МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
"СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 57 ИМЕНИ СТЕПНОВОЙ ЗОИ ИВАНОВНЫ"
(МБОУ «СОШ № 57»)

Принято
Педагогический совет
Протокол №2
от 24.09.2025 г.

УТВЕРЖДАЮ
Директор МБОУ «СОШ №57»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 7EFB7840DCEDF9DB36EB3C90D58F23B1
Владелец: Мананков Сергей Анатольевич
Действителен: с 27.05.2025 до 20.08.2026

_____ С. А. Мананков
24.09.2025 г.
приказ № 332-од

Положение
об учете, хранении и использовании носителей ключевой информации, криптографических средств и электронной подписи

1. Нормативная база

Настоящее Положение разработано в соответствии с Федеральным законном от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи» и Федеральным законом от 20.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Термины и определения

Администратор информационной безопасности - лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена электронными документами.

Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

Средства криптографической защиты информации (далее - СКЗИ) и квалифицированная электронная цифровая подпись предназначены для подписания электронных документов ЭЦП с целью подтверждения подлинности информации, ее авторства и шифрования при передаче по открытым каналам связи для обеспечения конфиденциальности.

Закрытый ключ подписи - уникальная последовательность символов, известная владельцу сертификата и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

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

Сертификат ключа подписи (сертификат) - 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 владельца сертификата.

Носитель ключевой информации (ключевой носитель) - материальный носитель информации, содержащий закрытый ключ подписи или шифрования.

Шифрование - способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.

СКЗИ и средства ЭЦП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

3. Общие положения

Электронная цифровая подпись выдается сроком на один год с момента изготовления. Срок действия ЭЦП указан в сертификате. По истечении этого срока владельцу ЭЦП необходимо провести плановую смену ЭЦП в Удостоверяющем центре.

Использование ЭЦП в конкретной информационной системе (программе) определяется руководством по эксплуатации данной системы (программы).

ЭЦП является аналогом собственноручной подписи и должна использоваться только ее владельцем в соответствии с ограничениями, содержащимися в сертификате. Пользователь принимает на себя риски, связанные с неправомочным использованием ЭЦП и средств ЭЦП, с подделкой, подлогом либо иным искажением информации, которая содержится в документах, предоставленных Пользователем для получения ЭЦП, компрометацией используемых ключей ЭЦП, нарушений положений Регламента оказания услуг Удостоверяющего центра.

4. Работа с СКЗИ и средствами ЭЦП

Для работы с СКЗИ и средствами ЭЦП в качестве пользователя привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Работу с ключами ЭЦП и шифрования координирует администратор безопасности. Должностные лица, уполномоченные соответствующим приказом руководителя организации, могут эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭЦП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
- сохранение в тайне содержания закрытых ключей ЭЦП;
- сохранность носителей ключевой информации.

В школе должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

Для обеспечения безопасности ЭЦП необходимо:

- хранить ключи ЭЦП на специальных защищенных носителях электронных идентификаторах с использованием надежного пароля;
- обеспечить надежное хранение носителей ключевой информации, исключающее доступ к ним посторонних лиц, не передавать сами носители лицам, к ним не допущенным;
- вставлять ключевой носитель при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.);
- не записывать на ключевой носитель постороннюю информацию;

- не вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭЦП;
- не использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования.

5. Проверка электронной цифровой подписи

Для создания и проверки электронной подписи используются средства ЭЦП, которые:

- позволяют установить факт изменения подписанного электронного документа после момента его подписания;
- обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

При проверке электронной подписи средства ЭЦП должны:

- показывать содержимое электронного документа, подписанного электронной подписью;
- показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;
- указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Пользователь может осуществлять проверку ЭЦП как с помощью используемых средств ЭЦП, так и обратившись в Удостоверяющий центр.

6. Уничтожение ключевой информации

После прекращения действия ключей ЭЦП пользователь должен удалить их путем форматирования ключевого носителя. Инструкцию по форматированию конкретного ключевого носителя необходимо скачать с сайта производителя.

7. Плановая замена ключей и сертификатов ключей

Плановая смена ключей и сертификатов открытых ключей осуществляется за месяц до окончания срока действия имеющихся ответственным лицом организации пользователя.

После окончания действия ключей ЭЦП пользователь должен удалить их с ключевого носителя путем его форматирования.

8. Внеплановая замена ключей и сертификатов ключей

Внеплановая замена ключей и сертификатов закрытых ключей проводится в следующих случаях:

- компрометация ключей;
- изменение идентификационных данных и/или областей использования ключа, указанных в заявлении на изготовление ключей;
- выход из строя ключевого носителя.

К событиям, относящимся к компрометации ключей, относятся следующие ситуации:

- утрата ключевых носителей ключа;

- утрата носителей ключа с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
- доступ посторонних лиц к ключевой информации.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для Пользователя. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет организация, в которой работает Пользователь.

При компрометации ключа Пользователь должен немедленно поставить в известность Удостоверяющий центр о факте компрометации ключей, сообщив номер сертификата. В течение 30 минут после поступления сообщения о компрометации ключа, действие его будет приостановлено до подачи в Удостоверяющий центр письменного заявления об аннулировании скомпрометированных ключей.

Возобновление работы с ЭЦП будет возможно только после замены скомпрометированных ключей.

9. Эксплуатация и хранение электронного идентификатора (носителя ЭЦП)

9.1. Рекомендуется хранить ключевые носители в помещениях, которые имеют прочные входные двери с установленными на них надежными замками. В обязательном порядке для хранения ключевых носителей в помещении должно использоваться металлическое хранилище (сейф, шкаф, секция) заводского изготовления, оборудованное приспособлением для его опечатывания.

9.2. 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.

9.3. На технических средствах, оснащенных средствами ЭЦП, должно использоваться только лицензионное программное обеспечение фирм-производителей.

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

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

9.6. Ответственные исполнители ЭЦП обязаны вести журнал учета хранения электронных носителей конфиденциальной информации и своевременно заполнять его.

9.7. Закрытые ключи изготавливаются в 2-х экземплярах: эталонная и рабочая

копии. В повседневной работе используется рабочая копия ключевого носителя.

9.8. При физической порче рабочей копии ключевого носителя, пользователь немедленно уведомляет об этом администратора безопасности.

10. Категорически не допускается

10.1. Осуществлять несанкционированное администратором безопасности копирование ключевых носителей.

10.2. Разглашать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер.

10.3. Использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭЦП, либо использовать ключевые носители на посторонних ПЭВМ.

10.4. Записывать на ключевые носители постороннюю информацию.

Для нормальной работы носителя ЭЦП, необходимо придерживаться следующих правил эксплуатации и хранения:

- не разбирать электронный идентификатор, это ведет к потере гарантии! Кроме того, при этом возможна поломка корпуса электронного идентификатора, поломка элементов печатного монтажа и т. д.;
- оберегать электронный идентификатор от механических воздействий (падения, сотрясения, вибрации и т. п.), воздействия высоких и низких температур, агрессивных сред, высокого напряжения;
- не прилагать излишних усилий при подсоединении электронного идентификатора к порту компьютера;
- не допускать попадания на электронный идентификатор (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема электронного идентификатора принять меры для его очистки. Для очистки корпуса и разъема использовать сухую ткань. Использование органических растворителей недопустимо.
- в случае неисправности или неправильного функционирования электронного идентификатора обращаться в Удостоверяющий центр.