УДОСТОВЕРЯЮЩИЙ ЦЕНТР www.nwudc.ru

Малоохтинский проспект, д. 68, Санкт-Петербург, 195112
телефон/факс: (812) 578-01-96
e-mail: udc@nwudc.ru

УТВЕРЖДАЮ
Генеральный директор
АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР»

_____С.В. Телелюшкин

РЕГЛАМЕНТ

оказания услуг аккредитованным удостоверяющим центром
АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР»

Редакция 4.2

Санкт-Петербург, 2017

СОДЕРЖАНИЕ

1. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ 4
2. СТАТУС РЕГЛАМЕНТА 5
3. СТОИМОСТЬ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 5
4. ТЕРМИНЫ И СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В РЕГЛАМЕНТЕ 6
5. ОБЩИЕ ПОЛОЖЕНИЯ 8
6. ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ 9
7. ФУНКЦИИ И ЗАДАЧИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 9
8. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ И ЗАЯВИТЕЛЯ 13
9. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ 14
10. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 15
11. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНЕПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 16
12. ПОРЯДОК ПОДКЛЮЧЕНИЯ (РЕГИСТРАЦИИ) ПОЛЬЗОВАТЕЛЕЙ 16
13. ПОРЯДОК ПОДАЧИ ЗАЯВЛЕНИЯ НА СОЗДАНИЕ И ВЫДАЧУ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА 17
14. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ЗАЯВЛЕНИЯ НА СОЗДАНИЕ И ВЫДАЧУ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА 17
15. ПОРЯДОК УСТАНОВЛЕНИЯ ЛИЧНОСТИ ЗАЯВИТЕЛЯ 18
16. ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ЗАПРАШИВАЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ У ЗАЯВИТЕЛЯ ДЛЯ ИЗГОТОВЛЕНИЯ И ВЫДАЧИ СЕРТИФИКАТА, В ТОМ ЧИСЛЕ ДЛЯ УДОСТОВЕРЕНИЯ ЛИЧНОСТИ ЗАЯВИТЕЛЯ, А ТАКЖЕ ТРЕБОВАНИЯ К ТАКИМ ДОКУМЕНТАМ 19
17. ПОРЯДОК СОЗДАНИЯ И ВЫДАЧИ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА 20
18. ПОДТВЕРЖДЕНИЕ ДЕЙСТВИТЕЛЬНОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ, ИСПОЛЬЗОВАННОЙ ДЛЯ ПОДПИСАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ 21

19. ПРОЦЕДУРЫ, ОСУЩЕСТВЛЯЕМЫЕ ПРИ ПРЕКРАЩЕНИИ ДЕЙСТВИЯ И АННУЛИРОВАНИИ СЕРТИФИКАТА 22
20. ПОРЯДОК ВЕДЕНИЯ РЕЕСТРА СЕРТИФИКАТОВ 23
21. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 24
22. СМЕНА КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ВЛАДЕЛЬЦА СЕРТИФИКАТА 26
23. ДЕЙСТВИЯ СТОРОН ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭП 27
24. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ 27
25. ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ СИСТЕМЫ 27
26. ВЗАИМОДЕЙСТВИЕ СТОРОН ПРИ НЕШТАТНЫХ СИТУАЦИЯХ 28
27. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ 28

1. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Акционерное общество «УДОСТОВЕРЯЮЩИЙ ЦЕНТР», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Санкт-Петербург (Свидетельство о регистрации № 171260 выдано Регистрационной палатой Санкт-Петербурга 16 января 2002 года, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1037816019647 от 10 февраля 2003 года).

Удостоверяющий центр АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР» аккредитован в Министерстве связи и массовых коммуникаций Российской Федерации на соответствие требованиям Федерального закона от 06.04.2011 года № 63-ФЗ "Об электронной подписи" (Свидетельство №16 от 19 июля 2012 года).

АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР», в соответствии с законодательством Российской Федерации, имеет все необходимые лицензии и аккредитации, дающие право осуществлять деятельность, определенную настоящим Регламентом, а также выполнять функции аккредитованного Удостоверяющего центра.

Для защиты информации используются средства СКЗИ, а также средства ЭП, позволяющие идентифицировать владельца СКПЭП и установить отсутствие искажения информации. Применяемые средства ЭП и СКЗИ сертифицированы, в порядке, установленном законодательством Российской Федерации.

Реквизиты АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР»:

Полное наименование: Акционерное общество «УДОСТОВЕРЯЮЩИЙ ЦЕНТР»
Сокращенное наименование: АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР»
Адрес места нахождения: 195027, г. Санкт-Петербург, ул. Малыгина, д. 6, литера А
Почтовый адрес: 195112, г. Санкт-Петербург, Малоохтинский пр., д. 68
ИНН/КПП 7806122720 / 780601001
ОГРН: 1037816019647
Код по ОКВЭД: 62.09, 61.10, 61.20, 62.01, 62.02, 62.03, 63.11, 63.11.1, 72.19, 73.20, 74.90, 95.11, 95.12
Код по ОКПО: 57945252
Телефон/Факс: (812) 578-01-96
E-mail: udc@nwudc.ru
Адрес официального сайта в сети Интернет: www.nwudc.ru
График работы: 09.00 – 19.00, кроме выходных и праздничных дней

Обособленное подразделение в г. Москва:
Адрес места нахождения: 107078, Москва, ул. Каланчевская 15 А
Телефон: (495) 783-15-25, 8 (800) 333-01-96
E-mail: 7831525@comita.ru
График работы: 10.00 – 18.00, кроме выходных и праздничных дней

Обособленное подразделение в г. Севастополь:
Адрес места нахождения: 299011, г. Севастополь, ул. Ленина, д. 5
Телефон: (8692) 54-18-19, 8 (800) 333-01-96
E-mail: sev@nwudc.ru
График работы: 09.00 – 18.00, кроме выходных и праздничных дней

2. СТАТУС РЕГЛАМЕНТА

2.1. Настоящий Регламент разработан на основании действующего законодательства Российской Федерации, а также организационно-методических документов АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР», и определяет:

- перечень услуг Удостоверяющего центра, условия и порядок их предоставления;
- устанавливает порядок пользования услугами Удостоверяющего центра, финансовые условия, а также регулирует права и обязанности сторон в рамках договорных отношений;
- порядок организации криптографической защиты информации при обмене электронными документами в автоматизированных информационных системах обмена информацией, в том числе по телекоммуникационным каналам связи в виде юридически значимых электронных документов с использованием электронной подписи;
- порядок управления ключевой информацией (формирование ключей электронной подписи и ключей проверки электронной подписи (ЭП) Пользователей, изготовление квалифицированных сертификатов ключей проверки электронной подписи, учет, хранение, распределение, ввод в действие, смена и уничтожение ключей Пользователей.);
- порядок действий при возникновении конфликтных ситуаций, связанных с применением средств криптографической защиты информации (далее - СКЗИ), средств электронной подписи (далее - ЭП) и сертификатов ключей проверки (далее - СКП) электронной подписи.

2.2. Настоящий Регламент распространяется в форме электронного документа на официальном сайте АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР». Пользователь вправе запросить бумажную копию Регламента, заверенную подписью руководителя и печатью организации.

2.3. Присоединение к настоящему Регламенту осуществляется путем заключения Договора с АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР» и/или акцептом счета, выставленного Удостоверяющим центром. Заключение Договора с УЦ производится на условиях, предусмотренных для договора присоединения в соответствии со ст. 428 Гражданского Кодекса Российской Федерации, т.е. путем присоединения к Регламенту в целом, с учетом условий и оговорок, которые изложены в настоящем Регламенте.

2.4. Внесение изменений (дополнений) в настоящий Регламент производится Удостоверяющим центром в одностороннем порядке.

2.5. Уведомление о внесении изменений (дополнений) в настоящий Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений (дополнений) на официальном сайте Удостоверяющего центра по адресу: www.nwudc.ru.

