

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ОРЛОВСКАЯ ОБЛАСТЬ

 АДМИНИСТРАЦИЯ ЗАЛЕГОЩЕНСКОГО РАЙОНА

 ПОСТАНОВЛЕНИЕ

 30 декабря 2019 год\_\_\_\_\_\_ № 908

 п. Залегощь

Об утверждении Положения

об электронной подписи администрации

Залегощенского района Орловской области

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации"; Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (Приказ ФАПСИ от 13 июня 2001 года № 152), администрация Залегощенского района п о с т а н о в л я е т:

 1.Утвердить Положение об электронной подписи в администрации Залегощенского района Орловской области, согласно приложению.

 2. Отделу по организационно - кадровой работе и делопроизводству (Котова М.В.) разместить данное постановление на официальном сайте администрации Залегощенского района.

 3.Контроль над выполнением данного постановления возложить на заместителя Главы администрации Щукину О.В.

 Глава района В.Н. Брежнев

Приложение

 к постановлению администрации

 Залегощенского района

 от 30 декабря 2019г. № 908

**Положение**

**об электронной подписи в администрации**

**Залегощенского района орловской области**

1. Общие положения

1.1. Настоящее Положение об электронной подписи в администрации Залегощенского района Орловской области разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации"; Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (Приказ ФАПСИ от 13 июня 2001 года № 152) и определяет:

* порядок обеспечения правовых условий, при соблюдении которых электронная подпись (далее – ЭП) в электронном документообороте признается равнозначной собственноручной подписи в документе на бумажном носителе;
* порядок использования ключей ЭП в информационных системах, используемых администрацией Залегощенского района Орловской области;
* порядок взаимодействия уполномоченных лиц администрации Залегощенского района Орловской области в сфере обращения с ключами ЭП;
* порядок выдачи и отзыва сертификатов ключей проверки ЭП уполномоченных лиц администрации Залегощенского района Орловской области, использующих ЭП;
* порядок включения и исключения сотрудников администрации Залегощенского района Орловской области для простановки ЭП на электронных документах (далее – ЭД);
* основные организационно-технические мероприятия, направленные на обеспечение безопасности при работе со средствами криптографической защиты информации.

1.2. Действие настоящего Положения распространяется на должностных лиц, определенных распоряжением администрации Залегощенского района Орловской области.

1.3. Информационные системы, используемые администрацией Залегощенского района Орловской области являются системами, участники электронного взаимодействия которой используют для собственных нужд усиленную неквалифицированную электронную подпись.

1.4. В администрации Залегощенского района Орловской области, используются только сертифицированные средства электронной подписи.

Использование несертифицированных средств электронной подписи и созданных ими ключей электронной подписи не допускается.

1.5. Электронная подпись используется строго в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи.

**2. Термины и сокращения, используемые в Положении**

2.1. **Электронная подпись** (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию; получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.

2.2. **Сертификат ключа проверки электронной подписи (СКПЭП)** - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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

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

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

2.6. **Владелец ключа электронной подписи** - сотрудник организации, который приказом руководителя организации наделен правом простановки ЭП на электронных документах и имеющий СКПЭП.

2.7. **Регистрационная карточка сертификата ключа проверки электронной подписи** –документ на бумажном носителе, который формируется в момент генерации СКПЭП, в двух экземплярах, имеющих одинаковую юридическую силу, подписывается уполномоченными сотрудниками, скрепляется печатями, и содержит:

* уникальный регистрационный номер СКПЭП;
* даты начала и окончания срока действия СКПЭП
* фамилию, имя и отчество владельца ключа ЭП;
* должность владельца ключа ЭП;
* структурное подразделение владельца ключа ЭП;
* содержимое файла СКПЭП в шестнадцатеричном виде, позволяющем восстановить файл СКПЭП в электронном виде;
* наименование средств ЭП, с которыми используется СКПЭП;
* наименование и место нахождения удостоверяющего центра, выдавшего СКПЭП;
* описание отношений, для которых создан СКПЭП.

Регистрационная карточка СКПЭП подлежит хранению на срок не меньший срока исковой давности для ЭД, подписанных соответствующими ключами ЭП.

2.8. **Удостоверяющий центр** - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные федеральными законами;

2.9. **Аккредитация удостоверяющего центра** - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям федеральных законов;

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

2.11. **Участники электронного взаимодействия** - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации;

2.12. **Компрометация ключевой информации** – событие, определенное владельцем ключевой информации, как ознакомление неуполномоченным лицом (лицами) с его ключевой информацией, утеря ключевого носителя, копирование или другие причины появления у владельца ключевой информации сомнений в сохранении ее тайны.

2.13. **Средства криптографической защиты информации** (далее – **СКЗИ**) – средства шифрования, ЭП, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации).

2.14. **Электронный обмен** – проведение Сторонами операций обмена информацией с использованием ЭД, подписанными ЭП, по открытым или защищенным каналам связи.

2.15. **Криптографический ключ (криптоключ)** – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

2.16. **Ключевая информация** – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

2.17. **Ключевой документ** – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

2.18. **Ключевой носитель** – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory,Rutoken, eToken и т.п.).

2.19. **Конфликтная ситуация**– ситуация, при которой у владельца сертификата ключа проверки электронной подписи возникает необходимость разрешения вопросов признания или непризнания авторства и/или подлинности электронных документов, обработанных средствами криптографической защиты информации.

