



Министерство образования и молодежной политики
Свердловской области

Государственное автономное профессиональное образовательное учреждение
Свердловской области

«Екатеринбургский техникум химического машиностроения»

Инструкция по правилам обращения с ЭЦП

Рассмотрено
на заседании Совета
ГАПОУ СО «ЕТХМ»
Протокол № 06,
от « 15 » июня 2020 г.

УТВЕРЖДЕНО
Приказом директора
ГАПОУ СО «ЕТХМ»
№ 174 - о/д от « 15 » июня 2020 г.



**ИНСТРУКЦИЯ
по правилам обращения с ключевыми документами
электронной цифровой подписи
в ГАПОУ СО «ЕТХМ»**

Екатеринбург
2020 г.

Введено в действие с 15.06.2020 г.

1. Общие положения

1.1. Настоящая Инструкция разработана на основании Федерального закона от 06.04.2011 Г. № 63-ФЗ «Об электронной подписи».

1.2. Инструкция определяет правила обращения с ключевыми документами электронной цифровой подписи (далее - ЭЦП) в том числе при работе со средствами криптографической защиты информации (далее - СКЗИ) и в информационной системе ГАПОУ СО «ЕТХМ».

1.3. СКЗИ и ЭЦП предназначены для подписания электронных документов с целью подтверждения подлинности информации, ее авторства и шифрования при передаче по открытым каналам связи для обеспечения конфиденциальности.

1.4. ЭЦП является реквизитом электронного документа и предназначена для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать пользователя, а также установить отсутствие искажения информации в электронном документе.

1.5. Наделение сотрудника ГАПОУ СО «ЕТХМ» правом ЭЦП определяется распоряжением руководителя ГАПОУ СО «ЕТХМ».

1.6. ЭЦП выдается сроком на один год с момента изготовления. Срок действия ЭЦП указан в сертификате.

1.7. ЭЦП является аналогом собственноручной подписи и должна использоваться только ее владельцем в соответствии с ограничениями, содержащимися в сертификате.

1.8. Сотрудник, обладающий правом ЭЦП (далее - пользователь), вырабатывает самостоятельно или в сопровождении ответственного лица личные закрытый и открытый ключи подписи, а также запрос на получение сертификата открытого ключа (в электронном виде и на бумажном носителе).

1.9. Закрытый ключ подписи - это уникальная последовательность символов, известная только пользователю и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

1.10. Открытый ключ подписи - это уникальная последовательность символов, соответствующая закрытому ключу подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения подлинности ЭЦП в электронном документе.

1.11. Сертификат ключа подписи - это документ на бумажном носителе или электронный документ, который включает в себя открытый ключ ЭЦП и который выдается удостоверяющим центром для подтверждения подлинности ЭЦП и идентификации пользователя.

1.12. Работу с ключами ЭЦП координирует ответственное лицо, назначенное приказом руководителя ГАПОУ СО «ЕТХМ».

1.13. Ответственное лицо проводит инструктаж с пользователями по правилам изготовления, хранения, обращения и эксплуатации ключей.

1.14. Ответственное лицо осуществляет административное и методическое руководство работой пользователей.

1.15. Перед началом работы с ЭЦП пользователь/ответственное лицо обязан изучить настоящую Инструкцию и ознакомиться с ответственностью за выполнение требований Инструкции по правилам обращения с ключевыми документами электронной цифровой подписи.

1.16. В своей деятельности пользователь/ответственное лицо руководствуется настоящей Инструкцией и действующим законодательством в сфере защиты информации.

1.17. Пользователь/ответственное лицо несёт персональную ответственность за выполнение настоящей Инструкции в установленном законом порядке.

2. Правила хранения ключевых документов электронной цифровой подписи

2.1. Право доступа к рабочим местам с установленным программным обеспечением средств ЭЦП и СКЗИ (далее - АРМ пользователя) предоставляется только пользователям и ответственным лицам на основании приказа руководителя ГАПОУ СО «ЕТХМ».

2.2. Несанкционированный доступ посторонних лиц в помещения, в которых установлены технические средства ЭЦП и СКЗИ, исключается.

2.3. На технических средствах, оснащенных средствами ЭЦП и СКЗИ, должно использоваться только лицензионное программное обеспечение.

2.4. Системные блоки АРМ пользователей с установленным СКЗИ и ЭЦП в обязательном порядке подлежат опечатыванию, исключающему возможность несанкционированного изменения аппаратной части АРМ пользователя.