2.6. В случае противоречия и/или расхождения наименования какого-либо раздела Регламента со смыслом какого-либо пункта в нем содержащегося, доминирующим считается смысл и формулировки каждого конкретного пункта.

3. СТОИМОСТЬ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1. Услуги по созданию и выдаче СКПЭП, выдаче средств электронной подписи, а также по проверке квалифицированных электронных подписей осуществляются Удостоверяющим центром на платной основе. Актуальная информация о стоимости услуг размещается на официальном сайте в сети Интернет. Пользователь так же может получить информацию о стоимости услуг удостоверяющего центра по справочным телефонам, указанным в Разделе 1 настоящего Регламента.

3.2. Оплата услуг производится в безналичной форме на основании счета путем перечисления денежных средств на расчетный счет Удостоверяющего центра.

3.3. Сроки и порядок расчетов за услуги, оказываемые Удостоверяющим центром, регулируются условиями договора между Удостоверяющим центром и Пользователем.

3.4. Услуги Удостоверяющего центра считаются оказанными, если Пользователь не предъявил мотивированный отказ в письменном виде по их качеству и объему в течение 5 (пяти) рабочих дней со дня их оказания, с обязательным предварительным уведомлением Удостоверяющего центра о наличии претензии по телефону, факсимильной связи, электронной почте или с использованием других средств связи.

4. ТЕРМИНЫ И СОКРАЩЕНИЯ, ИСПОЛЬЗУЕМЫЕ В РЕГЛАМЕНТЕ

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона № 63-ФЗ от 06.04.2011г. «Об электронной подписи».

Аутентификация информации – подтверждение подлинности и целостности информации, содержащейся в документе. Аутентификация может осуществляться как на основе структуры и содержания документа или его реквизитов, так и путем реализации криптографических алгоритмов преобразования информации. Доказательная аутентификация информации осуществляется анализом (экспертизой) подписей должностных лиц и печатей на бумажных документах или проверкой правильности ЭП.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

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

Договор – договор, заключенный между Пользователем и АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР». Договор определяет состав, порядок исполнения и стоимость услуг, оказываемых Пользователю Удостоверяющим центром.

Заявитель – лицо, подающее в Удостоверяющий центр заявление на создание и выдачу квалифицированного сертификата ключа проверки электронной подписи и признающее данный Регламент.

Заявление Пользователя – надлежащим образом оформленное заявление Пользователя на изготовление СКПЭП.

Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – СКПЭП, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган).

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи. Ключ ЭП является секретным (закрытым) ключом и хранится Пользователями в тайне. Ключ ЭП используется для формирования ЭП Пользователя и шифрования информации.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее – проверка электронной подписи).

Ключевой носитель – отчуждаемый носитель, содержащий один или несколько ключей ЭП. Вид ключевого носителя устанавливается Удостоверяющим центром, в соответствии с действующим законодательством и/или требованиями информационных систем, в которых используются ключи ЭП и СКПЭП, изготовленные Удостоверяющим центром.

Компрометация ключа – утрата доверия к тому, что используемые ключи электронной подписи (закрытые ключи) недоступны посторонним лицам. К событиям, связанным с компрометацией ключей, относятся (включая, но, не ограничиваясь) следующие события:

- утеря ключевых носителей;
- утеря ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение;
- нарушение целостности печатей на сейфах с ключевыми носителями, если используется процедура опечатывания;
- утеря ключей от сейфов (помещений) в момент нахождения в них ключевых носителей;
- утеря ключей от сейфов (помещений) в момент нахождения в них ключевых носителей с последующим обнаружением;
- доступ посторонних лиц к ключевой информации;
- случаи, когда нельзя достоверно установить причину выхода из строя ключевых носителей (в том числе, когда не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с действующим законодательством Российской Федерации, владельцем информации, а также настоящим Регламентом, и требующая защиты.

Конфликтная ситуация – ситуация, при которой у Пользователей возникает необходимость разрешить вопросы признания или непризнания авторства и/или подлинности электронных документов, обработанных СКЗИ.

Корпоративная информационная система – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Некорректный электронный документ – электронный документ, не прошедший процедуры проверки ЭП, имеющий искажения в тексте сообщения, не позволяющие понять его смысл.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий установленные правила ее получения.

Подтверждение подлинности электронной подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством ЭП, с использованием СКПЭП, принадлежности ЭП в электронном документе владельцу СКПЭП и отсутствия искажений в подписанном данной ЭП электронном документе.

Подтверждение владения ключом электронной подписи – получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

Пользователь – юридическое лицо, индивидуальный предприниматель или физическое лицо, заключившее с договор АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР» и признающее данный Регламент. Пользователь может не являться владельцем квалифицированного сертификата (Заявителем).

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 ЭП владельцу СКПЭП.

Средства криптографической защиты информации (СКЗИ) – шифровальные (криптографические) средства защиты информации конфиденциального характера.

Средства удостоверяющего центра – программные и/или аппаратные средства, используемые для реализации функций удостоверяющего центра;

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.

Реестр аннулированных сертификатов (Список отзыва сертификатов, COC, Certificate Revocation List, CRL) – электронный документ с ЭП уполномоченного лица Удостоверяющего центра, включающий в себя серийные номера отозванных (аннулированных) СКПЭП, и информацию о датах прекращения действия или аннулирования СКПЭП и об основаниях таких прекращения или аннулирования. Формат документа определяется X.509 версии 2. COC (CRL) публикуется на официальном сайте Удостоверяющего центра (www.nwudc.ru).

Удостоверяющий центр – АО «УДОСТОВЕРЯЮЩИЙ ЦЕНТР», осуществляющее функции по созданию и выдаче СКПЭП, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ от 06.04.2011г.

Управление ключами – создание (генерация) ключей (ключевой информации), их хранение, распространение, удаление (уничтожение), учет и применение, а также выдача и отзыв СКПЭП в соответствии с политикой безопасности Удостоверяющего центра.

Целостность информации – обеспечение достоверности и полноты информации и методов её обработки.

Электронный документ (ЭД) – документ, в котором информация представлена в электронно-цифровой форме.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1. Регламент начинает действовать в отношении Пользователя с момента заключения им договора с Удостоверяющим центром и/или оплаты выставленного счета. При обмене электронными документами Пользователи должны руководствоваться положениями настоящего Регламента.

5.2. Используемые во взаимоотношениях между Пользователями электронные документы, заверенные ЭП, являются оригиналами, имеют юридическую силу, подлежат хранению в архиве юридически значимых документов и могут использоваться в качестве доказательств в суде, а также при рассмотрении споров в досудебном порядке.

5.3. Пользователи признают, что использование сертифицированных СКЗИ и средств ЭП, достаточно для обеспечения конфиденциальности информационного взаимодействия Пользователей, а также подтверждения того, что электронный документ:

- исходит от Пользователя, ЭП которого содержится в документе (подтверждение авторства документа);
- не претерпел искажений при информационном взаимодействии (подтверждение целостности и подлинности документа).

5.4. Удостоверяющий центр осуществляет работы по управлению ключами в соответствии с положениями настоящего Регламента, на основании Заявления пользователя и Договора, заключенного с Пользователем.

5.5. В случае нарушения правил использования СКЗИ и/или возникновения конфликтных ситуаций, связанных с подтверждением авторства и/или подлинности электронных документов, заверенных ЭП, или иных конфликтных ситуаций, связанных с использованием ЭП, участники информационного обмена руководствуются Порядком разрешения конфликтных ситуаций, изложенным в настоящем Регламенте, если иное не оговорено в Договоре.

6. ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ

6.1. Удостоверяющий центр использует программные и технические средства генерации ключевой информации в неизменном виде по отношению к сертифицированному эталону. Удостоверяющий центр гарантирует отсутствие привнесенных нерегламентированных процедур скрытого копирования индивидуальной секретной ключевой информации в используемых программных и технических средствах.

6.2. Допускается вместо документов на бумажном носителе оформлять электронные документы с ЭП уполномоченных лиц, если это не запрещено Федеральным законодательством, нормативно-правовыми актами или соглашениями сторон.

