Приложение к приказу отдела по

информатизации и сетевым ресурсам

№ 1-ЭП

**ПОРЯДОК ПОЛУЧЕНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ДЛЯ ИСПОЛЬЗОВАНИЯ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ АДМИНИСТРАЦИИ РАЙОНА**

# **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**Автоматизированная система (АС)** *–* Программное обеспечение «Бюджет» и «Удаленное рабочее место», разработанное ООО «Информационные системы «Криста»;

**Электронная цифровая подпись (ЭЦП)** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа ЭЦП, а также установить отсутствие искажения информации в электронном документе

**Владелец сертификата ключа ЭЦП** – физическое лицо, являющееся пользователем КИС на имя которого Удостоверяющим центром выдан сертификат ключа ЭЦП и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах;

**Закрытый ключ ЭЦП** - уникальная последовательность символов, известная владельцу сертификата ключа ЭЦП и предназначенная для создания в электронных документах электронной цифровой подписи;

**Корпоративная информационная система электронного документооборота (КИС)** – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц. КИС является корпоративной муниципальной информационной системой;

**Ключи ЭЦП** *–* закрытые и открытые ключи электронной цифровой подписи, предназначенные для формирования/проверки электронной цифровой подписи, действующие в течение определенного периода времени.

**Ключевой документ** *–* физический носитель определенной структуры, содержащий ключи ЭЦП.

**Организатор КИС** *–* Департамент финансов администрации района (далее – ДФ)

**Оператор КИС** – Отдел по информатизации и сетевым ресурсам администрации района

**Открытый ключ ЭЦП** *-* уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе.

**Подтверждение подлинности электронной цифровой подписи в электронном документе** - положительный результат проверки средством электронной цифровой подписи с использованием сертификата ключа ЭЦП принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

**Пользователь КИС** – физическое лицо, сотрудник Организатора КИС и Клиента КИС, владелец сертификата ключа ЭЦП и/или пользователь сертификата ключа ЭЦП.

**Пользователь сертификата ключа ЭЦП** – физическое лицо, являющееся пользователем КИС и использующее сведения о сертификате ключа ЭЦП для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа ЭЦП.

**Клиент КИС** – организация, которой в установленном порядке открыты лицевые счета организатором КИС

**Сертификат ключа ЭЦП** *–* электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра или документ на бумажном носителе с собственноручной подписью уполномоченного лица Удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются Удостоверяющим центром пользователям КИС для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа ЭЦП.

**Корневой сертификат** – сертификат удостоверяющего центра, используемый для проверки цифровой подписи сертификатов и списков отзыва, издаваемых этим центром

**Список отозванных сертификатов** - электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей подписей, которые на момент времени формирования списка отозванных сертификатов были отозваны или действие которых было приостановлено. Момент времени формирования списка отозванных сертификатов определяется по значению поля ThisUpdate списка отозванных сертификатов.

**Компрометация ключа ЭЦП** - утрата доверия к закрытому ключу электронной цифровой подписи вследствие возникновения обоснованного подозрения о доступе третьих лиц к ключевой информации;

**Средство электронной цифровой подписи** *-* сертифицированное средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», обеспечивающие реализацию следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

**Удостоверяющий центр** (далее - УЦ )– Отдел по информатизации и сетевым ресурсам администрации района, обеспечивающий согласно № 63-ФЗ от 06.04.2011 года «Об электронной подписи», распоряжения администрации района от 21.09.2012 № 620-р выполнение целевых функций удостоверяющего центра в КИС.

**Формат электронного документа** *–* структура содержательной части электронного сообщения, на основе которого сформирован электронный документ.

**Электронный документ** – электронное сообщение, соответствующее установленному настоящим Порядком формату, подписанное электронной цифровой подписью и способное быть преобразованным средствами КИС в форму, пригодную для однозначного восприятия его содержания.

