

Муниципальное образование

«ЗАНЕВСКОЕ ГОРОДСКОЕ ПОСЕЛЕНИЕ»

Всеволожского муниципального района Ленинградской области

**АДМИНИСТРАЦИЯ**

**ПОСТАНОВЛЕНИЕ**

30.07.2020 № 368

д. Заневка

Об утверждении Положения

об использовании электронной

цифровой подписи администрации

муниципального образования

«Заневское городское поселение»

Всеволожского района Ленинградской области

В соответствии с Федеральными законами от 27 июля 2006 года
№ 149-ФЗ «Об информации, информационных технологиях и о защите информации»; от 06 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, утвержденной Приказом ФАПСИ от 13 июня 2001 года № 152, Уставом муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области, администрация муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области

**ПОСТАНОВЛЯЕТ:**

1. Утвердить прилагаемое Положение об использовании электронной цифровой подписи администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области.
2. Настоящее постановление вступает в силу после его подписания.
3. Контроль за исполнением постановления возложить на заместителя главы администрации Гречица В.В.

Глава администрации А.В. Гердий

Приложение

УТВЕРЖДЕНО

постановлением администрации

МО «Заневское городское поселение»

от 30.07.2020 № 368

**Положение**

**об использовании электронной цифровой подписи администрации**

**муниципального образования «Заневское городское поселение»**

 **Всеволожского муниципального района Ленинградской области**

1. Общие положения

 1.1. Настоящее Положение об электронной цифровой подписи администрации муниципального образования «Заневское городского поселение» Всеволожского муниципального района Ленинградской области (далее - Положение)разработано в соответствии с Федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 06 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, утвержденной Приказом ФАПСИ от 13 июня 2001 года № 152 и определяет:

порядок обеспечения правовых условий, при соблюдении которых усиленная квалифицированная цифровая электронная подпись (далее ЭЦП) в электронном документообороте признается равнозначной собственноручной подписи в документе на бумажном носителе;

порядок использования ключей ЭЦП в информационных системах администрации;

основные организационно-технические мероприятия, направленные на обеспечение безопасности при работе со средствами криптографической защиты информации.

1.2. Термины и сокращения, используемые в Положении

1.2.1. Ответственный специалист – полномочное лицо муниципального казенного учреждения «Центр оказания услуг», назначенное для обеспечения информационной безопасности администрации муниципального образования «Заневское городское поселение» Всеволожского муниципального района Ленинградской области (далее – администрация) при обмене электронными документами с использованием ЭЦП ( по согласованию).

1.2.2. Электронная усиленная квалифицированная цифровая подпись (ЭЦП) – 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.

1.2.3. Cертификат ключа проверки электронной цифровой подписи (СКПЭЦП) - 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.

1.2.4. Квалифицированный сертификат ключа проверки электронной цифровой подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной цифровой 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).

1.2.5. Ключ электронной цифровой подписи - уникальная последовательность символов, предназначенная для создания электронной цифровой подписи;

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

1.2.7. Владелец ключа электронной цифровой подписи – должностное лицо администрации, наделённый правом простановки ЭЦП на электронных документах и имеющий СКПЭЦП.

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

уникальный регистрационный номер СКПЭЦП;

даты начала и окончания срока действия СКПЭЦП

фамилию, имя и отчество владельца ключа ЭЦП;

должность владельца ключа ЭЦП;

структурное подразделение владельца ключа ЭЦП;

содержимое файла СКПЭЦП в шестнадцатиричном виде, позволяющем восстановить файл СКПЭЦП в электронном виде;

наименование средств ЭЦП, с которыми используется СКПЭЦП;

наименование и место нахождения удостоверяющего центра, выдавшего СКПЭЦП;

описание отношений, для которых создан СКПЭЦП.

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

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

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

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

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

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

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

1.2.15. 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, eToken и т.п.).