6.3. Признание ЭП, созданных в соответствии с нормами иностранного права и международными стандартами осуществляется в соответствии с федеральными законами и нормативно-правовыми актами РФ.

6.4. Пользователь получает доступ к реестру СКПЭП пользователей и реестру аннулированных сертификатов (публикуются на сайте Удостоверяющего центра в Интернете по адресу http://www.nwudc.ru).

Примечание: Удостоверяющий центр принимает все возможные меры, чтобы в кратчайшие сроки внести в СОС СКПЭП недействительных (скомпрометированных) ключей.

6.5. Максимальный срок действия ключей Пользователя, определяется производителем средств ЭП (отражен в эксплуатационно-технической документации). Начало периода действия ключей Пользователя исчисляется с даты и времени начала действия соответствующего им СКПЭП.

7. ФУНКЦИИ И ЗАДАЧИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

7.1. Удостоверяющий центр оказывает следующие услуги:

7.1.1. создает СКПЭП и выдает такие сертификаты лицам, обратившимся за их получением (заявителям);

7.1.2. устанавливает сроки действия СКПЭП;

7.1.3. аннулирует выданные СКПЭП;

7.1.4. выдает по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП заявителем;

7.1.5. ведет реестр выданных и аннулированных СКПЭП (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром СКПЭП, и информацию о датах

прекращения действия или аннулирования СКПЭП и об основаниях таких прекращения или аннулирования;

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

7.1.7. создает по обращениям заявителей ключи ЭП и ключи проверки ЭП;

7.1.8. проверяет уникальность ключей проверки ЭП в реестре сертификатов;

7.1.9. осуществляет по обращениям участников электронного взаимодействия проверку ЭП;

7.1.10. осуществляет иную связанную с использованием ЭП деятельность.

7.2. В рамках исполнения функций, предусмотренных статьями 13 и 15 Федерального закона «Об электронной подписи», Удостоверяющий центр вправе:

7.2.1. запрашивать у заявителя документы для подтверждения информации, содержащейся в заявлении на создание и выдачу сертификата;

7.2.2. с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных заявителем;

7.2.3. запрашивать и получать из государственных информационных ресурсов:

- выписку из единого государственного реестра юридических лиц в отношении заявителя – юридического лица;
- выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя – индивидуального предпринимателя;
- выписку из Единого государственного реестра налогоплательщиков в отношении заявителя – иностранной организации;

7.2.4. запросить у заявителя дополнительные документы, подтверждающие достоверность представленных им сведений, в случае наличия противоречий и/или сомнений между сведениями, представленными заявителем и сведениями, полученными Удостоверяющим центром в соответствии с частью 2.2 статьи 18 Федерального закона «Об электронной подписи»;

7.2.5. не принимать от заявителя документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации;

7.2.6. отказать заявителю в выдаче сертификата в случае невыполнения заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами;

7.2.7. отказать владельцу сертификата в прекращении действия сертификата в случае, если сертификат уже аннулирован или прекратил свое действие по другим основаниям;

7.2.8. без заявления владельца сертификата прекратить действие сертификата в случае наличия у Удостоверяющего центра достоверных сведений о нарушении

конфиденциальности ключа электронной подписи владельца сертификата, а также невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи, а также в случае появления у Удостоверяющего центра достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включенной в данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

7.3. Удостоверяющий центр уведомляет Пользователей о фактах, которые стали ему известны и которые существенным образом могут сказаться на возможности дальнейшего использования СКЗИ и СКПЭП.

7.4. Удостоверяющий центр обязан аннулировать СКПЭП в случае, если:

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

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

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

7.5. Удостоверяющий центр вправе досрочно прекратить действие СКПЭП:

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

7.5.2. если Удостоверяющему центру стало достоверно известно о прекращении действия документа, на основании которого был оформлен СКПЭП;

7.6. Удостоверяющий центр обеспечивает хранение СКПЭП Пользователя в реестре УЦ в форме электронного документа после его аннулирования не менее трех лет. По истечении указанного срока хранения, СКПЭП переводится в режим архивного хранения. СКПЭП в форме документа на бумажном носителе хранится в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

7.7. Удостоверяющий центр участвует в работе Экспертной комиссии при рассмотрении спорных вопросов (конфликтных ситуаций).

7.8. Удостоверяющий центр контролирует правила использования СКЗИ Пользователями.

7.9. Удостоверяющий центр обязан:

7.9.1. информировать в письменной форме заявителей об условиях и 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;

7.9.2. вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами;

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

7.9.4. обеспечивать круглосуточную доступность реестра сертификатов в информационно-телекоммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания;

7.9.5. обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей;

7.9.6. в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» направлять в единую систему идентификации и аутентификации сведения о лице, получившем сертификат ключа проверки электронной подписи (далее – 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);

7.9.7. по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществить регистрацию указанного лица в единой системе идентификации и аутентификации;

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

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

7.9.10. строго соблюдать срок действия ключей электронной подписи Удостоверяющего центра, используемых для подписания создаваемых сертификатов, распределяя сроки их действия таким образом, чтобы по окончании таких сроков все подписанные этими ключами сертификаты прекратили свое действие.

7.10. Удостоверяющий центр вправе наделить третьих лиц (далее - доверенные лица) полномочиями по вручению сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром, его владельцу.

7.11. Удостоверяющий центр вправе досрочно прекратить действие СКПЭП в случае невыполнения владельцем обязанностей, установленных законодательством Российской Федерации в области электронной подписи, настоящим Регламентом, а также в случае появления у Удостоверяющего центра достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им СКПЭП, не являются подлинными и/или не подтверждают достоверность всей информации, включаемой сертификат и/или в случае, если услуга по созданию и выдаче сертификата не оплачена в надлежащем порядке.

7.12. Удостоверяющий центр обязан обеспечить любому лицу по его обращению, в соответствии с установленным порядком доступа, безвозмездный доступ с использованием информационно-телекоммуникационных сетей к выданным им квалифицированным сертификатам и к актуальному списку аннулированных квалифицированных сертификатов в любое время в течение срока деятельности

удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

8. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ И ЗАЯВИТЕЛЯ

8.1. Пользователь обязан:

8.1.1. Ознакомиться с положениями настоящего Регламента и соблюдать их;

8.1.2. Предоставить достоверную информацию в объеме, определенном положениями настоящего Регламента и Договором;

8.1.3. Подготовить и содержать в рабочем состоянии ПЭВМ и программное обеспечение, предназначенные для работы, в соответствии с эксплуатационной документацией на СКЗИ. Пользователю рекомендуется не использовать средства разработки и отладки программ на ПЭВМ, на которой установлено СКЗИ;

8.1.4. Перед использованием услуг Удостоверяющего центра, оказываемых на платной основе, оплатить данные услуги в полном объеме в соответствии с Договором и настоящим Регламентом;

8.1.5. Для создания ключа электронной подписи и ключа проверки электронной подписи использовать средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи»;

8.1.6. Организовать режим функционирования рабочих мест таким образом, чтобы исключить возможность доступа к СКЗИ, несанкционированной модификации или использования СКЗИ лицами, не имеющими допуска к работе с СКЗИ, а также исключить возможность использования ключей ЭП не уполномоченными на то лицами;

8.1.7. Своевременно оплачивать услуги по созданию и выдаче квалифицированного сертификата ключа проверки электронной подписи;

8.1.8. Соблюдать установленную последовательность действий при обмене электронными документами и проверке их подлинности в соответствии с настоящим Регламентом, эксплуатационной документацией на СКЗИ и инструкциями по использованию СКЗИ.