1. **Права и обязанности сторон**

2.1. Обязанности Удостоверяющего центра

1. Предоставить пользователю Удостоверяющего центра сертификаты открытых ключей уполномоченного лица Удостоверяющего центра в электронной форме.
2. Использовать закрытый ключ уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов открытых ключей и списков отозванных сертификатов.
3. Обеспечить сохранность в тайне и защиту от несанкционированного доступа к закрытому ключу уполномоченного лица Удостоверяющего центра.
4. Организовать свою работу по Ханты-Мансийскому времени и синхронизировать по нему все свои программные и технические средства обеспечения деятельности.
5. Обеспечить регистрацию пользователей, изготовление и управление сертификатами открытых ключей в соответствии с утвержденным порядком.
6. Обеспечить выполнение процедур по подтверждению подлинности ЭЦП в электронном документе в соответствии с утвержденным порядком.
7. В случае формирования ключей пользователя в Удостоверяющем центре обеспечить защиту от несанкционированного доступа к закрытому ключу пользователя с момента генерации закрытого ключа до момента его предоставления пользователю Удостоверяющего центра.
8. Обеспечить уникальность серийных номеров в изготовленных сертификатах открытых ключей пользователей Удостоверяющего центра.
9. Обеспечить уникальность значений открытых ключей в изготовленных сертификатах открытых ключей пользователей Удостоверяющего центра.
10. Обеспечить информирование пользователей Удостоверяющего центра о статусе сертификатов открытых ключей путем публикации списка отозванных сертификатов Период публикации списка отозванных сертификатов - 1 (одни) сутки (по рабочим дням).
    1. Обязанности пользователя Удостоверяющего центра
11. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.
12. Применять для формирования электронной цифровой подписи электронных документов только действующий личный закрытый ключ.
13. Применять для шифрования электронного документа сертификат открытого ключа пользователя-получателя документа, одновременно удовлетворяющего следующим условиям: сертификат открытого ключа действует; закрытый ключ, соответствующий данному сертификату открытого ключа, также действует.
14. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.
15. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате открытого ключа (поля Key Usage, Extended Key Usage сертификата открытого ключа).
16. С целью отзыва сертификата открытого ключа немедленно обратиться с заявлением в Удостоверяющий центр в случае потери, раскрытия, искажения личного закрытого ключа, а также, в случае если пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.
17. Не использовать личный закрытый ключ, связанный с сертификатом открытого ключа, заявление, на отзыв которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на отзыв сертификата по момент времени официального уведомления об отзыве сертификата, либо об отказе в отзыве сертификата.
18. Не использовать закрытый ключ, связанный с сертификатом открытого ключа, который отозван.
19. Не использовать личный закрытый ключ до предоставления в Удостоверяющий центр подписанного сертификата открытого ключа на бумажном носителе, соответствующего данному закрытому ключу.
20. Сертификат открытого ключа на бумажном носителе может быть представлен в Удостоверяющий центр по факсу с последующим обязательным предоставлением в течение одного месяца оригинала документа.
    1. Права Удостоверяющего центра
21. Отказать в регистрации пользователя, изготовлении и отзыве сертификатов открытых ключей в случае ненадлежащего оформления заявительных документов.
22. Отказать в проведении процедуры подтверждения подлинности ЭЦП в электронном документе в случае ненадлежащего оформления заявительных документов.
23. Отказать в отзыве сертификата открытого ключа пользователя Удостоверяющего центра в случае, если истек срок действия закрытого ключа, соответствующего этому сертификату.
24. В одностороннем порядке отозвать сертификат открытого ключа пользователя Удостоверяющего центра с обязательным уведомлением его владельца и указанием обоснованных причин.
    1. Права пользователя Удостоверяющего центра
25. Обратиться в Удостоверяющий центр для изготовления, отзыва сертификатов открытых ключей согласно установленного порядка.
26. Обратиться в Удостоверяющий центр для проведения экспертизы по подтверждению подлинности ЭЦП в электронном документе согласно установленного настоящим порядка.
27. Обратиться в Удостоверяющий центр за получением информации о статусе сертификата открытого ключа пользователя на определенный момент времени.

6.5.4. Для хранения личного закрытого ключа применять любой носитель, поддерживаемый используемым средством криптографической защиты информации и Удостоверяющим центром.

**3. Порядок предоставления и пользования услугами Удостоверяющего центра**

3.1. Порядок получения электронной цифровой подписи в первый раз.

Для получения электронной цифровой подписи (далее ЭЦП) необходимо:

* 1. Обратиться в УЦ одним из удобных для вас способов:
* 6286000, г. Нижневартовск, ул. Ленина, 6. каб. 513. (по предварительной записи по телефону!);
* Тел. 8(3466) 49-84-35, 8(3466) 49-84-40, 8 (3466) 49-84-44
* E-mail: uprinf@nvraion.ru
  1. Получить комплект документов и образцов для заполнения у оператора УЦ:
     1. Бланк заявления на регистрацию Пользователя УЦ (Приложение № 1 к настоящему Порядку);
  2. Заполнить и предоставить для проверки комплект документов (по электронной почте на e-mail: uprinf@nvraion.ru ) в УЦ
  3. Связаться с оператором УЦ по телефону для проверки и согласования предоставленного пакета документов либо дождаться ответа оператора УЦ по электронной почте.
  4. Подписать комплект документов и предоставить оригиналы в УЦ (лично, почтой, курьером и др.).
  5. Получить ЭЦП и необходимые документы:
* получить электронную цифровую подпись;
* расписаться в сертификате открытого ключа.

