



АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
СЕВЕРСКИЙ РАЙОН

РАСПОРЯЖЕНИЕ

от 18.09.2023

станция Северск

№ 140-р

Об утверждении Правил работы с электронной
подписью в администрации муниципального
образования Северский район

2

заместителя главы администрации М.Н. Чернову.

8. Распоряжение вступает в силу со дня его подписания.

Глава муниципального образования
Северский район

А.В. Дорошевский

В целях реализации требований Федерального закона от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи», руководствуясь статьями 31, 66 Устава муниципального образования Северский район:

1. Утвердить Правила работы с электронной подписью в администрации муниципального образования Северский район (далее – Правила) согласно приложению к настоящему распоряжению.
2. Ответственному за обеспечение защиты информации (Сергиевская) организовать контроль и выполнение организационных и технических мероприятий по защите информации при изготовлении электронной подписи согласно Правил.
3. Назначить администратором безопасности, ответственным за прием заявок на изготовление сертификата ключа электронной подписи сотрудников администрации муниципального образования Северский район заместителя начальника управления информатизации и информационной безопасности Подливанова Вячеслава Николаевича.
4. Администратору безопасности (Подливанов) обеспечить мероприятия по обеспечению эксплуатации программно-технических средств автоматизированного рабочего места должностного лица - владельца сертификата ключа электронной подписи и учет криптографических средств в журнале учета.
5. На период болезни, отпуска обязанности администратора информационной безопасности Сергиевскую Наталью Николаевну.
6. Установить, что ответственные лица за выполнение требований по защите информации при эксплуатации информационных систем принимают организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные Правилами;
7. Контроль за выполнением настоящего распоряжения возложить на

УТВЕРЖДЕНЫ

распоряжением администрации
муниципального образования

Северский район
от 18.09.2023 № 140-р.

ПРАВИЛА работы с электронной подписью в администрации муниципального образования Северский район

1. Общие положения

1.1. Правила работы с электронной подписью в структурных подразделениях администрации муниципального образования Северский район (далее – Правила) разработаны на основании требований:

Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

Приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (далее – приказ ФАПСи);

Приказа Федерального казначейства от 14 сентября 2018 года № 261 «Об утверждении Регламента удостоверяющего центра Федерального казначейства и признании утратившими силу некоторых приказов Федерального казначейства» (далее – приказ ФК).

1.2. Правила описывают поведение сотрудников администрации муниципального образования Северский район (далее – администрации) при использовании электронной подписи в электронных информационных системах (федеральных, региональных или локальных).

2. Термины и сокращения

2.1. Электронная подпись (далее – 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.

2.2. Электронная подпись состоит из 2х компонентов – закрытой части (контейнера) и открытой части (сертификата).

2.3. Носитель ЭП - материальный носитель информации, содержащий закрытую ЭП. В качестве такого материального носителя электронной подписи могут выступать флеш-носители, e-Token, ruToken.

2.4. Администратор информационной безопасности (далее – Администратор ИБ) – сотрудник управления информатизации и информационной безопасности, назначенный ответственным за изготовление, продление и учет электронных подписей.

2.5. ЭП ОВ – электронная подпись органа власти – администрации как юридического лица. Выдается организацией, зарегистрированной в Федеральной налоговой службе.

2.6. ЭП СП – электронная подпись сотрудника структурного подразделения администрации (подпись физического лица).

2.7. Сертификат ключа проверки электронной подписи (далее -сертификат ЭП) - 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.

2.8. СКЗИ – средства криптографической защиты информации.

2.9. УЦ ФК– удостоверяющий центр Федерального казначейства.

2.10. ИС – информационная система.

3.Право пользования электронной подписью

3.1. Безусловным правом пользования электронной подписью (ЭП СП и ЭП ОВ) наделены: глава администрации и заместители главы администрации. Фактом, подтверждающим назначение сотрудника на должность руководителя администрации, является наличие его фамилии в выписке из единого реестра юридических лиц федеральной налоговой службы (далее – ФНС). Данная информация находится в открытом доступе по адресу <https://egrul.nalog.ru/>.