8.2. Владелец СКПЭП (Заявитель) обязан:

8.2.1. Ознакомиться с положениями настоящего Регламента и соблюдать их;

8.2.2. Для создания квалифицированной электронной подписи использовать средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи»;

8.2.3. Хранить в тайне свой ключ электронной подписи, принимать всевозможные меры для предотвращения его потери, раскрытия, изменения, или несанкционированного использования;

8.2.4. Не использовать ключ ЭП и немедленно обратиться в удостоверяющий центр, выдавший ему СКПЭП, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа ЭП нарушена;

8.2.5. Использовать ЭП в соответствии с ограничениями, содержащимися в СКПЭП (если такие ограничения установлены);

8.2.6. Осуществлять архивирование электронных документов и хранить эти архивы в течение срока, установленного соответствующими законами и нормативными актами для хранения документов;

8.2.7. При разрешении конфликтных ситуаций, связанных с установлением подлинности и/или авторства спорного документа или иных конфликтных ситуаций, связанных с использованием ЭП, предоставить экспертной комиссии, создаваемой и действующей в соответствии с Разделом 27 настоящего Регламента, все документы и материалы, относящиеся к предмету конфликтной ситуации.

8.3. Пользователь и/или заявитель имеют право:

8.3.1. Не принимать к исполнению электронные документы, заверенные ЭП, если:

8.3.1.1. СКПЭП отправителя утратил силу (не действует, находится в СОС) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

Примечание: перед принятием решения по исполнению полученного электронного документа, Пользователь самостоятельно определяет необходимость проверки нахождения СКПЭП и отправителя в реестре аннулированных сертификатов. Актуальный список отзыва СКПЭП опубликованы на сайте Удостоверяющего центра в Интернете по адресу http://www.nwudc.ru.

8.3.1.2. не подтверждена подлинность ЭП в электронном документе;

8.3.1.3. ЭП используется не в соответствии со сведениями и ограничениями, указанными в СКПЭП.

8.3.2. Запрашивать подтверждение по полученным им электронным документам в случае возникновения сомнений;

8.3.3. Требовать от Удостоверяющего центра прекращения действия своего СКПЭП в случае наступления событий, трактуемых как компрометация ключевой информации;

8.3.4. Требовать исполнения обязательств настоящего Регламента от других Пользователей по принятым ими электронным документам;

8.3.5. В случае возникновения конфликтной ситуации, связанной с установлением подлинности и/или авторства спорного документа, требовать разрешения указанных вопросов экспертной комиссией в соответствии с настоящим Регламентом.

9. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

9.1. Заявитель вправе создать ключ электронной подписи и ключ проверки электронной подписи самостоятельно с использованием следующих способов:

9.1.1. На рабочем месте Заявителя, с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» и совместимого со средствами электронной подписи, используемыми в Удостоверяющем центре по форматам ключей и сертификатов;

При реализации данного способа Заявитель обеспечивает конфиденциальность ключа электронной подписи с момента его создания. При обращении в Удостоверяющий центр предоставить файл запроса в формате PKCS#10, содержащий ключ проверки электронной подписи и информацию идентифицирующую владельца ключа проверки

электронной подписи в объеме, определенном Федеральным законом «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

При обращении в Удостоверяющий центр с заявлением на изготовление и выдачу квалифицированного сертификата Заявитель должен подтвердить владение ключом электронной подписи. Подтверждение владения ключом электронной подписи производится путем проверки электронной подписи в файле запроса на квалифицированный сертификат, который предоставляет заявитель, с использованием средств удостоверяющего центра. При отрицательном результате проверки электронной подписи в предоставленном файле запроса на квалифицированный сертификат удостоверяющий центр отказывает заявителю в изготовлении и выдаче квалифицированного сертификата.

9.1.2. С использованием автоматизированного рабочего места Удостоверяющего центра при обращении с заявлением на создание и выдачу квалифицированного сертификата. Создание ключей электронной подписи осуществляется Заявителем самостоятельно или выполняется сотрудником удостоверяющего центра в присутствии Заявителя.

При реализации данного способа используется автоматизированное рабочее место, аттестованное на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, размещенное в аттестованном помещении, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель, который выдается заявителю либо доверенному лицу заявителя по окончании процедуры выдачи сертификата.

10. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

10.1. Плановая смена ключей электронной подписи удостоверяющего центра выполняется не ранее чем через 1 год и не позднее чем через 1 год и 3 месяца после начала действия ключей электронной подписи удостоверяющего центра в соответствии с требованиями используемого средства электронной подписи.

Процедура плановой смены ключа электронной подписи осуществляется в следующем порядке:

- уполномоченное лицо удостоверяющего центра формирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи, а также запрос на выдачу квалифицированного сертификата удостоверяющего центра в формате PKCS#10 Base-64;
- сгенерированный файл запроса направляется в головной удостоверяющий центр федерального органа исполнительной власти, уполномоченного в сфере использования электронной подписи (далее - Уполномоченный орган) для изготовления и выдачи квалифицированного сертификата удостоверяющего центра;
- уполномоченный орган с использованием средств головного удостоверяющего центра выдает квалифицированный сертификат удостоверяющего центра и публикует его в Реестре выданных квалифицированных сертификатов;
- полученный квалифицированный сертификат устанавливается на средства удостоверяющего центра и публикуется на официальном сайте Удостоверяющего центра.

Ранее действовавший ключ электронной подписи удостоверяющего центра используется

только для формирования списков отозванных сертификатов в электронной форме, изданных удостоверяющим центром в период действия предыдущих ключей удостоверяющего центра.

Уведомление пользователей о плановой смене ключей электронной подписи удостоверяющего центра осуществляется путем публикации нового квалифицированного сертификата удостоверяющего центра в реестре Уполномоченного органа, а также на официальном сайте Удостоверяющего центра в сети Интернет.

11. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНЕПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Внеплановая смена ключей электронной подписи удостоверяющего центра выполняется в случае компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего центра. Одновременно со сменой такого ключа электронной подписи прекращается действие всех сертификатов, подписанных этим ключом электронной подписи, с занесением сведений об этих сертификатах в реестр сертификатов.

Процедура внеплановой смены ключа электронной подписи осуществляется в следующем порядке:

- уполномоченное лицо удостоверяющего центра при обнаружении факта компрометации или угрозы компрометации незамедлительно уведомляет об этом уполномоченный орган;
- уполномоченный орган с использованием средств головного удостоверяющего центра аннулирует (отзывает) квалифицированный сертификат удостоверяющего центра;
- после этого уполномоченное лицо удостоверяющего центра получает новый сертификат в соответствии с порядком плановой смены ключей.

Информирование владельцев квалифицированных сертификатов о внеплановой смене ключей производится путем публикации отзыва квалифицированного сертификата в реестре Уполномоченного органа, а также на официальном сайте Удостоверяющего центра в сети Интернет.

При внеплановой смене ключей удостоверяющего центра все квалифицированные сертификаты, выданные в период действия скомпрометированного ключа электронной подписи, аннулируются удостоверяющим центром. Замена аннулированных квалифицированных сертификатов производится удостоверяющим центром на безвозмездной основе после получения нового квалифицированного сертификата от Уполномоченного органа.

12. ПОРЯДОК ПОДКЛЮЧЕНИЯ (РЕГИСТРАЦИИ) ПОЛЬЗОВАТЕЛЕЙ

12.1. Пользователь заключает договор с Удостоверяющим центром и производит оплату.

12.2. Пользователь представляет Удостоверяющему центру заявление на изготовление квалифицированного сертификата ключа проверки электронной подписи, содержащее:

- данные на сотрудников, которым необходимо создать ключи ЭП и/или изготовить

СКПЭП;

Актуальные формы заявления и документов, необходимых для выпуска СКПЭП, содержатся на официальном сайте Удостоверяющего центра по адресу: www.nwudc.ru

12.3. Уполномоченное лицо Удостоверяющего центра согласует с Пользователем график выполнения работ.

12.4. В соответствии с согласованным графиком работ, владельцы СКПЭП (заявители), указанные в заявлении Пользователя, лично или их доверенные лица, прибывают в офис Удостоверяющего центра, где:

- получают СКЗИ и ключи и/или СКПЭП;
- подписывают акт о получении СКЗИ, ключей ЭП, СКПЭП;
- расписываются в СКПЭП на бумажном носителе, подтверждая достоверность информации, внесенной в СКПЭП;
- получают в электронном виде актуальный СКПЭП Удостоверяющего центра;
- получают пароль для связи на случай компрометации ключей;
- получают инструктаж и руководство (памятку) 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.