3.2. Регистрация пользователя в Удостоверяющем центре и изготовление сертификата открытого ключа в первый раз и повторные разы.

Регистрация пользователя в Удостоверяющем центре и изготовление сертификата открытого ключа в первый раз осуществляется на основании заявления при личном прибытии пользователя, проходящего процедуру регистрации (либо его полномочного представителя), в офис Удостоверяющего центра.

Форма заявления приведена в Приложении № 1 к настоящему Порядку.

После предоставления в Удостоверяющий центр заявительных регистрационных документов оператором УЦ осуществляется их рассмотрение и обработка. Обработка заявительных регистрационных документов должна быть осуществлена не позднее рабочего дня следующего за рабочим днем, в течение которого указанные документы были приняты Удостоверяющим центром.

В случае отказа в регистрации пользователь уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения оператор УЦ регистрирует пользователя, формирует ключи и сертификат открытого ключа пользователя.

После изготовления сертификата открытого ключа оператор УЦ формирует два экземпляра сертификата открытого ключа на бумажном носителе. Все экземпляры сертификата открытого ключа на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру регистрации, или собственноручной подписью его доверенного представителя, а также собственноручной подписью уполномоченного лица Удостоверяющего центра.

По окончании процедуры регистрации пользователя, формирования ключей и изготовления сертификата открытого ключа пользователю Удостоверяющего центра предоставляются:

* ключевой носитель, содержащий закрытый ключ пользователя Удостоверяющего центра; изданный сертификат открытого ключа пользователя Удостоверяющего центра (в форме файла формата PKCS#7), сертификаты уполномоченного лица Удостоверяющего центра (в форме файла формата PKCS#7);
* один экземпляр изданного сертификата открытого ключа на бумажном носителе;
  1. Плановая смена ключей и сертификата открытого ключа пользователя Удостоверяющего центра аналогично пункту 3.2 настоящего Порядка.
  2. Внеплановая смена ключей и сертификата открытого ключа пользователя Удостоверяющего центра.

Внеплановая смена ключей и сертификата открытого ключа осуществляется пользователем Удостоверяющего центра в следующих случаях:

* При компрометации закрытого ключа пользователя Удостоверяющего центра;
* При компрометации закрытого ключа уполномоченного лица Удостоверяющего центра.

Порядок подачи заявительных документов, принятия по нему решения и предоставления ключевых документов осуществляется в соответствии с пунктом 3.2. настоящего Порядка.

* 1. Аннулирование (отзыв) сертификата открытого ключа пользователя Удостоверяющего центра.

Удостоверяющий центр аннулирует (отзывает) сертификат открытого ключа пользователя в следующих случаях:

* по истечении срока его действия;
* при компрометации закрытого ключа уполномоченного лица Удостоверяющего центра;
* по заявлению пользователя Удостоверяющего центра;
* по заявлению на отзыв доверенности пользователя Удостоверяющего центра.

Удостоверяющий центр отзывает сертификат открытого ключа пользователя только в период действия закрытого ключа, соответствующего данному сертификату.

* + 1. Отзыв сертификата открытого ключа по заявлению пользователя Удостоверяющего центра

Заявление на отзыв сертификата открытого ключа оформляется по форме Приложения № 2 настоящего Порядка и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

После получения Удостоверяющим центром заявления на отзыв сертификата открытого ключа оператором УЦ осуществляется его рассмотрение и обработка. Обработка заявления на отзыв сертификата должна быть осуществлена не позднее

рабочего дня следующего за рабочим днем, в течение которого указанное заявление было принято Удостоверяющим центром.

В случае отказа в отзыве сертификата открытого ключа Удостоверяющий центр уведомляет об этом пользователя Удостоверяющего центра.

При принятии положительного решения оператор УЦ отзывает сертификат открытого ключа.

Официальным уведомлением о факте отзыва сертификата открытого ключа является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени предоставления заявления на отзыв сертификата. Временем отзыва сертификата открытого ключа признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты открытых ключей в расширение CRL Distribution Point (CDP).

10.9. Подтверждение подлинности ЭЦП в электронном документе.

Подтверждение подлинности ЭЦП в электронном документе осуществляется на основании заявления, направляемого пользователем УЦ. Данное заявление оформляется по форме Приложения № 3 настоящего Порядка и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

* время и дата подачи заявления;
* идентификационные данные пользователя, подлинность ЭЦП которого необходимо подтвердить в электронном документе;
* время и дата, на момент наступления которых, требуется установить подлинность ЭЦП.