2.5. Ключевая информация как содержащая сведения конфиденциального характера, хранится на учтенных в установленном порядке носителях и не подлежит передаче третьим лицам.

2.6. При обращении с носителями ключевой информации (далее - ключевые носители) должны выполняться требования Инструкции по организации хранения, учета и работы с материальными носителями, содержащими конфиденциальную информацию и персональные данные.

2.7. Хранение ключевых носителей допускается в помещениях, которые имеют прочные входные двери с установленными на них надежными замками, оборудованы охранной сигнализацией и по окончании рабочего дня опечатываются и сдаются под охрану.

2.8. Ключевые носители закрытых ключей подписи и шифрования хранятся в хранилищах в контейнерах, опечатанных личной печатью пользователей.

2.9. Ключевой носитель извлекается из опечатанного контейнера только на время работы с ключами. Перед вскрытием контейнера необходимо проверить целостность печати и ее принадлежность. В нерабочее время опечатанный контейнер с ключевыми носителями должен находиться в хранилище.

2.10. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ и ЭЦП после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

2.11. При необходимости временно покинуть помещение, в котором проводятся работы с использованием ЭЦП, ключевой носитель должен быть вновь помещен в контейнер и опечатан.

2.12. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, в условиях, исключающих возможность несанкционированного доступа (в специальном опечатанном контейнере).

2.13. Транспортирование ключевых носителей за пределы организации допускается только в случаях, связанных с производственной необходимостью. Транспортирование ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

3. Правила работы с ключевыми документами электронной цифровой подписи

3.1. Управление ключевой информацией осуществляют ответственные лица.

3.2. Формирование закрытых ключей ЭЦП производится на учетные съемные носители информации.

3.3. Закрытые ключи изготавливаются не менее чем в двух экземплярах: эталонная и рабочая копии.

3.4. В повседневной работе используется рабочая копия ключевого носителя.

3.5. При физической порче рабочей копии ключевого носителя, пользователь немедленно уведомляет об этом ответственное лицо, которое в присутствии пользователя изготавливает очередную рабочую копию ключевого носителя с эталонной копии с отражением выполненных действий в соответствующих учетных документах.

3.6. Не позднее, чем за 10 рабочих дней до окончания срока действия закрытого ключа, пользователь обязан выполнить мероприятия по формированию новых закрытых ключей.

3.7. Ключи должны быть выведены из действия и уничтожены в следующих случаях:

- плановая смена ключей;

- изменение реквизитов пользователя ЭЦП;
- компрометация ключей;
- выход из строя (износ, порча) ключевых носителей;
- прекращение полномочий пользователя ЭЦП.

3.8. Ключи должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется соответствующим актом.

3.9. Уничтожение ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) ключей без повреждения ключевого носителя.

3.10. Ключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования. Непосредственные действия по стиранию ключевой информации регламентируются эксплуатационной и технической документацией к СКЗИ.

3.11. Для сохранения целостности и нормальной работы ключевого носителя пользователи обязаны:

- оберегать ключевой носитель от механических воздействий (падения, сотрясения, вибрации и т. п.), воздействия высоких и низких температур, агрессивных сред, высокого напряжения;
- не допускать попадания на ключевой носитель (особенно разъем) пыли, грязи, влаги и т. п.;
- при засорении разъема ключевой носитель очистить сухой тканью, использование органических растворителей недопустимо;
- при любых сбоях в работе ключевого носителя проинформировать ответственное лицо/уполномоченных технических специалистов, не предпринимая попыток ликвидировать проблему собственными силами.

3.12. Пользователям/ответственным лицам запрещается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое ключевых носителей и передачу самих носителей лицам, не имеющим соответствующего допуска;
- выводить ключевую информацию на дисплей и принтер;
- использовать ключевые носители в режимах, не предусмотренных правилами пользования СКЗИ, либо использовать ключевые носители на посторонних ПЭВМ;
- записывать на ключевые носители постороннюю информацию.

4. Ответственность

Пользователи и ответственные лица несут ответственность за:

4.1. Сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ.

4.2. Сохранение в тайне содержания закрытых ключей ЭЦП.

4.3. Сохранность носителей ключевой информации.

4.4. Неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, - в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.5. За причинение материального ущерба работодателю - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

4.6. За правонарушения, совершенные в процессе осуществления своей деятельности, - в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

Разработал:
Секретарь

Титова Н.А.