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

1.2.17. Компрометация ЭЦП — факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

1.2.18. Сокращения, используемые в настоящем Положении:

ЭД – электронный документ;

ЭЦП – электронная усиленная квалифицированная цифровая подпись;

КПЭЦП – ключ проверки электронной цифровой подписи;

СКПЭЦП – сертификата ключа проверки электронной цифровой подписи

ИБ – информационная безопасность;

АРМ – автоматизированное рабочее место;

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

1.3. Действие настоящего Положения распространяется на следующих должностных лиц администрации:

глава администрации;

заместитель главы администрации;

начальник финансово-экономического сектора-централизованной бухгалтерии;

начальник сектора ЖКХ и благоустройства;

начальник сектора архитектуры, градостроительства и землеустройства;

начальник сектора организационной работы;

начальник сектора по управлению муниципальным имуществом, учета и распределения муниципального жилищного фонда;

1.4. Информационная система администрации является корпоративной информационной системой, участники электронного взаимодействия которой используют для собственных нужд усиленную квалифицированную электронную подпись.

1.5. Функции удостоверяющего центра для администрации определены следующими организациями:

Удостоверяющий центр государственного казенного учреждения Ленинградской области "Оператор" электронного правительства" (ГКУ ЛО "ОЭП") (по согласованию);

ООО «Удосверяющий центр «Тензор» (по согласованию);

Удостоверящию центр АО «ПФ «СКБ Контур» (по согласованию).

1.6. Внешним органом обеспечения построения и сопровождения защищённых сетей ОИВ и обеспечения построения, развития и сопровождения защищённого сегмента ЕСПД ОИВ администрации является Комитет цифрового развития Ленинградской области (по согласованию), Удостоверяющий центр государственного казенного учреждения Ленинградской области «Оператор" электронного правительства» (ГКУ ЛО «ОЭП»)(по согласованию).

1.7. В администрации и организациях, участие которых в обмене ЭД регламентировано договором с администрацией и которые являются участниками информационной системы МО «Заневское городское поселение», используются только сертифицированные средства электронной подписи.

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

1.8. Для подписания и обмена электронными документами между администрацией с государственными органами, органами местного самоуправления, организациями, физическими лицами, не являющимися участниками информационной системы администрации, используется усиленная квалифицированная электронная цифровая подпись.

1.9. Для подписания финансовых, бухгалтерских и налоговых документов, отчетностей, запросов, сверок и иной документации в сфере финансово-экономической деятельности администрации. используется усиленная квалифицированная электронная цифровая подпись.

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

2. Порядок изготовления ключей ЭЦП и СКПЭЦП

2.1. Носителями ключевой информации ЭЦП являются:

электронные ключи eToken (Aladdin)

USB флеш-накопитель.

2.2. Порядок изготовления СКПЭЦП сотрудникам администрации определяется в соответствии с требованиями, выставленным удостоверяющим центрами, указанными в п. 1.5 настоящего Положения.

2.3. Учет ключей ЭЦП и регистрационных карточек СКЭЦП осуществляется в Журналe поэкземплярного учета ЭЦП и СКПЭЦП администрации, ведение которого возложена на муниципальное казенное учреждение «Центр оказания услуг» (приложение 1 к настоящему Положению).

3. Сроки действия ЭЦП, порядок их учета и хранения

3.1. Регистрационные карточки запроса на СКПЭЦП, а также регистрационные карточки СКПЭЦП, подлежат поэкземплярному учету в Журнале учета ЭЦП и СКПЭЦП.

Срок их хранения равен сроку хранения электронных документов, подписанных соответствующими ключами ЭЦП.

3.2. Срок действия криптоключей не может превышать 1 года.

3.3. Владельцы ключей хранят ЭЦП в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.4. В случае отсутствия у владельцев ключей ЭЦП шкафов (ящиков, хранилищ) индивидуального пользования, исключающих бесконтрольный доступ к ним, учет и хранение ключевых документов владельцев ключей ЭЦП осуществляет ответственным сотрудником .

 Ключевые носители этим владельцам ключей ЭЦП выдаются по Журналу выдачи ключевых носителей (приложение 2 к настоящему Положению) с отметкой даты и времени выдачи, даты и времени возвращения ключевых носителей.

3.5. 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 ПЭВМ в режимах, не предусмотренных функционированием средств обмена ЭД, а также в дисководы других ПЭВМ;

записывать на ключевой носитель постороннюю информацию.

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

Процедура получения новых сертификатов СКПЭЦП идентична процедуре их первоначального получения.

3.7. Внеплановая смена ключей ЭЦП производится до окончания срока их действия, в случае компрометации ЭЦП.

3.8. Плановая смена ЭЦП администрации производится по инициативе ответственного сотрудника не позднее 20 рабочих дней до даты окончания срока их действия. При этом оформляется новый СКПЭЦП.