Обязательным приложением к заявлению на подтверждение подлинности ЭЦП в электронном документе является магнитный носитель, содержащий:

* сертификат открытого ключа, с использованием которого необходимо осуществить подтверждение подлинности ЭЦП в электронном документе;
* электронный документ - в виде одного файла формата PKCS#7, содержащего данные и значение ЭЦП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭЦП этих данных формата PKCS#7.

Проведение работ по подтверждению подлинности ЭЦП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

По результатам проведения работ по подтверждению подлинности ЭЦП в электронном документе Удостоверяющим центром оформляется заключение.Заключение содержит:

* результат подтверждения подлинности ЭЦП в электронном документе;
* отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

* время и место проведения проверки;
* состав комиссии, осуществлявшей проверку;
* основание для проведения проверки;
* содержание и результаты проверки;
* данные, представленные для проведения проверки.

Заключение составляется в простой письменной форме, подписывается всеми членами комиссии, заверяется печатью Удостоверяющего центра и предоставляется заявителю.

Предоставление заявителю заключения по подтверждению подлинности ЭЦП должно быть осуществлено не позднее десяти рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

Приложение № 1

Начальнику отдела по информатизации

и сетевым ресурсам администрации района

Д.С. Морозу

Заявление на получение сертификата ЭЦП, ключей ЭЦП для работы в корпоративной информационной системе департамента финансов администрации района

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

(полное наименование организации, включая организационно-правовую форму)

находящееся по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(почтовый адрес организации)

в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(должность)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество)

действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Просит зарегистрировать уполномоченного представителя

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

(фамилия, имя, отчество)

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

(должность)

в корпоративной информационной системы департамента финансов администрации района, наделить полномочиями Пользователя корпоративной информационной системы департамента финансов администрации района, и сформировать ключи подписи и изготовить сертификат ключа подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

|  |  |
| --- | --- |
| CommonName (CN) | Общее имя – Фамилия, Имя, Отчество |
| Title (T) | Должность |
| E-Mail (E) | Адрес электронной почты |
| Organization (O) | Наименование организации |
| OrganizationUnit (OU) | Наименование подразделения |
| Locality (L) | Город |
| State (S) | Область |
| Contry (C) | Страна |

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

Администратор УЦ / /

Приложение № 2

Заявление на аннулирование (отзыв) сертификата открытого ключа Пользователя УЦ (форма)

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность)

(фамилия, имя, отчество)

действующего на основании

в связи с

(причина отзыва сертификата)

Просит отозвать сертификат открытого ключа своего уполномоченного представителя - пользователя УЦ:

(фамилия, имя, отчество пользователя УЦ)

содержащий следующие данные:

|  |  |  |
| --- | --- | --- |
| SerialNumber (SN) | Серийный номер сертификата ключа подписи | |
| CommonName (CN) | Общее имя - Фамилия, Имя, Отчество | |
| Title (T) | Должность | |
| E-Mail (E) | Адрес электронной почты | |
| Organization (0) | Наименование организации | |
| OrganizationUnit (OU) | Наименование подразделения | |
| Locality (L) | Город | |
| State (S) | Область | |
| Contry (C) | Страна | |
| Extended Key Usage | Проверка подлинности клиента Защищенная электронная почта Пользователь Центра Регистрации | (1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4) (1.2.643.2.2.34.6) |

Владелец сертификата открытого ключа / /

« » 20 г.

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

« : » « / / »

час минута день месяц год

Администратор УЦ / /

Приложение № 3

Заявление на подтверждение подлинности электронной цифровой подписи в

электронном документе (форма)

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность)

(фамилия, имя, отчество)

действующего на основании

Просит подтвердить подлинность ЭЦП в электронном документе на основании следующих данных:

1. Файл формата PKCS#7, содержащий сертификат открытого ключа, с использованием которого необходимо осуществить подтверждение подлинности ЭЦП в электронном документе на прилагаемом к заявлению магнитном носителе - per № МД-ХХХ;
2. Файл, содержащий подписанные ЭЦП данные и значение ЭЦП формата PKCS#7, либо файл, содержащий исходные данные и файл, содержащий значение ЭЦП формата PKCS#7 на прилагаемом к заявлению магнитном носителе - per. № МД- ХХХ
3. Время и дата[[1]](#footnote-1) на момент наступления которых требуется подтвердить подлинность ЭЦП: « : » « / / »;

час минута день месяц год

Должность и Ф.И.О. руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

(Заполняется в Удостоверяющем центре)

Время и дата принятия заявления:

« : » « / / »

час минута день месяц год

Администратор УЦ / /

20 г.

1. Время и дата должны быть указаны с учетом часового пояса г. Ханты-Мансийск. Если время и дата не указаны, то подтверждение подлинности ЭЦП устанавливается на момент времени принятия заявления Удостоверяющим центром [↑](#footnote-ref-1)