Приложение к приказу 1
от 29.01.2018 № 17-О

РЕГЛАМЕНТ
по правилам обращения с ключевыми документами электронной цифровой подписи МАДОУ ДСКВ «Сказка»

1. Термины и определения

Администратор безопасности информации – 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.

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.

2. Общие положения

2.1. Настоящий Регламент предназначена для пользователей автоматизированных систем, использующих средства электронной цифровой подписи (ЭЦП).

2.2. Электронно-цифровая подпись юридически равносильна живой подписи ее владельца.

2.3. Криптографические методы защиты позволяют обеспечить защиту целостности и авторства электронной информации применением ЭЦП. Невозможность ввода информации от чужого имени (невозможность подделки ЭЦП) гарантируется при сохранении в тайне закрытого ключа ЭЦП пользователей.

2.4. Регламент содержит основные правила обращения с системами электронного документооборота и ключами ЭЦП, строгое выполнение которых необходимо для обеспечения защиты информации при обмене электронными документами.

2.5. Лица, допущенные к работам с ключами ЭЦП, несут персональную ответственность за безопасность (сохранение в тайне) закрытых ключей подписи и обязаны обеспечивать их сохранность, неразглашение и нераспространение, несут персональную ответственность за нарушение требований настоящей Инструкции.

2.6. Непрерывная организационная поддержка функционирования автоматизированных рабочих мест (АРМ) с ЭЦП предполагает обеспечение строгого соблюдения всеми пользователями требований администратора безопасности.

3. Порядок генерации ЭЦП

3.1. Порядок генерации ЭЦП регламентируется соответствующим Регламентом Удостоверяющего центра.

3.2. Владельцы ЭЦП и ответственные исполнители ЭЦП назначаются приказом руководителя (см. Приложение №1).

3.3. Пользователь, обладающий правом ЭЦП (ответственный исполнитель ЭЦП), вырабатывает самостоятельно или в сопровождении администратора безопасности личный открытый ключ подписи, а также запрос на получение сертификата открытого ключа (в электронном виде и на бумажном носителе).

3.4. Сертификаты ЭЦП и сами ЭЦП выдаются ответственному должностному лицу учреждения по доверенности, согласно соответствующего Регламента удостоверяющего центра.

3.5. Формирование закрытых ключей подписи и шифрования производится на учтенные съемные носители информации:

- дискета 3.5";
- идентификатор Touch-Memory DS1993 – DS1996;
- идентификатор Rutoken и т.д.

3.6. Закрытые ключи изготавливаются в 1 экземпляре. Срок действия ключей – 1 год с момента выдачи сертификата.

3.7. Ни при каких обстоятельствах нельзя хранить ключи ЭЦП на жестких дисках АРМ.

4. Порядок хранения и использования ЭЦП

4.1. Право доступа к рабочим местам с установленным программным обеспечением средств ЭЦП предоставляется только тем лицам, которые по приказу руководителя назначены ответственными исполнителями ЭЦП (см. Приложение №1) и им предоставлены полномочия на эксплуатацию этих средств.

4.2. Рекомендуется хранить ключевые носители в помещениях, которые имеют прочные входные двери с установленными на них надежными замками. Допускается для хранения ЭЦП использовать кассовое помещение.

4.3. В обязательном порядке для хранения ключевых носителей в помещении должно использоваться металлическое хранилище (сейф, шкаф, секция) заводского изготовления, оборудованное приспособлением для его опечатывания. Опечатывание хранилища должно производиться личной печатью ответственного исполнителя ЭЦП или его владельца.

4.4. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним. Для этого ключевые носители помещаются в специальный контейнер, опечатываемый личной металлической печатью ответственного исполнителя или владельца ЭЦП.

4.5. 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.

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

4.7. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства ЭЦП.

4.8. 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.

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

4.10. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения и должны быть учтены по соответствующим учетным формам

4.11. Формирование закрытых ключей подписи и шифрования производится на учтенные съемные носители информации:

- дискета 3.5";
- идентификатор Touch-Memory DS1993 - DS1996;
- идентификатор Rutoken и т.д.

4.12. Закрытые ключи изготавливаются в 1 экземпляре эталонная. Срок действия ключей – 1 год с момента выдачи сертификата.

4.13. Ни при каких обстоятельствах нельзя хранить ключи ЭЦП на жестких дисках АРМ.

4.14. 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.

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

4.16. Категорически не допускается:

- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер;
- использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭЦП, либо использовать ключевые носители на посторонних ПЭВМ;
- записывать на ключевые носители постороннюю информацию.

4.17. Не позднее, чем за 30 рабочих дней до окончания срока действия закрытого ключа, его ответственный исполнитель обязан выполнить мероприятия по формированию новых закрытых ключей, соответствующего запроса на издание сертификата и оформить заявку на получение нового сертификата.

5. Порядок уничтожения ключей на ключевых носителях

5.1. Приказом директора института или руководителей его филиалов и подразделений должна быть создана комиссия по уничтожению ключевой информации.

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

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

5.3. Уничтожение ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) ключей без повреждения ключевого носителя. Ключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, Touch Memory, Rutoken и т.п.). Непосредственные действия по стиранию ключевой информации регламентируются эксплуатационной и технической документацией.

6. Ключи должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется актом (см. Приложение № 2) и отражается в соответствующих учетных формах.