Примечание: допускается вместо бумажных документов оформление электронных документов с ЭП уполномоченных лиц, если это не запрещено ФЗ или нормативно-правовыми актами.

13. ПОРЯДОК ПОДАЧИ ЗАЯВЛЕНИЯ НА СОЗДАНИЕ И ВЫДАЧУ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

13.1. Актуальная форма заявления на изготовление и выдачу квалифицированного сертификата ключа проверки электронной подписи публикуется на официальном сайте Удостоверяющего центра.

13.2. Заявление заполняется на русском языке печатными буквами лично заявителем и заверяется собственноручной подписью.

13.3. Заявитель или его законный представитель вправе обратиться в офис Удостоверяющего центра или его обособленные подразделения, указанные в Разделе 1 настоящего Регламента, с заявлением и документами, необходимыми для выпуска квалифицированного сертификата.

14. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ЗАЯВЛЕНИЯ НА СОЗДАНИЕ И ВЫДАЧУ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

14.1. При оформлении заявления на создание и выдачу квалифицированного сертификата на физическое лицо в заявлении указывается:

- фамилия, имя и отчество заявителя полностью, без сокращений;
- индивидуальный номер налогоплательщика (ИНН) физического лица;
- сведения о документе, удостоверяющем личность заявителя (вид документа, серия, номер, кем выдан документ и дата его выдачи);
- страховой номер индивидуального лицевого счета (СНИЛС);
- адрес электронной почты и телефон для связи с заявителем;
- адрес регистрации по месту жительства (пребывания);

- назначение использования квалифицированного сертификата (при необходимости).

14.2. При оформлении заявления на создание и выдачу квалифицированного сертификата на физическое лицо - представителя юридического лица в заявлении указываются:

- полное или сокращенное наименование юридического лица в соответствии с уставными документами;
- должность, фамилия, имя отчество руководителя юридического лица;
- индивидуальный номер налогоплательщика (ИНН) юридического лица, код причины постановки на учет в налоговом органе и основной государственный регистрационный номер юридического лица;
- фамилия, имя, отчество заявителя полностью;
- сведения о документе, удостоверяющем личность заявителя (вид документа, серия, номер, кем выдан документ и дата его выдачи);
- страховой номер индивидуального лицевого счета (СНИЛС) физического лица – заявителя;
- адрес электронной почты и телефон для связи с заявителем;
- адрес места нахождения юридического лица в соответствии с регистрационными документами;
- назначение использования квалифицированного сертификата (при необходимости).

14.3. В заявлении указывается, что заявитель ознакомлен с настоящим Регламентом и обязуется его выполнять, выражает свое согласие на обработку, передачу и хранение предоставленных персональных данных в целях изготовления и обслуживания СКПЭП и гарантирует достоверность и подлинность предоставленных данных, признает, что персональные данные, заносимые в квалифицированный сертификат, относятся к общедоступным персональным данным. Указанные сведения подтверждаются личной подписью заявителя с указанием даты заполнения заявления.

В случае подачи заявления представителем юридического лица достоверность данных дополнительно подтверждается подписью руководителя и печатью организации.

14.4. Заявление может быть предоставлено в удостоверяющий центр как на бумажном носителе, так и в электронной форме. В случае подачи Заявления в электронной форме, оно должно быть подписано квалифицированной электронной подписью заявителя и может быть направлено с использованием сети Интернет. При последнем способе подачи Пользователь самостоятельно несет ответственность за сохранение конфиденциальности персональных данных, содержащихся в заявлении.

14.5. Вместе с заявлением на создание и выдачу квалифицированного сертификата Пользователь предоставляет в Удостоверяющий центр перечень документов, определенный Разделом 16 настоящего Регламента.

15. ПОРЯДОК УСТАНОВЛЕНИЯ ЛИЧНОСТИ ЗАЯВИТЕЛЯ

15.1. В случае личного обращения заявителя в Удостоверяющий центр для подачи заявления и/или получения квалифицированного сертификата сотрудники Удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» обязаны установить личность заявителя или его представителя:

- личность гражданина Российской Федерации устанавливается по основному

документу, удостоверяющему личность, – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;

- личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, с учетом требований Раздела 16 настоящего Регламента;
- личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц;

16. ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ЗАПРАШИВАЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ У ЗАЯВИТЕЛЯ ДЛЯ ИЗГОТОВЛЕНИЯ И ВЫДАЧИ СЕРТИФИКАТА, В ТОМ ЧИСЛЕ ДЛЯ УДОСТОВЕРЕНИЯ ЛИЧНОСТИ ЗАЯВИТЕЛЯ, А ТАКЖЕ ТРЕБОВАНИЯ К ТАКИМ ДОКУМЕНТАМ

При обращении в удостоверяющий центр заявитель или его доверенное лицо предоставляет документы необходимые для установления личности заявителя (его доверенного лица), а также документы (или их надлежащим образом заверенные копии), подтверждающие сведения, на основании которых удостоверяющим центром вносятся данные в квалифицированный сертификат.

16.1. В случае изготовления квалифицированного сертификата на Заявителя - физическое лицо, в удостоверяющий центр предоставляются следующие документы (оригиналы или их надлежащим образом заверенные копии):

- основной документ, удостоверяющий личность заявителя (его доверенного лица) в соответствии с требованиями Раздела 15 настоящего Регламента;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- нотариальная доверенность (в случае если от имени заявителя действует доверенное лицо).
- В случае изготовления квалифицированного сертификата на физическое лицо - представителя юридического лица, в удостоверяющий центр представляются следующие документы:
- основной документ, удостоверяющий личность в соответствии с требованиями Раздела 15 настоящего Регламента;
- номер страхового свидетельства государственного пенсионного страхования
- копия свидетельства о государственной регистрации юридического лица, заверенная руководителем юридического лица и печатью юридического лица
- копия свидетельства о постановке на учет в налоговом органе, заверенная руководителем юридического лица и печатью юридического лица
- копия решения (протокола) о назначении или об избрании руководителя или доверенность на право обращения за получением квалифицированного сертификата, заверенные подписью руководителя и печатью юридического лица.

16.2. В случае изготовления квалифицированного сертификата на лицо, выступающее от имени заявителя - иностранной организации предоставляет в удостоверяющий центр следующие документы:

- основной документ, удостоверяющий личность в соответствии с требованиями Раздела 15 настоящего Регламента;
- номер свидетельства о постановке на учет в налоговом органе или идентификационный номер налогоплательщика заявителя - иностранной организации;
- доверенность или иной документ, подтверждающий полномочия обращаться за получением квалифицированного сертификата.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

Если для подтверждения каких-либо сведений, вносимых в сертификат, действующим законодательством установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Удостоверяющий центр вправе потребовать у заявителя дополнительные документы для подтверждения сведений, включаемых в квалифицированный сертификат.

17. ПОРЯДОК СОЗДАНИЯ И ВЫДАЧИ КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

17.1. Удостоверяющий центр с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем для изготовления и выдачи сертификата, в том числе запрашивает и получает из государственных информационных ресурсов:

- выписку из единого государственного реестра юридических лиц – в отношении заявителя - юридического лица;
- выписку из единого государственного реестра индивидуальных предпринимателей - в отношении заявителя - индивидуального предпринимателя;
- выписку из Единого государственного реестра налогоплательщиков - в отношении заявителя - иностранной организации.

17.2. В случае, если полученные из государственных реестров сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и удостоверяющим центром установлена личность заявителя - физического лица или получено подтверждение полномочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата, удостоверяющий центр создает ключи электронной подписи (при необходимости) и квалифицированный сертификат.

17.3. Если представленные заявителем данные не подтверждены, удостоверяющий центр отказывает в создании квалифицированного сертификата.