3.2. Другие сотрудники администрации получают право пользования личной ЭП СП либо СП ОВ на основании распоряжения администрации. В распоряжении должны быть указаны конкретные информационные системы, в которых сотрудник администрации получает право применять ЭП СП или ЭП ОВ.

3.3. Правила использования типов подписи (ЭП СП либо ЭП ОВ) определяет оператор информационной системы. Пользователи информационной системы применяют тот вид ЭП, которые установлены оператором ИС.

3.4. Если оператор информационной системы требует под электронным документом наличие только ЭП ОВ (руководителя организации) (например – Распоряжения) то для обеспечения оперативной и непрерывной деятельности администрации в этой ИС глава администрации издает распоряжение администрации, в котором передает право (доверяет, уполномочивает) использовать своего ЭП ОВ ответственным сотрудникам администрации, указав наименование информационной системы и цели, для которых сотрудники получают право применять ЭП главы администрации.

3.5. К такому распоряжению администрации также предоставляется достоверность главы администрации на проведение мероприятий в ИС: внесение данных, изменений в размещенную ранее информацию, подписание документов, отpravку сведений, подписанных электронной подписью сотрудника и другие действия, которые глава муниципального образования Северский район доверит производить сотруднику администрации – владельцу электронной подписи, действующему в ИС от имени администрации).

4. Получение (генерация) электронной подписи

4.1. Данный раздел Правил описывает действия сотрудников по получению электронной подписи с помощью портала Федерального казначейства на сайте (<https://fsz.poskazna.ru/>).

4.2. Работу с ЭП координирует Администратор ИБ администрации. Все необходимые действия по генерации, получению, продлению и блокированию ЭП ОВ и ЭП СП, порядок генерации ЭП регламентируются Регламентом УЦ ФК, актуальным на день генерации ЭП.

4.3. ЭП изготавливается администратором ИБ и помещается на ключевой носитель. Информация о сертификате ЭП, владельцы ЭП, дате выдачи, дате окончания срока действия сертификата ЭП заносится в журнал покемпированного учета внешних носителей персональных данных и ЭЦП (далее – Журнал).

4.4. При выдаче ЭП Администратор ИБ проводит инструктаж с пользователями по хранению, обращению и эксплуатации с ЭП.

4.5. После проведения инструктажа сотрудник администрации, получивший ЭП распределяется в Журнале о получении носителя ЭП и сертификата ЭП.

4.6. Испорченный носитель ЭП сотрудник администрации возвращает администратору ИБ для последующего уничтожения.

5. Порядок хранения и использования носителей ЭП

5.1. Хранилищем для носителя ЭП может служить сейф, замкнутый и опечатываемый ящик, опечатываемый контейнер.

5.2. Хранение носителей ЭП, выданных разным сотрудникам, допускается в одном общем хранилище при условии, что носители ЭП каждого сотрудника упакованы в личный контейнер (бокс, конверт и т.п.) и опечатан личным маркером. В качестве маркера могут служить личная печать сотрудника, пломбировочные наклейки на контейнер и другие средства, контролирующие факт вскрытия личного хранилища посторонним лицом.

6. Обязанности сотрудников

6.1. Обязанности сотрудника, наделенного правом пользования ЭП:

6.1.1. Обеспечить хранение носителей ЭП в хранилище в личном контейнере в нерабочее время.

6.1.2. Перед вскрытием контейнера проверить целостность маркера.

6.1.3. Использовать ЭП только для целей, предусмотренных распорядительными документами, закрепляющим данное право.

6.1.4. Ключи ЭП на ключевом носителе должны быть защищены паролем (ПИН-кодом) соответствующей сложности.

6.1.5. В компьютере на учетную запись пользователя операционной системы должен быть установлен пароль, удовлетворяющий требованиям, приведенным в разделе 3 Правил.

6.1.6. Личные пароли и ПИН-коды сотрудник не имеет право никому сообщать.

6.1.7. Запрещается оставлять без контроля компьютер, на которых эксплуатируется ЭП после ввода ключевой информации. При уходе пользователя с рабочего места компьютер должен быть заблокирован, а носители ЭП убраны в хранилище.

6.1.8. Не записывать на носитель с ЭП любую другую информацию, кроме компонентов ЭП.