7. Действия при компрометации ключей

7.1. Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

7.2. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей;
- потеря ключевых носителей с последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия ключа);
- возникновение подозрений на утечку информации или ее искажение;
- нарушение печати на контейнере с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в т.ч. случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

7.3. При компрометации ключа пользователь немедленно прекращает обмен электронными документами с другими пользователями и извещает о факте компрометации.

7.4. По факту компрометации ключей должно быть проведено служебное расследование с оформлением уведомления о компрометации.

7.5. Факт компрометации закрытых ключей подписи должен быть подтвержден официальным уведомлением института в адрес Удостоверяющего центра о компрометации в письменном виде. Уведомление должно содержать идентификационные параметры сертификата, дату и время компрометации, характер компрометации, подпись владельца ключа подписи, подпись руководителя и печать института или его филиала.

7.6. Выведенные из действия скомпрометированные ключи уничтожаются (см. п.5.2 настоящей Инструкции), о чем делается запись в журнале учета ЭЦП.

8. Обязанности Администратора безопасности информации

8.1. Администратор безопасности проводит опечатывание системных блоков рабочих станций с установленным средством ЭЦП, исключающее возможность несанкционированного изменения аппаратной части рабочих станций. При этом номер пломбы заносится в Учетную карточку персонального компьютера и в Журнал заявок на ремонт персональных компьютеров и оргтехники.

8.2. Администратор безопасности инструктирует Пользователей систем электронного документооборота по правилам обращения с ЭЦП.

8.3. Администратор безопасности контролирует целостность аппаратных средств и программных продуктов, используемых для систем электронного документооборота, в которых используются ЭЦП.

8.4. Контроль за правильностью и своевременностью выполнения регламентных работ с ЭЦП осуществляет Администратор безопасности и уполномоченные лица Удостоверяющего центра.

8.5. Администратор безопасности осуществляет непрерывный контроль за всеми действиями Пользователей систем электронного документооборота, в которых используются ЭЦП.

8.6. Не реже чем 2 раза в год Администратор безопасности информации проводит проверки всех АРМ пользователей, используемых для систем электронного документооборота на предмет соблюдения требований действующих Регламентов Удостоверяющих центров и настоящей Инструкции.

9. Обязанности Ответственных исполнителей ЭЦП

9.1. Ответственные исполнители ЭЦП при работе с ключевыми документами обязаны руководствоваться положениями соответствующего Регламента Удостоверяющего центра и настоящей Инструкции.

9.2. Ответственные исполнители ЭЦП обязаны организовать свою работу по генерации ЭЦП в полном соответствии с положениями соответствующего Регламента Удостоверяющего центра и п.3 настоящей Инструкции.

9.3. Ответственные исполнители ЭЦП обязаны организовать свою работу с ключевыми документами в полном соответствии с п.4 настоящей Инструкции.

9.4. Уничтожение ключевой информации с ключевого носителя может производится только в полном соответствии с положениями соответствующего Регламента Удостоверяющего центра и п.5 настоящей Инструкции.

9.5. В случае каких-либо изменений реквизитов ЭЦП (плановая смена ключей, изменение реквизитов владельцев или Ответственных исполнителей, генерация новой ЭЦП, и др.) в течении 3 суток Ответственные исполнители ЭЦП обязаны предоставить Администратору безопасности информации следующие документы:

- копию Приказа о назначении Владельцев и Ответственных исполнителей ЭЦП;
- копию Сертификата новой ЭЦП;
- копию Акта на уничтожение ключей ЭЦП (см. Приложение № 1).

9.6. Ответственные исполнители ЭЦП обязаны выполнять требования Администратора безопасности информации в части, касающейся обеспечения информационной безопасности института, его подразделений и филиалов.

Приложение № 2
по правилам обращения с ключевыми документами
электронной цифровой подписи
МАДОУ ДСКВ «Сказка»

АКТ

на уничтожение ключей ЭЦП (шифрования)

"_____" _____ 200__г

Комиссия, _____
(наименование организации, номер и дата приказа)
в составе: председателя _____,
и членов комиссии _____
в присутствии пользователя КД по причине _____
(окончание срока действия , прекращение полномочий , компрометация)
подготовила к уничтожению ключевые документы **стиранием** ключевой информации:

Таблица 1.*

Ключевой носитель	**Учетный № ДСП**	**Экз. №**	**Реквизиты сертификата**	**Ф.И.О. владельца сертификата ключа ЭЦП**
ГМД				

Комиссия установила, что при подготовке данных информация с ГМД, указанных в табл. 2, не считывается. Перечисленные ГМД к дальнейшему использованию не пригодны и подлежат **уничтожению** измельчением магнитных дисков.

Таблица 2.*

Ключевой носитель	**Учетный № ДСП**	**Экз. №**	**Реквизиты сертификата**	**Ф.И.О. владельца сертификата ключа ЭЦП**
ГМД				

Члены комиссии:

_____ _____
(подпись) (Ф.И.О)

_____ _____
(подпись) (Ф.И.О)

«Разрешаю уничтожить»

_____
(руководитель организации)

_____
(подпись) (Ф.И.О.)

МП «_____»

_____200__г.

Ключевые документы, перечисленные в табл. 1, уничтожены стиранием ключевой информации двойным форматированием.

Ключевые документы, перечисленные в табл. 2, уничтожены методом измельчения магнитных дисков.

Члены комиссии:

_____ _____
(подпись) (Ф.И.О)

_____ _____
(подпись) (Ф.И.О)