**4. Прекращение действия ключей ЭЦП**

4.1. СКПЭЦП и регистрационные карточки СКПЭЦП уничтожаются только после истечения сроков хранения электронных документов, подписанных соответствующими ключами ЭЦП .

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

4.3. Бумажные и прочие сгораемые ключевые носители уничтожаются путем сжигания или с помощью любых бумагорезательных машин после окончания установленного для них срока хранения.

4.4. Уничтожение производит комиссия в составе не менее двух человек из числа владельцев ключей ЭЦП иответственного сотрудника. В акте указывается, что именно уничтожается и в каком количестве.

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 ЭЦП и СКПЭЦП .

**5. Действия в случае компрометация ЭЦП**

5.1. К событиям, связанным с компрометацией ЭЦП 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).

Различают два вида компрометации криптографического ключа: явную и неявную*.* Первые четыре события должны трактоваться как явная компрометация ЭЦП. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

При наступлении любого из перечисленных выше событий ответственный сотрудник должен немедленно прекратить обмен ЭД и сообщить о факте компрометации (или предполагаемой компрометации) своему непосредственному руководству и главе администрации.

5.2. Ответственный сотрудник на основе полученных сведений о скомпрометированных ЭЦП формирует список на отзыв СКПЭП.

5.3. При компрометации или подозрению в компрометации ЭЦП проводится служебное расследование по выявлению причин, приведших к компрометации. Результаты служебного расследования доводятся до главы администрации для принятия соответствующих мер.

Скомпрометированные ЭЦП немедленно выводятся из работы, и проводится их экстренная смена.

5.4. Мероприятия по розыску и локализации последствий компрометации информации, передававшейся (хранящейся) организует и осуществляет обладатель скомпрометированной ключевой информации.

6. Хранение и архивирование ключевых документов

6.1. Архивированию у ответственного сотрудника подлежит следующая информация:

договоры с ПБС, учетная информация в соответствии с этими договорами;

запросы на СКПЭЦП;

СКПЭЦП сотрудников администрации;

электронные документы, подписанные ЭЦП.

6.2. Срок архивного хранения документов устанавливается в соответствии со сроками, определенными федеральным законодательством. Для платежных документов он составляет, как правило, не менее 5 лет.

7. Ответственность владельцев ключей ЭЦП

7.1. За неисполнение или ненадлежащее исполнение обязанностей в соответствии с настоящим Положением должностное лицо администрации несет ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. Владелец ключа ЭЦП несет ответственность за сохранность своих криптографических ключей.

7.3.Отвественный сотрудник, его заместитель и владелец ключа ЭЦП обязаны:

не разглашать информацию, к которой они допущены, в том числе сведения о [криптоключах](#sub_901);

соблюдать требования к обеспечению безопасности информации с использованием средств защиты информации ;

сообщать главе администрации о ставших им известными попытках посторонних лиц получить сведения об используемых ЭЦП или [ключевых документах](#sub_904) к ним;

сдать Журнал учета ЭЦП и СКПЭЦП, иную документацию по использованию ЭЦП в соответствии с порядком, установленным настоящим Положением, при увольнении или отстранении от исполнения обязанностей.

7.4. В случае если владелец ключа ЭЦП допустил компрометацию криптографических ключей и не уведомил об этом факте ответственного исполнителя и главу администрации, то всю ответственность за возможные при этом последствия несет допустивший компрометацию владелец ключа ЭЦП.

Приложение 1

к Положению об использовании электронной цифровой подписи администрации «Заневское городское поселение» Всеволожского района

Ленинградской области

# Типовая форма журнала поэкземплярного учета ЭЦП и СКПЭЦП

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Информация по**СКПЭЦП**От кого полученыили Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы | Дата и место получения ЭЦП | Отметка о полученииЭЦП | Дата ввода в эксплуатацию ЭЦП | Дата вывода из эксплуатации ЭЦП | Отметка об уничтожении ЭЦП | Примечание |
| От кого полученыили Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы | Дата и место получения |
| Дата уничтожения | № акта или расписка об уничтожении |
|  |  |  |  |  |  |  |  |  |  |

п

Приложение 2

к Положению об использовании

электронной цифровой подписи

администрации муниципального образования «Заневское городское поселение» Всеволожского района

Ленинградской области

**ЖУРНАЛ**

**выдачи ключевых носителей**

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