Согласовано:
Председатель ПК
_____А.В.Нефёдова

Утверждаю:
Заведующий МБДОУ
«Детский сад № 2»
_____Е.А.Чихун
Приказ №61/1 -ОД от 01.04.2023г.

ИНСТРУКЦИЯ
по работе с электронной подписью в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад общеразвивающего вида с приоритетным осуществлением деятельности по познавательно-речевому развитию детей №2».

1. Общие положения

Инструкция разработана для сотрудников МБДОУ «Детский сад № 2» в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ РФ от 13 июня 2001 г. № 152, Приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» и иными нормативными правовыми актами Российской Федерации.

1. Пользователи средствами электронной подписи обязаны:

обеспечить сохранность, функционирование и безопасность средств электронной подписи (далее – средства ЭП);

обеспечить сохранность личных печатей, ключей от помещений и хранилищ;

обеспечить конфиденциальность ключей электронных подписей;

выполнять указания ответственного пользователя;

не разглашать информацию об средствах ЭП, ключевых документах к ним;

не допускать снятие копий с ключевых документов;

не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

не допускать записи на ключевой носитель посторонней информации;

не допускать установки ключевых документов в другие ПЭВМ;

под расписку в журнале поэкземплярного учета получать экземпляры средств электронной подписи (далее - пользователей), эксплуатационной и технической документации к ним, ключевых документов;

на время отсутствия пользователей средствами ЭП, оборудование, функционирующее со средствами ЭП, должно быть выключено, отключено от линии связи и убрано (при технической возможности) в опечатываемые хранилища;

по окончании рабочего дня закрыть и сдать под охрану: помещения в которых осуществляется работа со средствами ЭП; сейфы (металлические шкафы, хранилища) предназначенные для хранения средств ЭП. Находящиеся в пользовании ключи от сейфов (металлических шкафов, хранилищ) сдать под расписку в соответствующем журнале пользователю, ответственному за обработку информации содержащей персональные данные (далее – ответственный пользователь);

сдать и списать со своего лицевого счёта средства ЭП, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием средств ЭП;

немедленно сообщить ответственному пользователю о возможном несанкционированном проникновении в помещения, сейфы (металлические шкафы, хранилища) посторонних лиц;

немедленно сообщить ответственному пользователю о попытках посторонних лиц получить сведения об используемых ЭП или ключевых документах к ним;

немедленно уведомить ответственного пользователя о фактах утраты или недостачи средств ЭП, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

2. Ответственный пользователь обязан:

обеспечить функционирование и безопасность средств ЭП;

осуществлять текущий контроль за организацией и обеспечением функционирования средств ЭП;

осуществлять поэкземплярный учет используемых средств ЭП, эксплуатационной и технической документации к ним, носителей персональных данных;

осуществлять учет лиц, допущенных к работе со средствами ЭП;

осуществлять контроль за соблюдением условий использования средств ЭП;

осуществлять разбирательство и составление заключений по фактам нарушения условий хранения и использования средств ЭП;

осуществлять допуск пользователей к работе со средствами ЭП по решению руководителя Учреждения;

вести на каждого пользователя лицевой счет и регистрировать числящиеся за ними средства ЭП, эксплуатационную и техническую документацию к ним;

выдавать пользователям средства ЭП, эксплуатационную и техническую документацию к ним и ключевые документы под расписку в соответствующем журнале поэкземплярного учета;

по окончании рабочего дня закрыть и опечатать помещения, сейфы (металлические шкафы, хранилища).

3. Учёт средств электронной подписи.

Средства ЭП, эксплуатационная и техническая документация подлежат поэкземплярному учету с использованием индексов или условных наименований и регистрационных номеров.

Средства ЭП, эксплуатационная и техническая документация числящиеся за пользователями подлежат регистрации на их лицевых счетах.

Средства ЭП, эксплуатационная и техническая документация выдаются пользователям под расписку в соответствующем журнале поэкземплярного учета.

4. Хранение средств электронной подписи.

Хранение средств ЭП, эксплуатационной и технической документации должно осуществляется в сейфах или хранилищах, оборудованных внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания замочных скважин.

Хранение действующих и резервных средств ЭП, эксплуатационной и технической документации должно осуществляется раздельно.

5. Передача средств электронной подписи.

Передача по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования средств ЭП осуществляется только с использованием средств ЭП.

Передача средств ЭП, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями и (или) ответственным пользователем под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями должна быть санкционирована ответственным пользователем.

6. Уничтожение средств электронной подписи.

Уничтожение средств ЭП (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) средств ЭП (исходной ключевой информации) без повреждения ключевого носителя.

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации.

Средства ЭП уничтожают по решению руководителя, владеющего средствами ЭП, с уведомлением организации, ответственной за ведение поэкземплярного учета средств ЭП.

Электронные записи ключевой информации выведенные из действия уничтожаются пользователями этих средств самостоятельно под расписку в техническом (аппаратном) журнале.

7. Компрометация и потеря средств электронной подписи.

При наличии оснований полагать, что конфиденциальность ключа нарушена (скомпрометирована), использование ключа электронной подписи – запрещено.

В случае компрометации средств ЭП необходимо уведомить удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

О нарушениях, которые могут привести к компрометации средств ЭП, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи обязаны сообщать ответственному пользователю (руководителю организации).

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации средств ЭП, если при этом исключалась возможность их копирования (чтения, размножения).

В случаях потери, недостачи или не предъявления ключевых носителей, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

8. Организация режима охраны в помещениях где проводится работа с электронной подписью.

Организация режима доступа в помещения должна исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними ведущихся там работ.

Помещения, как правило, должны быть оснащены охранной сигнализацией. Режим охраны помещений должен предусматривать периодический контроль за состоянием технических средств охраны.

Входные двери помещений должны быть прочными, с замками, гарантирующими надежное закрытие помещений в нерабочее время.

Входные двери должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.

Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в помещения, под расписку в журнале учета. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе ответственного пользователя.

Окна помещений должны быть защищены от просмотра извне. Окна помещений, расположенных на первых или последних этажах зданий, около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками (ставнями) и системой предотвращения просмотра извне.

Аппаратные средства, с которыми осуществляется штатное функционирование средств ЭП, а также аппаратные и аппаратно-программные средства ЭП должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).