17.4. Удостоверяющий центр выдает квалифицированный сертификат заявителю в электронной форме. При выдаче квалифицированного сертификата заявителю для ознакомления с информацией, содержащейся в квалифицированном сертификате, предоставляется копия квалифицированного сертификата на бумажном носителе в двух экземплярах.

17.5. Заявитель подтверждает корректность данных, внесенных в квалифицированный сертификат, собственноручной подписью на бумажных экземплярах сертификата, один из которых остается у заявителя, второй экземпляр - передается на архивное хранение в Удостоверяющий центр.

17.6. Вместе с квалифицированным сертификатом заявителю передается парольная группа, использующаяся для аутентификации Пользователя Удостоверяющего центра при выполнении регламентных процедур, возникающих при нарушении конфиденциальности ключевых документов Пользователя.

17.7. Заявитель информируется в письменной форме 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.

17.8. Срок создания и выдачи квалифицированного сертификата не превышает 5 (пяти) рабочих дней с момента подачи заявления и комплекта подтверждающих документов, при условии оплаты услуг по созданию и выдаче квалифицированного сертификата.

18. ПОДТВЕРЖДЕНИЕ ДЕЙСТВИТЕЛЬНОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ, ИСПОЛЬЗОВАННОЙ ДЛЯ ПОДПИСАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

18.1. Актуальная форма заявления на подтверждение действительности электронной подписи в электронных документах публикуется на официальном сайте Удостоверяющего центра в сети Интернет.

18.2. Пользователь передает в удостоверяющий центр заполненное заявление в бумажном виде. К заявлению необходимо приложить электронные документы, в которых необходимо проверить действительность квалифицированной электронной подписи, и квалифицированный сертификат, при помощи которого производится проверка. При использовании отделенной электронной подписи к каждому электронному документу пользователь услуг должен предоставить соответствующий файл с квалифицированной электронной подписью.

18.3. После получения заявления и всей необходимой информации, удостоверяющий центр с использованием инфраструктуры и средств удостоверяющего центра производит проверку подлинности и действительности квалифицированной электронной подписи в соответствии со статьей 11 Федерального закона «Об электронной подписи», в том числе процедуру проверки действительности всех сертификатов, включенных в цепочку проверки для данного сертификата до сертификата аккредитованного удостоверяющего центра, выданного удостоверяющему центру головным удостоверяющим центром.

18.4. По результатам проверки удостоверяющий центр формирует отчет в электронной форме или в форме документа на бумажном носителе. Отчет в электронной форме подписывается квалифицированной электронной подписью уполномоченного лица удостоверяющего центра. Отчет в форме документа на бумажном носителе заверяется подписью руководителя удостоверяющего центра и печатью удостоверяющего центра.

18.5. Срок предоставление услуги по подтверждению подлинности электронной подписи не более 3 (трех) рабочих дней с момента поступления заявления и всех

необходимых данных, при условии поступления оплаты стоимости данной услуги на расчетный счет удостоверяющего центра.

18.6. Услуга оказывается на платной основе. Актуальная информация о стоимости услуги по подтверждению действительности электронной подписи опубликована на официальном сайте Удостоверяющего центра в сети Интернет.

19. ПРОЦЕДУРЫ, ОСУЩЕСТВЛЯЕМЫЕ ПРИ ПРЕКРАЩЕНИИ ДЕЙСТВИЯ И АННУЛИРОВАНИИ СЕРТИФИКАТА

19.1. Квалифицированный сертификат может быть аннулирован до истечения срока его действия по заявлению его владельца.

19.2. Удостоверяющий центр вправе самостоятельно, без предоставления заявления владельца квалифицированного сертификата аннулировать квалифицированный сертификат с обязательным уведомлением владельца в следующих случаях:

- в случае прекращения деятельности удостоверяющего центра без передачи его функций другим лицам;
- не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в квалифицированном сертификате;
- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;
- вступило в силу решение суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию.

Удостоверяющий центр уведомляет владельца квалифицированного сертификата об аннулировании его сертификата путем направления документа на бумажном носителе или электронного документа.

19.3. Актуальная форма заявления на аннулирование квалифицированного сертификата опубликована на официальном сайте Удостоверяющего центра. Заявление может быть представлено в удостоверяющий центр как в форме электронного документа, так и в форме документа на бумажном носителе. Заявление в форме электронного документа должно быть подписано квалифицированной электронной подписью. Заявление в форме документа на бумажном носителе должно заверено собственноручной подписью владельца квалифицированного сертификата и/или руководителя юридического лица и печатью юридического лица.

19.4. Владелец квалифицированного сертификата вправе обратиться в удостоверяющий центр по телефонам, указанным в Разделе 1 настоящего Регламента, для аннулирования сертификата. При этом для установления личности владельца квалифицированного сертификата используется парольная группа, выдаваемая владельцу вместе с квалифицированным сертификатом. В течение 1 (одного) рабочего дня владелец квалифицированного сертификата должен предоставить в удостоверяющий центр заявление на аннулирование сертификата в соответствии с требованиями настоящего Регламента.

19.5. В случае получения заявления на аннулирование сертификата или наступления событий, указанных в пункте 6.1 статьи 14 Федерального закона «Об электронной подписи», удостоверяющий центр вносит информацию об аннулировании квалифицированного сертификата в реестр сертификатов путем публикации

обновленного списка отозванных сертификатов в электронной форме с добавлением в него уникального номера аннулированного сертификата не позднее 12 (двенадцати) часов с момента наступления указанных событий или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

20. ПОРЯДОК ВЕДЕНИЯ РЕЕСТРА СЕРТИФИКАТОВ

20.1. Реестр выданных квалифицированных сертификатов ведется в электронной форме в формате базы данных с использованием средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

20.2. Удостоверяющий центр издает списки отзыва сертификатов ключей проверки электронной подписи в электронной форме формата X.509 версии 2.

20.3. Квалифицированный сертификат вносится в Реестр выданных сертификатов сразу после создания.

20.4. Информация об аннулировании (прекращении действия) квалифицированного сертификата заносится в список отозванных сертификатов не позднее 12 часов с момента поступления заявления или наступления событий, указанных в пункте 6.1 статьи 14 Федерального закона «Об электронной подписи».

20.5. При использовании протокола OCSP для проверки статуса квалифицированных сертификатов информация об аннулировании квалифицированного сертификата отображается немедленно, начиная с момента выполнения процедуры аннулирования. Сетевой адрес OCSP-сервера включается в структуру выдаваемых квалифицированных сертификатов в расширение «Authority Information Access (AIA)» (OID 1.3.6.1.5.5.7.48.1). Доступ к серверу осуществляется по протоколу HTTP.

20.6. Актуальность информации в Реестре квалифицированных сертификатов обеспечивается с использованием средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, которые в режиме реального времени заносят информацию в Реестр.

20.7. Хранение информации, содержащейся в Реестре сертификатов, осуществляется в защищенных базах данных Удостоверяющего центра и в электронных архивах в форме, позволяющей проверить ее целостность и достоверность.

20.8. Защита информации, содержащейся в Реестре, от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий обеспечивается путем размещения технических средств удостоверяющего центра в контролируемой зоне, исключающей свободное пребывание посторонних лиц, использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, систем резервного копирования и систем разграничения доступа.

20.9. Плановое и внеплановое техническое обслуживание Реестра сертификатов осуществляется, как правило, в нерабочее время Удостоверяющего центра и не может превышать 3 (трех) часов. Удостоверяющий центр заблаговременно оповещает Пользователей о планируемом проведении планового или внепланового технического обслуживания Реестра сертификатов, путем публикации информации на официальном сайте Удостоверяющего центра в сети Интернет.

21. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

21.1. Информирование заявителей об условиях и о порядке использования квалифицированных электронных подписей и средств электронной подписи производится путем размещения настоящего Регламента на официальном сайте Удостоверяющего центра. Заявитель, подписывая заявление на создание и выдачу квалифицированного сертификата, соглашается с тем, что изучил настоящий Регламент и ознакомлен с порядком использования квалифицированных электронных подписей и средств электронной подписи.