6.1.9. При физической порче носителя ЭП сотрудник уведомляет об этом администратора ИБ. Далее администратор ИБ изготавливает новую копию ЭП на новый носитель.

6.1.10. При подозрении на компрометацию ЭП – сообщить о данном факте руководителю подразделения, предпринять все необходимые оперативные действия по замене ЭП: блокировке скомпрометированной ЭП и изготовлению новой, сообщить руководителю подразделения и в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним.

6.1.11. Немедленно уведомить руководителя подразделения и орган криптографической защиты 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 конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

6.1.12. При увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, необходимо сдать администратору ИБ носители ЭП, эксплуатационную и техническую документацию к ним, ключевые документы.

6.1.13. Контролировать срок жизни ЭП. Заблаговременно (не позже, чем за 14 календарных дней) до даты истечения срока действия ЭП предпринимать необходимые действия по продлению действия ЭП на новый срок, не допускать срыва в работе по причине невовремя изготовления ЭП СП.

6.1.14. Не допускать к работе на закреплённой компьютере с установленной СКЗИ третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе.

6.1.15. Сотрудники, допущенные к работе с ЭП, несут персональную ответственность за безопасность (сохранение в тайне) закрытых компонентов ЭП,

обязаны обеспечивать их сохранность и нераспространение, несут персональную ответственность за нарушение требований настоящих Правил, за неправомерное использование ЭП, компрометацией используемых ЭП, нарушений положений Регламента оказания услуг Удостоверяющего центра.

6.2. Обязанности администратора ИБ:

6.2.1. Подготовить носители для ключевой информации (флэш-носитель, token): каждый носитель должен иметь уникальную маркировку и быть зарегистрирован в Журнале учета СКЗИ.

6.2.2. Своевременно выдавать подготовленные ключевые носители ответственным сотрудникам.

6.2.3. Контролировать выполнение сотрудниками администрации правил работы с личным ключевыми носителями. При выявлении фактов нарушения правил уведомлять об этом руководителя структурного подразделения.

6.2.4. Формировать заявки на ЭП только на основании распорядительных документов, организующих работы сотрудников структурных подразделений с СКЗИ.

6.2.5. Заблаговременно направлять главе муниципального образования Серовский район предложения по приобретению, уничтожению носителей ключевой информации.

6.2.6. Обеспечить сотрудников структурных подразделений достаточным количеством электронных носителей ключевой информации, хранилищ для ЭП (запираемых шкафов, сейфов, контейнеров) индивидуального пользования.

6.2.7. Обеспечить приобретение лицензионного программного обеспечения, операционных систем, антивирусных программ в достаточном количестве для всех рабочих станций с установленными СКЗИ.

6.2.8. Проводить периодический контроль работы сотрудников в части соблюдения Правил работы с ключевыми носителями.

6.2.9. Принимать организационные административные меры, стимулирующие сотрудников на качественное выполнение данных Правил.

7. Порядок уничтожения ЭП на ключевых носителях

7.1. ЭП может быть выведена из действия и уничтожена в следующих случаях:

- плановая смена ключей;
- изменение должностных обязанностей владельца ЭП СП, повлёкших исключение права на использование ЭП;
- компрометация ЭП;
- выход из строя (износ, порча) ключевых носителей.

7.2. Удаление ключей на работоспособном носителе после прекращения срока действия ЭП возлагается на пользователя ЭП при необходимости совместно с администратором ИБ. Ключи должны быть уничтожены не позднее 10 рабочих дней после вывода их из действия.

7.3. Уничтожение ключей на рабочем носителе производится путем стирания (разрушения) ключей специальным программным продуктом (КриптоПРО) без повреждения ключевого носителя.

7.4. Уничтожение носителя ЭП в случае его порчи производится путем его физического уничтожения (разрушения). Данный факт фиксируется в Журнале учёта СКЗИ.

8. Ответственность сотрудников

Сотрудники, наделенные правом пользования ЭП, нарушающие положения данных Правил и других требований законодательства, несут персональную административную ответственность.

Начальник управления информатизации
и информационной безопасности

Н.Н.Сергиевская