия требованиям,

установленным Федеральным законом 63-ФЗ об электронной подписи от 06.04.2011 г.

СКЗИ и средства ЭП могут использоваться для защиты конфиденциальной информации, не

содержащей сведений, составляющих государственную тайну.

2. Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов,

предназначенная для создания электронной подписи.

3. Для работы с СКЗИ и ключами ЭП привлекаются уполномоченные лица, назначенные

соответствующим приказом руководителя организации. Данные должностные лица,

уполномоченные соответствующим приказом руководителя организации, несут

персональную ответственность за:

 а. Сохранение в тайне конфиденциальной информации, ставшей им известной в

процессе работы с СКЗИ;

 b. Сохранение B тайне содержания ключей ЭП и СКЗИ;

 с. Сохранность носителей ключевой информации и других документов о ключах,

выдаваемых с ключевыми носителями.

4. В организации должны быть обеспечены условия хранения ключевых носителей и

карточки отзыва ключей ЭП, исключающие возможность доступа к ним посторонних лиц,

несанкционированного использования или копирования ключевой информации и паролей

отзыва ключей.

5. Уполномоченные лица несут ответственность за то, чтобы на компьютере, на котором

установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе,

вирусы), которые могут нарушить функционирование программных СКЗИ. При

обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов,

нарушающих работу указанных средств, работа со средствами защиты информации на

данном рабочем месте должна быть прекращена и должны быть организованы мероприятия

по анализу и ликвидации негативных последствий данного нарушения.

6. Организация - обладатель конфиденциальной информации обязана вести журнал

поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним,

ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 года № 152

«Об утверждении Инструкции об организации и обеспечении безопасности хранения,

обработки и передачи по каналам связи с использованием средств криптографической

защиты информации с ограниченным доступом, не содержащей сведений, составляющих

государственную тайну» (Приложение 2). Неиспользованные или выведенные из действия

ключевые документы подлежат уничтожению обладателем конфиденциальной

информацией на месте, путем переформатирования ключевых носителей средствами ПО СКЗИ.

7. Не допускается:

 а. разглашать содержимое носителей ключевой информации или передавать сами

носители лицам, к ним не допущенным, выводить ключевую информацию на

дисплей и принтер;

 b. вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся

штатными процедурами использования ключей (шифрование/расшифровывание

информации, проверка электронной подписи и т.д.), а также в другие ПЭВМ;

 с. записывать на ключевом носителе постороннюю информацию;

 d. вносить какие-либо изменения B СКЗИ и ключ ЭП;

 е. использовать бывшие в работе ключевые носители для записи новой информации

без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

8. Действия B случае компрометации ключей:

 а. Под компрометацией ключей ЭП понимается их утрата (в том числе с их

последующим обнаружением), хищение, разглашение, несанкционированное

копирование, передача их по линии связи в открытом виде, увольнение по любой

причине сотрудника, имеющего Доступ к ключевым носителям или к ключевой

информации на данных носителях, любые другие виды разглашения ключевой

информации, в результате которых ключи ЭП могут стать доступными

несанкционированным лицам и (или) процессам.

 b. Владелец ключа ЭП (уполномоченное лицо) самостоятельно должен определить

факт компрометации ключа ЭП и оценить значение этого события для Пользователя.

Мероприятия по розыску и локализации последствий компрометации

конфиденциальной информации, переданной с использованием СКЗИ, организует и

осуществляет сам владелец.

 с. При компрометации ключа ЭП, владелец ключа должен немедленно поставить в

известность представителей ООО Компания «Сервис ТВ-Инфо» о факте компрометации

(контактная информация размещена на сайте http://stv-it.ru). Информация

о компрометации может передаваться по телефону или непосредственно

представителю Удостоверяющего центра B его офисе. Не позднее 1 часа после

поступления сообщения о компрометации ключа ЭП, сертификат проверки ключа

ЭП будет отозван. Последующая разблокировка отозванного сертификата ключа

проверки ЭП не возможна.

9. Для получения новых ключей уполномоченный представитель организации, у которой

были скомпрометированы ключи, должен обратиться B Удостоверяющий центр, имея при

себе документы, необходимые для выпуска нового ключа ЭП.

Приложение №2

к Регламенту Удостоверяющего центра ООО КОМПАНИЯ «СЕРВИС ТВ-ИНФО»

Директору ООО Компания «Сервис ТВ-Инфо»

Лепехину Е.П.

153003, город Иваново, улица Парижской Коммуны, дом 16.

**Заявление об отзыве согласия на обработку персональных данных владельца сертификата ключа подписи удостоверяющего Центра**

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество)

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

(серия и номер паспорта)

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

(кем и когда выдан)

Прошу с «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года отозвать согласие на обработку персональных данных владельца сертификата ключа подписи.

Я ознакомлен с тем, что Согласие на обработку персональных данных, содержащихся в

сертификатах ключей подписи, не может быть отозвано и действует до принятия решения о

прекращении пользования услугами удостоверяющего центра.

Пользователь УЦ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

 (подпись) (Ф.И.О.)