2.25. Сокращения, используемые в Положении:

**ЭД** – электронный документ;

**ЭП** – электронная подпись;

**КПЭП** – ключ проверки электроннойподписи;

**СКПЭП** – сертификата ключа проверки электронной подписи

**ИБ** – информационная безопасность;

**АРМ** – автоматизированное рабочее место;

**Спецпомещения** – помещения, в которых находятся СКЗИ и/или хранятся ключевые документы к ним.

3. Сроки действия криптографических ключей и сертификатов ключей ЭП, порядок их учета и хранения

3.1. Единицей ключевых носителей считается ключевой носитель многократного использования (Rutoken, eToken, USB флеш-накопитель).

3.2. Срок действия криптоключей не может превышать 1 года.

3.3. Все полученные экземпляры ключевых документов должны быть получены под расписку несущим персональную ответственность за их сохранность.

3.4. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только сотрудникам администрации Залегощенского района Орловской области.

3.5. Пользователи СКЗИ хранят ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.6. Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих (экз. № 1) и резервных (экз. № 2) ключевых документов.

3.7. В случае отсутствия у владельцев ключей ЭП шкафов (ящиков, хранилищ) индивидуального пользования, исключающих бесконтрольный доступ к ним, учет и хранение ключевых документов владельцев ключей ЭП осуществляет администратор ИБ.

 Ключевые носители ЭП выдаются по Журналу выдачи ключевых носителей (Приложение № 1 к настоящему Положению) с отметкой даты и времени выдачи, даты и времени возвращения ключевых носителей.

3.8. Запрещается:

* осуществлять копирование ключевой информации на носители не являющиеся ключевыми;
* передавать носители ключевой информации лицам, к ним не допущенным;
* выводить ключевую информацию на дисплей и принтер;
* вставлять ключевой носитель в дисковод ПЭВМ в режимах, не предусмотренных функционированием средств обмена ЭД, а также в дисководы других ПЭВМ;
* записывать на ключевой носитель постороннюю информацию.

3.9. Плановая смена ключей ЭП производится один раз в год в связи с истечением установленного срока их действия.

Процедура получения новых сертификатов СКПЭП идентична процедуре их первоначального получения.

3.10. Внеплановая смена ключей ЭП производится до окончания срока их действия, в случае компрометации соответствующего криптоключа.

3.12. Плановая смена криптоключей администрации Залегощенского района Орловской области производится не позднее 10 рабочих дней до даты окончания срока их действия. При этом оформляется новый СКПЭП.

**4. Прекращение действия ключей ЭП.**

**Порядок уничтожения ключевых документов**

4.1. Неиспользованные или выведенные из действия криптографические ключи должны быть уничтожены на месте.

 4.2. СКПЭП и регистрационные карточки СКПЭП уничтожаются только после истечения сроков хранения электронных документов, подписанных соответствующими ключами ЭП.

4.3. Уничтожение ключевых дискет производится путем физического уничтожения ключевого носителя, на котором они расположены, методом разрезания.

4.4. Криптоключи на Rutoken, eToken, USB флеш-накопитель стирают по технологии, принятой для соответствующих ключевых носителей многократного использования.

4.5. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин после окончания установленного для них срока хранения.

4.6. Криптоключи должны быть уничтожены в срок не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета.

4.7. Ключевые документы уничтожаются c оформлением акта уничтожения.

При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи.

После уничтожения владельцы ключей ЭП должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ОКЗ для списания уничтоженных документов с их лицевых счетов.

Не реже одного раза в год ПБС должны направлять в ОКЗ копии актов об уничтожении ключевых документов.

4.8. Уничтожение производит комиссия в составе не менее двух человек из числа владельцев ключей ЭП ПБС и администратора ИБ. В акте указывается, что именно уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации.

Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении.

О проведенном уничтожении делаются отметки в Журнале учета СКЗИ. Номер акту присваивается по журналу учета входящих документов организации.

**5. Действия в случае компрометация ключевых документов**

5.1. К событиям, связанным с компрометацией криптоключей относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Прекращение полномочий или увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (после окончания срока действия) криптографического ключа.
5. Возникновение подозрений на утечку ключевой информации или ее искажение.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями с записанным на них криптографическими ключами (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

5.2. Мероприятия по розыску и локализации последствий компрометации информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной ключевой информации.

6. Ответственность владельцев ключей ЭП и сотрудников ОКЗ

6.1. За неисполнение или ненадлежащее исполнение обязанностей в соответствии с настоящим Положением сотрудники ОКЗ несут ответственность в соответствии с действующим законодательством Российской Федерации.

6.2. Владелец ключа ЭП несет ответственность за сохранность своих криптографических ключей.

6.3. Администратор ИБ, его заместитель и владелец ключа ЭП обязаны:

* не разглашать информацию, к которой они допущены, в том числе сведения о [криптоключах](#sub_901);
* соблюдать требования к обеспечению безопасности информации с использованием СКЗИ;
* сообщать в ОКЗ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или [ключевых документах](#sub_904) к ним;
* сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящим Положением, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
* немедленно сообщать в ОКЗ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений, а также о причинах и условиях возможной утечки таких сведений.

6.4. В случае если владелец ключа ЭП допустил компрометацию криптографических ключей и не уведомил об этом факте ОКЗ, то всю ответственность за возможные при этом последствия несет допустивший компрометацию владелец ключа ЭП.

Приложение № 1

к Положению, утвержденному постановлением администрации Залегощенского района Орловской области

 от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ года № \_\_\_\_

**ЖУРНАЛ**

**выдачи ключевых носителей**

|  |  |  |  |
| --- | --- | --- | --- |
| *№ п.п.* | Учетный номер ключа | Выдано | Возвращено |
| Дата | Время | Ф. И. О. | Роспись | Дата | Время | Роспись |
| *1* | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |