Маркова Светлана Николаевна

Подписано цифровой подписью: Маркова Светлана Николаевна
DN: 1.2.643.3.131.1.1=120C323434333033033033232 31, 1.2.643.100.3=120B303437353235333731363 4, email=belya_yar2016@mail.ru, c=RU, st=Красноярский край, o=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "БЕЛОЯРСКИЙ ДЕТСКИЙ САД", givenName=Светлана Николаевна, sn=Маркова, cn=Маркова Светлана Николаевна
Дата: 2022.12.06 14:02:02 +07'00'

Приложение № 1
к Приказу № 117 от «06» декабря 2022 г

УТВЕРЖДАЮ:
Заведующий МБДОУ «Белоярский ДС»
_____ С.Н. Маркова

РЕГЛАМЕНТ
применения электронной цифровой подписи в Муниципальном бюджетном дошкольном образовательном учреждение «Белоярский детский сад»

2022г

Редакция действует с 06 декабря 2022 г.

СОДЕРЖАНИЕ 1.

1. Общие положения

1.1. Настоящий Регламент предназначен для пользователей автоматизированных систем, использующих средства электронной цифровой подписи (ЭЦП) и устанавливает порядок применения электронной подписи при организации электронного взаимодействия (далее - Регламент).

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

1.3. 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.

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

1.5. 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.

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

2. Термины и определения

Закрытый ключ ЭЦП - уникальная последовательность символов, предназначенная для создания электронной подписи с использованием средств электронной цифровой подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Подтверждение подлинности ЭЦП в электронном документе – положительный результат проверки принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи,

Квалифицированный сертификат - Сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный Аккредитованным удостоверяющим центром.

Квалифицированной электронной подписью является Электронная подпись, которая соответствует всем признакам Неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом.

Неквалифицированной электронной подписью является Электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

Оператор Системы электронного документооборота - лицо, обеспечивающее функционирование и использование Системы электронного документооборота. Оператором Системы электронного документооборота является Распространитель информации.

Подтверждение подлинности электронной подписи в электронном документе - положительный результат проверки средством электронной подписи с использованием сертификата ключа подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе.

Сертификат ключа проверки электронной подписи - 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.

Система электронного документооборота - организационно-техническая автоматизированная информационная система электронного документооборота, представляющая собой совокупность программного, аппаратного и информационного обеспечения ее участников. Система электронного документооборота является автоматизированной информационной системой, действующей по правилам, устанавливаемым Распространителем информации.

Средства аккредитованного удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций Аккредитованного удостоверяющего центра.

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

Формирование (создание) ЭЦП – процесс, в качестве исходных данных которого используются электронный документ, закрытый ключ ЭЦП и параметры ЭЦП, результатом которого является электронная цифровая подпись.

Удостоверяющий центр - юридическое лицо, либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче Сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, юридические и физические лица.

Электронная подпись - 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.

Электронный документ - сообщение или документ в электронной форме, соответствующей требованиям Распространителя информации к формату электронных документов, содержащий информацию о ценных бумагах и об иных финансовых инструментах, иную информацию, предоставленную Субъектами раскрытия информации, которая в соответствии с требованиями федеральных законов и принятых в соответствии с ними нормативных правовых актов, а также нормативных актов Банка России,

регулирующих объем, порядок и сроки раскрытия информации эмитентами ценных бумаг, и раскрытия информации, связанной с деятельностью акционерных инвестиционных фондов и управляющих компаний паевых инвестиционных фондов, подлежит раскрытию в ленте новостей и (или) на странице Распространителя информации в сети Интернет. Электронный документ должен быть подписан Квалифицированной электронной подписью.

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.
3.3. Сертификаты ЭЦП и сами ЭЦП выдаются ответственному должностному лицу учреждения по доверенности, согласно, соответствующего Регламента удостоверяющего центра.
3.4. Формирование закрытых ключей подписи и шифрования производится на учтенные съемные носители информации USB.
3.5. Закрытые ключи изготавливаются в 1 экземпляре. Срок действия ключей - 1 год с момента выдачи сертификата.
3.6. Ни при каких обстоятельствах нельзя хранить ключи ЭЦП на жестких дисках АРМ.

4. Порядок использования и хранения квалифицированной электронной подписи

4.1. Участники информационного обмена при размещении сведений обязаны использовать квалифицированные сертификаты ключей подписей, выданные авторизованными удостоверяющими центрами, соответствующие требованиям, установленным статьей 17 Федерального закона от 6 апреля 2011 г. № 63 ФЗ "Об электронной подписи".
Подписанные квалифицированной электронной подписью электронные документы, размещаемые Участниками информационного обмена, проходят процедуру проверки электронной подписи.
При информационном обмене обработке подлежат электронные документы, которые подписаны квалифицированной электронной подписью Участника информационного обмена, признанной действительной.
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) заводского изготовления.
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.
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. Формирование закрытых ключей подписи и шифрования производится на учтенные съемные носители информации: USB.
4.7. Закрытые ключи изготавливаются в 1 экземпляре эталонная. Срок действия ключей — 1 год с момента выдачи сертификата.
4.8. При необходимости временно покинуть помещение, в котором проводятся работы с использованием ЭЦП, ключевой носитель должен быть вновь помещен в контейнер и убран в сейф.
4.9. 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.
4.10. 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.
4.11 Компрометация ключей
Под компрометацией закрытого ключа электронной цифровой подписи (ЭЦП) понимается его утрата, хищение, разглашение, несанкционированное копирование, увольнение сотрудника, имеющего доступ к закрытому ключу ЭЦП, любые другие виды разглашения закрытого ключа ЭЦП, а также такие случаи, когда нельзя достоверно установить, что произошло с носителем, содержащим закрытый ключ ЭЦП.
Участник информационного обмена в случае компрометации принадлежащего ему ключа электронной подписи незамедлительно извещает об этом авторизованный удостоверяющий центр для прекращения действия сертификата ключа проверки электронной подписи, соответствующего этому ключу электронной подписи.

5. Порядок приостановления действия и отзыва сертификата
В процессе управления сертификатами ключей подписи Удостоверяющий центр, имеет возможность отзыва и приостановления действия выпущенных им сертификатов ключей подписи, что необходимо для досрочного прекращения их действия.
5.1 Отзыв сертификата ключа подписи
5.1.1 Ключи должны быть выведены из действия и уничтожены в следующих случаях:

- компрометация закрытого ключа ЭЦП;
- потеря закрытого ключа ЭЦП;
- подозрение на компрометацию закрытого ключа ЭЦП;
- прекращение полномочий пользователя ЭЦП.
- истечение срока действия сертификата ключа подписи;
- утрата юридической силы сертификата соответствующих средств электронной цифровой подписи;
- прекращение действия документа, на основании которого оформлен сертификат ключа подписи;
- заявление владельца сертификата ключа подписи.

5.1.2 Инициаторы отзыва сертификата
Запрос на отзыв сертификата ключа подписи может быть сделан:

- владельцем сертификата;
- Удостоверяющим центром;

5.1.3 Процедура отзыва сертификата
Отзыв сертификата ключа подписи, изготовленного Удостоверяющим центром, осуществляется по заявлению на отзыв сертификата ключа подписи.
В случае необходимости отзыва сертификата ключа подписи, пользователь должен немедленно сообщить об этом в Удостоверяющим центром. Для этого пользователь формирует заявление на отзыв сертификата.
Заявление на отзыв сертификата ключа подписи подается в Удостоверяющим центром пользователем, либо руководителем организации, сотрудником которой является пользователь, в бумажном виде, если это предусмотрено соответствующим соглашением с Удостоверяющим центром.

Удостоверяющий центр после получения запроса на отзыв сертификата ключа подписи в максимально короткие сроки аннулирует сертификат.
Отозванный сертификат немедленно помещается в список отозванных сертификатов (СОС).
5.2 Приостановление действия сертификата ключа подписи
Приостановление действия сертификата ключа подписи Удостоверяющим центром позволяет впоследствии возобновить действие приостановленного сертификата ключа подписи.
В том случае, если по истечении срока приостановления действия не поступает указания о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.
5.2.1 Процедура приостановления действия сертификата
Приостановление действия сертификата ключа подписи, изготовленного
Удостоверяющим центром, осуществляется по заявлению на приостановление сертификата ключа подписи его владельца.
Заявление на приостановление действия сертификата ключа подписи подается пользователем Удостоверяющим центром в бумажной форме.
Срок рассмотрения заявления на приостановление действия сертификата ключа подписи устанавливается регламентом функционирования, соответствующего Удостоверяющим центром.
Действие сертификата ключа подписи может быть приостановлено Удостоверяющим центром на основании указания лиц или органов, имеющих такое право в силу закона или договора.
5.2.2 Процедура возобновления действия приостановленного сертификата.
Возобновление действия приостановленного сертификата ключа подписи, изготовленного Удостоверяющим центром, осуществляется по соответствующему заявлению его владельца.
Заявление на возобновление действия приостановленного сертификата ключа подписи подается заявителем бумажной форме в Удостоверяющий центр.
Срок рассмотрения заявления на возобновление действия сертификата ключа подписи устанавливается регламентом функционирования, соответствующего удостоверяющего центра.
5.2.3 Настоящий Регламент применения электронной цифровой подписи в Муниципальном бюджетном дошкольном образовательном учреждение «Белоярский детский сад» действует с 06.12.2022г до принятия нового.