21.2. Информирование заявителей о мерах необходимых для обеспечения безопасности электронных подписей и их проверки, осуществляется путем выдачи заявителю памятки по обеспечению безопасности вместе с выдачей квалифицированного сертификата.

21.3. Удостоверяющий центр изготавливает ключи электронной подписи заявителей в единственном экземпляре с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» и не осуществляет депонирование и/или архивирование ключей электронных подписей Заявителей.

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

21.5. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании СКПЭП. Для самостоятельного получения информации из реестра Пользователь может воспользоваться формой запроса на сайте Удостоверяющего центра в сети Internet: www.nwudc.ru (раздел «Удостоверяющий центр» - подраздел «Реестр СКПЭП»).

При необходимости получения выписки из реестра СКПЭП Пользователь направляет запрос в свободной форме с указанием информации, позволяющей идентифицировать лицо, обратившееся за получением информации, а также данные запрашиваемого сертификата (ФИО владельца и серийный номер) и цели запроса, Удостоверяющему центру следующими способами:

- По электронной почте;
- При личном обращении.

21.6. Указанная информация предоставляется в форме выписки из реестра СКПЭП и направляется обратившемуся лицу с использованием информационно-телекоммуникационных сетей, либо передается лично (по выбору лица, обратившегося за получением информации из реестра СКПЭП).

21.7. Срок предоставления Удостоверяющим центром сведений из Реестра сертификатов не превышает 7 (семи) рабочих дней для направления информации на бумажном носителе почтовым отправлением и 24 (двадцати четырех) часов – для направления выписки посредством информационно-телекоммуникационных сетей либо при передаче сведений в офисе Удостоверяющего центра.

21.8. Актуальные списки отзыва сертификатов публикуются на сайте Удостоверяющего центра по адресу: www.nwudc.ru (раздел “Удостоверяющий

центр", подраздел «Сертификаты УЦ и CRL (СОС)»). Полный путь к точкам публикации списков отзыва сертификатов содержится в расширении сертификата CRLDistributionPoints (объектный идентификатор 2.5.29.31). Доступ к спискам отозванных (аннулированных) сертификатов осуществляется круглосуточно по протоколу HTTP.

Форма списка отзыва сертификатов Удостоверяющего центра в электронной форме

Название	Описание	Содержание
	Базовые поля	списка отзыва сертификатов
Version		V2
Issuer	Издатель СОС	Идентификационные данные Удостоверяющего центра в соответствии с Приказом ФСБ России от 27.12.2011 г. №795
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отзыва сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана " 1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись	Подпись издателя в соответствии с ГОСТ Р
Расширения списка отзыва сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа ЭП Уполномоченного лица Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего Центра
CRLNumber	Номер СОС	Порядковый номер выпущенного СОС

21.9. СКПЭП Удостоверяющего центра, используемые для подписания от своего имени сертификатов Пользователей, размещены в сети интернет (в том числе на сайте www.nwudc.ru).

21.10. В соответствии с требованиями статьи 18 Федерального закона «Об электронной подписи» Удостоверяющий центр осуществляет регистрацию выданных квалифицированных сертификатов в единой системе идентификации и аутентификации (далее - ЕСИА) с использованием сервисов, предоставляемых информационной системой межведомственного электронного взаимодействия.

21.11. Удостоверяющий центр оказывает услугу по регистрации владельца квалифицированного сертификата в ЕСИА в качестве физического лица по желанию владельца квалифицированного сертификата и на безвозмездной основе.

21.12. Регистрация владельца квалифицированного сертификата в ЕСИА осуществляется только при личном обращении владельца квалифицированного сертификата в удостоверяющий центр после установления его личности в соответствии с Разделом 15 настоящего Регламента. При обращении в удостоверяющий центр владелец квалифицированного сертификата должен предоставить ключевой носитель, содержащий ключ электронной подписи, соответствующий ключу проверки электронной подписи, включенному в состав квалифицированного сертификата.

22. СМЕНА КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ ВЛАДЕЛЬЦА СЕРТИФИКАТА

22.1. Смена ключа электронной подписи владельца сертификата может осуществляться по заявлению владельца сертификата о смене ключа электронной подписи;

22.2. Заявление на смену ключа электронной подписи владельца сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной подписью владельца сертификата;

22.3. Требования к заявлению на смену ключа электронной подписи владельца сертификата с указанием, что если смена ключа электронной подписи владельца сертификата связана с его компрометацией или угрозой компрометации и из заявления точно следует, какой ключ какого владельца сертификата подлежит смене, то смена осуществляется и в том случае, если заявление подано с нарушением отдельных требований к заявлению на смену ключа электронной подписи владельца сертификата;

22.4. Смена ключей Пользователя производится по инициативе Пользователя в следующем порядке:

- Пользователь направляет в Удостоверяющий центр заявление на замену ключей (рекомендуется за месяц до истечения срока действия сертификата старого ключа);
- Удостоверяющий центр согласовывает с Пользователем время проведения работ;
- Пользователь оплачивает работы по изготовлению и выдаче новых СКПЭП;
- работы по изготовлению новых ключей и выдаче сертификатов Удостоверяющий центр производит в соответствии с Разделом 17 настоящего Регламента;
- Пользователь проверяет работоспособность полученных новых ключей и сертификатов;
- Пользователь принимает решение о сроках и порядке архивного хранения или об уничтожении старых ключей самостоятельно, так как все риски, связанные с несанкционированным использованием старых ключей, ложатся на Пользователя.

  В случае принятия решения об уничтожении ключей, Пользователь понимает, что все нерасшифрованные электронные документы, зашифрованные с использованием уничтожаемых ключей, в дальнейшем прочитать будет невозможно.

22.5.

Пользователь обеспечивает хранение расшифрованных документов в электронном виде в соответствии с требованиями, установленными законодательством и настоящим Регламентом.

23. ДЕЙСТВИЯ СТОРОН ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭП

23.1. Удостоверяющий центр при выдаче СКПЭП передает Пользователю парольную фразу для экстренной связи в случае компрометации ключей электронной подписи. Пользователь обеспечивает сохранение конфиденциальности пароля.

23.2. Пользователь, в случае компрометации собственных ключей ЭП, обязан:

23.2.1. Прекратить обмен электронными документами с использованием скомпрометированных ключей;

23.2.2. Немедленно информировать Удостоверяющий центр по телефонным каналам связи с использованием парольной группы о наступлении события, трактуемого как компрометация ключей;

23.2.3. В течение 1 (одного) рабочего дня с момента определения компрометации ключей документально оформить уведомление (заявление на прекращение действия СКПЭП) и направить его в Удостоверяющий центр.

23.3. Удостоверяющий центр, получивший сообщение о компрометации ключей Пользователя, должен убедиться в достоверности сообщения о компрометации (запросить пароль или факсимильное сообщение, заверенное подписью и печатью Пользователя). Досрочное прекращение действия сертификата скомпрометированного ключа выполняется в течение 30 (тридцати) минут с момента получения заявления Пользователя, подаваемого в форме документа на бумажном носителе или в форме электронного документа, заверенного электронной подписью.

23.4. Пользователь, допустивший компрометацию собственных ключей ЭП, несет полную ответственность за ущерб связанный с использованием этих ключей, а также за все издержки, связанные с генерацией новых ключей, их сертификацией и вводом в действие.

24. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ

24.1. Удостоверяющий центр и Пользователь в процессе работы обязаны обеспечить сохранность и не разглашение полученной друг от друга конфиденциальной информации, в том числе персональных данных, в соответствии с действующим законодательством Российской Федерации.

24.2. Удостоверяющий центр обязан не разглашать (не публиковать) информацию, полученную от Пользователей, за исключением информации, содержащейся в СКПЭП Пользователей.

24.3. Порядок предоставления конфиденциальной информации налоговым, правоохранительным и судебным органам осуществляется в соответствии с действующим законодательством Российской Федерации.

