Муниципальное бюджетное дошкольное образовательное учреждение
детский сад №107

«УТВЕРЖДАЮ»

Заведующий _____ И.С.Лебедева

(должность) (подпись) (расшифровка подписи)

«01» сентября 2025 г.

ПОЛОЖЕНИЕ
об учете, хранении и использовании ЭЦП в МБДОУ детском саду № 107

1. Термины и определения

Заведующий – 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. Настоящее Положение предназначено 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. Положение 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 настоящего Положения.

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

2.7. Работу с ключами ЭЦП и шифрования координирует администратор безопасности (лицо, ответственное за безопасность информации). Администратор безопасности проводит инструктаж с пользователями по правилам изготовления, хранения, обращения и эксплуатации ключей.

3. Порядок генерации ЭЦП

3.1. Порядок генерации ЭЦП регламентируется соответствующим регламентом Организации.

3.2. Владельцы ЭЦП и ответственные исполнители ЭЦП назначаются приказом заведующего МБДОУ детским садом №107 Лебедевой И.С..

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 Организации по доверенности.

3.5. Формирование закрытых ключей подписи и шифрования

производится на учтенные съемные носители информации.

3.6. Закрытые ключи изготавливаются в двух экземплярах: эталонная и рабочая копии. В повседневной работе используется рабочая копия ключевого носителя. Срок действия ключей – один 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 заведующего МБДОУ детского сада № 107 назначены ответственными исполнителями ЭЦП 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.

4.3. В обязательном порядке для хранения ключевых носителей в помещении должно использоваться металлическое хранилище (сейф, шкаф, секция).

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. Ответственные исполнители ЭЦП обязаны вести журнал учета ключевых документов и своевременно заполнять его.

4.10. Ключевая информация содержит сведения

конфиденциального характера, хранится на учтенных в установленном порядке носителях и не подлежит передаче третьим лицам.

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

4.12. При физической порче рабочей копии ключевого носителя пользователь немедленно уведомляет об этом заведующего.

4.13.

4.14. Категорически не допускается:

- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на монитор 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;
- оставлять носитель ключевой информации без личного присмотра где бы то ни было;
- использовать носитель ключевой информации на заведомо неисправном дисководе и/или ПЭВМ;
- подписывать закрытым и открытым ключом подписи любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы;
- сообщать кому-либо вне работы, что он является владельцем ключа ЭЦП.

4.15. 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 заведующего 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. Непосредственные действия по стиранию ключевой информации регламентируются эксплуатационной и технической документацией.

5.4. Ключи должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется соответствующим актом и отражается в соответствующих учетных формах.

6. Действия при компрометации ключей

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

6.2. 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 том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

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

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

6.5. Факт компрометации закрытых ключей подписи должен быть подтвержден официальным уведомлением 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.

6.6. Выведенные из действия скомпрометированные ключи

уничтожаются (п. 5.2 Положения), о чем делается запись в журнале учета ЭЦП.

7. Обязанности Ответственных исполнителей ЭЦП

7.1. Ответственные исполнители ЭЦП при работе с ключевыми документами обязаны руководствоваться настоящим Положением.

7.2. Ответственные исполнители ЭЦП обязаны организовать свою работу по генерации ЭЦП в полном соответствии с настоящим Положением.

7.3. Ответственные исполнители ЭЦП обязаны организовать свою работу с ключевыми документами в полном соответствии с настоящим Положением.

7.4. Уничтожение ключевой информации с ключевого носителя может производиться только в полном соответствии с настоящим Положением.

7.5. Ответственные исполнители ЭЦП обязаны выполнять требования заведующего в части, касающейся обеспечения информационной безопасности Организации.