24.4. Удостоверяющий центр осуществляет действия по сбору, систематизации, записи, накоплению, использованию, хранению, уточнению, изменению, обновлению, блокированию и уничтожению персональных данных Пользователя и/или Заявителя в соответствии с Федеральным законом от 27.06.2006г. №152-ФЗ «О персональных данных».

25. ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ СИСТЕМЫ

25.1. Пользователь несет ответственность за достоверность сведений, указанных им в заявлении, а также обязан сообщать обо всех изменениях этих сведений.

25.2. Пользователь несет ответственность за сохранность и правильность эксплуатации СКЗИ и своих ключей электронной подписи.

25.3. В случае несвоевременного сообщения о факте компрометации ключей, Пользователь, допустивший компрометацию ключей, несет ответственность в полном объеме за ущерб, причиненный им другим пользователям.

25.4. Удостоверяющий центр имеет финансовое обеспечение ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в квалифицированном СКПЭП, выданном Удостоверяющим центром, или информации, содержащейся в реестре квалифицированных СКПЭП, который ведет Удостоверяющий центр, в сумме, установленной Федеральным Законом от 06.04.2011 №63-ФЗ "Об электронной подписи".

25.5. Удостоверяющий центр не несет ответственности за последствия и убытки в случае нарушения Пользователями положений настоящего Регламента.

25.6. Удостоверяющий центр не несёт ответственности перед владельцами СКПЭП и лицами, использующими СКПЭП для проверки подписи и шифрования сообщений, а также перед третьими лицами, за любые убытки, потери, иной ущерб, связанный с использованием СКПЭП, независимо от суммы заключенных с использованием СКПЭП сделок и совершения ими иных действий, за исключением случаев нарушения Удостоверяющим центром обязательств, предусмотренных Регламентом и/или действующим законодательством Российской Федерации.

25.7. Пользователь имеет право направить в адрес Удостоверяющего центра заявление о неисполнении/ненадлежащем исполнении им обязательств по Договору с требованием уплаты причиненного ему ущерба. Заявление в письменной форме должно быть направлено по почтовому адресу, указанному в Договоре, с приложением документов, подтверждающих неисполнение/ненадлежащее исполнение Удостоверяющим центром обязательств по Договору, а также расчетом размера убытков определяемым в соответствии с условиями Договора и настоящего Регламента.

25.8. За неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту Пользователи несут ответственность в соответствии с Договором и действующим законодательством Российской Федерации.

26. ВЗАИМОДЕЙСТВИЕ СТОРОН ПРИ НЕШТАТНЫХ СИТУАЦИЯХ

26.1. При возникновении нештатных ситуаций, таких как: выход из строя ключевого носителя, сбои и отказы в работе СКЗИ, сбои и отказы в работе средств ЭП и др., Пользователь обязан:

- руководствоваться положениями и инструкциями эксплуатационной документации;
- сообщить о возникшей ситуации Удостоверяющему центру;
- выполнить указания Удостоверяющего центра, касающиеся выхода из данной внештатной ситуации.

27. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

27.1. Разрешая конфликтные ситуации при нарушении процедур криптографической защиты информации и/или установлении авторства и/или подлинности электронных документов, заверенных ЭП, Пользователи исходят из того, что:

- информация в электронной форме, подписанная квалифицированной ЭП, признается электронным документом, равнозначным документу на бумажном носителе,

подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе;

- информация в электронной форме, подписанная простой ЭП или неквалифицированной ЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной ЭП равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки ЭП. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой ЭП, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям статьи 9 Федерального закона №63-ФЗ от 06.04.2011;
- если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной ЭП и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия, могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью;
- одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании ЭП пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным ЭП того вида, которой подписан пакет электронных документов;
- электронный документ порождает обязательства Пользователя перед другим Пользователем, если документ оформлен надлежащим образом, заверен ЭП и доставлен другому Пользователю. При этом ЭП используется в соответствии со сведениями, указанными в СКПЭП, а СКПЭП отправителя действует (не аннулирован);
- подтверждением того, что электронный документ Пользователя принят пользователем-получателем, является получение Пользователем или надлежащим образом оформленной электронной квитанции о принятии его документа, или получение того же самого документа, подписанных ЭП пользователя-получателя.
- Пользователь признает, что используемая в соответствии с настоящим Регламентом система защиты информации, которая обеспечивается ЭП и шифрованием,

достаточна для защиты информации, подтверждения целостности, подлинности и авторства электронных документов, а также разрешения конфликтных ситуаций по ним;

- математические свойства алгоритма ЭП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р34.10-2001, ГОСТ Р34.10-2012 и ГОСТ Р34.11-94, свидетельствуют о невозможности подделки ЭП любым лицом, не обладающим ключом ЭП. Пользователь признает, что разбор конфликтной ситуации в отношении авторства, целостности и подлинности электронного документа заключается в доказательстве подписания конкретного электронного документа на конкретном ключе ЭП.

27.2. В соответствии с настоящим порядком подлежат разрешению конфликтные ситуации двух типов:

- некорректность входящего электронного документа или ЭП (конфликтная ситуация типа А);
- для корректного электронного документа непризнание отправителем электронного документа факта подписания им документа, а также его целостности и/или подлинности (конфликтная ситуация типа Б).

27.2.1. Порядок разрешения конфликтных ситуаций типа А:

27.2.1.1. Принимающая Сторона по телефону (или иным образом) запрашивает у отправляющей Стороны информацию о документе, подлинность которого вызывает сомнения. При получении подтверждения об отправке указанного документа, запрашивает повторное оформление и отправку данного документа;

27.2.1.2. Результатом повторной обработки принимающей Стороной (проверка ЭП) полученного документа может быть:

27.2.1.2.1. Проверка ЭП в повторно переданном документе дала отрицательный результат.

В этом случае делается вывод о возможном нарушении действующего ключа ЭП либо о неисправности программно-аппаратных средств одной из Сторон.

При этом необходимо:

- проверить СКПЭП;
- штатными средствами в соответствии с эксплуатационной документацией проверить целостность и неизменность программного обеспечения СКЗИ. Переустановить его в случае необходимости.

Если положительный результат не достигнут, то необходимо обратиться к Удостоверяющему центру.

27.2.1.2.2. Повторная проверка дала положительный результат – электронный документ корректен, ЭП верна.

27.2.2. Порядок разрешения конфликтных ситуаций типа Б:

27.2.2.1. Если один из Пользователей приходит к выводу, что другой Пользователь ссылается на документ, предположительно исходящий от него, но им не подписывался и/или его содержание изменено, этот Пользователь немедленно извещает Удостоверяющего центра о наличии такой конфликтной ситуации;

27.2.2.2. Удостоверяющий центр формирует Экспертную (согласительную) комиссию для разрешения конфликтной ситуации, в состав которой входят представители Удостоверяющего центра и Пользователи, вовлеченные в конфликтную ситуацию. Дополнительно могут привлекаться авторитетные независимые специалисты в области криптографической защиты информации;

27.2.2.3. В ходе работы экспертной комиссии рассматриваются все документы и материалы, относящиеся к предмету разногласий, и выполняется процедура проверки ЭП документа. Экспертной комиссии должны быть представлены следующие данные:

- электронный документ с ЭП, авторство и/или целостность которого оспаривается;
- архивные копии этого электронного документа с ЭП, переданные Пользователями, вовлеченными в конфликтную ситуацию;
- СКПЭП, выданные Удостоверяющим центром;
- дистрибутивы СКЗИ;
- ключевые носители.

27.2.2.4. При необходимости экспертная комиссия имеет право провести экспертизу ПЭВМ Пользователей, вовлеченных в конфликтную ситуацию.

27.3. Экспертиза проводится на автоматизированном рабочем месте Удостоверяющего центра.

27.4. Экспертная комиссия подтверждает или опровергает авторство Пользователя и целостность оспариваемого электронного документа, вызвавшего данную конфликтную ситуацию. Решение экспертной комиссии оформляется в виде протокола.